



OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
— for —
British Columbia

SUBMISSION ON A NATIONAL IDENTITY CARD

Standing Committee on Citizenship & Immigration

February 17, 2003

Victoria, British Columbia

[1] This submission addresses privacy issues raised by the proposal of The Honourable Denis Coderre, Minister of Citizenship and Immigration (“Minister”), for a national identity card. This submission will form the substance of the February 17, 2003 testimony of David Loukidelis, Information and Privacy Commissioner for British Columbia, to the Standing Committee on Citizenship and Immigration at Victoria, British Columbia.

1.0 SUMMARY

[2] A considerably more comprehensive, deliberate and meaningful national consultation is necessary before the federal government even considers approving a national identity card scheme. The necessary consultation cannot happen, however, until the Minister’s proposal, which is vague, is considerably clarified.

[3] A national identity card with a unique identifier, which could be used to record transaction information, to give access to disparate data or to link data, is not desirable. Any controls placed on the uses of such a card would inevitably be open to function creep over time, with the card potentially, indeed almost certainly, evolving into a tool of surveillance.

[4] No case has been made that a new national identity card that better identifies its holder, including by using biometrics, would be effective in combating terrorism. The cost of a national identity card scheme would be well into the billions of dollars. A more secure form of identification could help combat identity theft, but it would be far more cost-effective for the federal government to invest, in co-operation with the provinces and territories, more modest amounts of tax dollars in enhancing the security of passports,

birth certificates and driver's licences. No case has been made for creating a new, single-point identity card from scratch, at great expense.

2.0 DISCUSSION

[5] The following discussion addresses, in summary fashion, some of the more serious issues raised by a national identity card scheme. Such a proposal raises other concerns. Given the uncertainty as to what the Minister actually has in mind in proposing a national identity card, however, it is not appropriate to discuss all possible issues and concerns at this time.

More consultation is necessary

[6] The Minister said in Parliament on February 13, 2003 that he wants to debate the issues, that he is open to debate on his proposal for a national identity card. Meaningful debate is next to impossible at this time, however, because it is not clear what is being proposed. Before proceeding, the government should better define the nature and uses of the proposed card, provide clear and unequivocal justifications for its implementation, and then undertake a comprehensive and deliberate consultation process. The government also should prepare, and release, a privacy impact assessment of the proposal as part of the groundwork for further consultation.

[7] Before addressing the merits of a national identity card, some observations about their constitutional and historical background are desirable.

Constitutional dimensions of privacy

[8] New laws and measures implemented since 9/11 have diminished the privacy rights of Canadians. The need for some of these measures is not seriously open to question. Others, however, are not warranted; a national identity card falls into this category. Before explaining why this is so, the prevailing climate of privacy-erosion calls for some discussion of the fundamental importance of privacy to our way of life.

[9] Privacy has a number of manifestations. One dimension of 'privacy' is the right to anonymityⁱ. The importance of preserving, as far as possible, the individual's right to choose to maintain or to give up anonymity has been expressed as followsⁱⁱ:

The right to remain anonymous (leaving no trace to one's identity) is something we have sought to maintain as a fundamental element in defending our private space. At best, we should only have to identify ourselves to government or business when knowledge of our identity is essential to concluding a particular transaction. It would not normally be essential when we are merely seeking information. Otherwise, we should be able to choose whether or not to reveal our identity. This is true as much in the electronic world as in the physical world.

[10] An identity card that must be produced on demand (whether by law or practically-speaking) by police, other state agents or private sector actors would strike at the heart of our right to generally choose when to identify ourselves to others. That right cannot be compromised unless a clear and compelling state interest in doing so has been

demonstrated. The consequences of the erosion or loss of anonymity through a generalized obligation to identify oneself promise to be far-reaching and profound:

... It is not easy to distinguish just what is lost when chances for anonymity are lost from all the other things that are typically also being lost in societies in which anonymity is eroded. But its loss does bring about in people a generalised anxiety arising from a sense of vulnerability and exposure. How people's behaviour changes in response to this is also difficult to disentangle from their behavioural responses to the other things that they are also experiencing in societies that are eroding anonymity, and in any case, this will vary between people in different situations and different kinds of local social organisation and sub-culture. However, among the responses are likely to be decreased trust in large organisations generally and in government bodies in particular, increased investment in more furtive behaviour, attempts to engage in petty misrepresentation of identity when one believes that one can do so without consequences, deepening distrust of organisations, withdrawal from public engagement (Raab, 1997) and perhaps investment in the informal economy – all phenomena that can be deeply corrosive of the very sense of communality that many people who advocate the limiting of privacy want to foster (cf. Etzioni, 1999).ⁱⁱⁱ

[11] Another dimension to privacy is the right to informational self-determination. This can be described, as others have done, as the claim to control over the conditions under which information about oneself is collected, compiled used and disclosed by others^{iv}. A 1972 federal task force on privacy and computers observed that informational privacy “derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain ... as he sees fit.” The report stated that every citizen has a “basic and continuing interest” in what happens to his or her personal information, and in “controlling access to it.”^v

[12] The Supreme Court of Canada has affirmed that the *Canadian Charter of Rights and Freedoms* embodies the principle that an individual should be in control of his or her own personal information. The Court has identified this as a defining characteristic of freedom in the modern state, a characteristic that becomes ever more important as the technological drive to, and capabilities for, data collection, linkage and analysis become more appealing to governments and easier to deploy. In *Hunter v. Southam Inc.*^{vi}, the Court held that privacy was to be given broad protection under the *Charter*. In *R. v. Dymont*^{vii}, the Court said the following about the fundamental importance of privacy in our modern state:

The foregoing approach is altogether fitting for a constitutional document enshrined at the time when, Westin tells us, society has come to realize that privacy is at the heart of liberty in a modern state; see Alan F. Westin, *Privacy and Freedom* (1970), pp. 349-50. Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for the public order. The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state.

[13] In *R. v. Plant*^{viii}, the Court later re-affirmed the fundamental importance, and nature, of privacy:

In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the *Charter* should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.

[14] In *R. v. Mills*^{ix}, the Court acknowledged that it had “most often characterized the values engaged by privacy in terms of liberty, or the right to be left alone by the state”^x, adding that the interest in being left alone by the state includes the ability to control the dissemination of confidential information.^{xi} Last, the Court again acknowledged that “the significance of privacy concerns should not be understated”^{xii} and went on to quote the following words of philosopher Charles Fried^{xiii}:

To respect, love, trust, feel affection for others and to regard ourselves as the objects of love, trust and affection is at the heart of our notion of ourselves as persons among persons, and privacy is the necessary atmosphere for these attitudes and actions, as oxygen is for combustion.

[15] The Supreme Court of Canada has, of course, acknowledged that privacy rights, like other rights guaranteed under the *Charter*, may be subjected to certain limits. The following statement in *R. v. Dyment*^{xiv} is an example of this:

One further general point must be made, and that is that if the privacy of the individual is to be protected, we cannot afford to wait to vindicate it only after it has been violated. This is inherent in the notion of being secure against unreasonable searches and seizures. Invasions of privacy must be prevented, and where privacy is outweighed by other societal claims, there must be clear rules setting forth the conditions in which it can be violated. This is especially true of law enforcement, which involves the freedom of the subject.

[16] To summarize, individual privacy rights are crucial to the well-being of each and all of us, to the health of our entire society. The constitutional underpinnings of privacy recognize its basic importance to the health of our democracy.

Historical background to the identity card debate

[17] The idea of a national identity card has always been received with great skepticism by a Canadian public protective of individual privacy rights and wary of government surveillance. It is sometimes said this is a cultural phenomenon. Many European countries have such cards, yet identity cards have never been accepted in any country with British roots. Proposals for identity cards have failed in Australia, New Zealand and the U.K. Following 9/11, an identity card was proposed in the U.S., but the idea was abandoned as criticism mounted on both the left and right of the political spectrum. The failure of identity card proposals in these countries shows that people oppose having to carry identification or being forced to identify themselves on a routine or general basis. Indeed, the situations in which authorities in Canada, the United States

and the United Kingdom can require an individual to identify himself or herself remain limited, *e.g.*, the requirement that motor vehicle drivers identify themselves to police.

[18] In some European countries, the police may ask citizens to produce their identity cards for specified reasons. These countries include France, Greece, Italy, Luxemburg, Portugal and Spain.^{xv} Even in European countries where citizens must have an identity card, however, it is not necessarily mandatory to always carry or produce it. In Germany, for example, citizens must have identity cards, but they are issued by local authorities, there is no central register, the cards do not carry a unique individual identifier, and the circumstances in which citizens must identify themselves on demand are limited^{xvi}.

[19] In Germany, moreover, a unique individual identifier has been declared unconstitutional by the Federal Constitutional Court^{xvii}. Similarly, the Constitutional Court of Hungary has ruled that “a general and uniform personal identification mark (personal number) for unrestricted use is unconstitutional.” The Court stated that “it should be obvious that consistent with the principle of protecting privacy rights, personal data should be released only for the performance of a “function” which is accurately defined, and whose performance warrants in a constructive manner that the risk related to the release of personal data be taken.”^{xviii}

[20] Many European identity card schemes pre-date computers, or at least the widespread use of powerful computer networks and databases. One therefore sees the potential for modern technology, with its powerful tools for surveillance, backing into legacy systems. These legacy schemes undoubtedly diminished the right to anonymity, but the layering of networked surveillance tools onto long-accepted legacy schemes would present much greater threats to privacy through networked public sector-private sector surveillance. The same could be said of any Canadian national identity card scheme using a universal identifier and carrying an obligation to produce that identifier.

[21] The Quebec Commission, the Ontario Information and Privacy Commissioner and the federal Privacy Commissioner have now all communicated their opposition to the Minister’s proposed national identity card^{xix}. Nor is this the first time commissioners and other public agencies have opposed identity cards proposed by one level of Canadian government or another. In the 1990s, privacy commissioners and ombudsmen consistently criticized various provincial government proposals for identity cards. Privacy commissioners have repeatedly warned that identity cards will erode the privacy of citizens because they are almost invariably used as keys to data-warehouses or linked databases. They have repeatedly urged governments to resist technological imperatives and, if a card is to proceed at all, strictly define and limit the uses of a card.^{xx} As recently as 2001, the government of Quebec scrapped plans for a smart identity card. The Quebec privacy commissioner, human rights commission and Ombudsman were all opposed to the card.

It is not clear what is being proposed

[22] It is not clear, even after his remarks in debate in the House of Commons last week, what the Minister has in mind. He seems to be saying that a new national identity card that would offer uniform, secure and well-authenticated identification of Canadians is needed. Such a card would be similar to the permanent resident card the federal government has introduced.

[23] The Minister may, however, have more in mind. It may be the new card would be associated with a new individual identifier, like the social insurance number (“SIN”). This would, as a technical matter, enable data from disparate databases (public and private) to be retrieved using the card. It would also enable linkages among data in a single or multiple databases.

[24] The privacy implications of these two kinds of national identity cards differ and will be discussed separately below. (I will note here, however, that I am not against the use of biometrics for identification purposes. If implemented properly, biometrics can in fact enhance security and help protect privacy.)

[25] There are several imperatives that cannot be ignored in enhancing the security of identification or in creating a new identity card:

- Identification should not facilitate increased government surveillance
- Identification should not have multiple purposes – it should only be identification
- Identification should not become an internal passport.

The search for more secure identification

[26] The Minister has been quoted as saying that a national identity card with biometric enhancements is desirable. He has hinted at more stringent United States border requirements, and mentioned identity theft, as reasons for such a card. Although enhancing the security of identification offers benefits, an entirely new form of national identification for Canadian citizens is not likely to be cost-effective. A new form of identification would be redundant and is not likely to appreciably improve matters given the costs involved.

[27] The Minister of National Revenue, the Hon. Elinor Caplan, has pointed out, moreover, that there are adequate security measures in place now to ensure a secure border.^{xxi} Even if concerns remained about this, the federal government would do better to spend a fraction of the costs required for a new national identity card on enhancing the security of passports, an existing form of identification. Investment in processes to better ensure that passports are validly issued and to secure issued documents, perhaps using biometrics, are far more likely to be cost-effective.

[28] The same goes for identity theft. The federal government should, instead of spending massive amounts of taxpayer dollars on an entirely new form of identification, invest public funds in improving existing forms of identification issued by the provinces and territories, namely birth certificates and driver's licences. Birth certificates obviously play an important role in passport issuance, so investments in improving processes for issuance of birth certificates would yield a double return.

[29] At least one model exists for such an approach. Significant funds have been committed to the Canada Health Infoway, a not-for-profit corporation with a mandate from the federal government and the provinces and territories to develop inter-operable, pan-Canadian solutions for electronic health records. In a similar vein, the federal government could, in co-operation with the provinces and territories, invest funds in developing common standards and best practices for the issuance of birth certificates and driver's licences. Money could also be invested in developing and implementing, if considered necessary, biometric enhancements to these forms of identification. Money could be directed at creating processes to keep abreast of changes in technology, to ensure that the security of certificates and licences remains ahead of methods of compromising them. A federal, provincial and territorial Council on Identity in Canada is already at work in this area and can be expected to report soon on its work.

[30] By contrast, reliance on a single identity card could actually increase the risk of identity theft or exploitation by terrorists. A national identity card would automatically become a valuable commodity that would be exploited by criminals both within and outside of Canada. The higher the perceived integrity of a card, the greater the risks of its compromise and the greater its value to criminals and illegal immigrants.

[31] It has been said that the Swedish national identification number, for example, is overly trusted, with serious risks to innocent individuals whose identification number has been stolen or where simple errors are made^{xxii}. The United Kingdom Home Office, in its consultation on an "entitlement card" – really, a national identity card – has said it is "highly likely that an entitlement card scheme would become the target of organized criminals who would attempt to produce counterfeit cards."^{xxiii} A similar conclusion was reached by the National Research Council in the United States. In a report the Council noted that identity cards may facilitate identity theft:

While offering better solutions to some problems surrounding identity theft, a nationwide identity system poses its own risks. For example, it is likely that the existence of a single, distinct source of identity would create a single point of failure that could facilitate identity theft. The theft or counterfeiting of an ID would allow an individual to "become" the person described by the card, in very strong terms, especially if the nationwide identity system were to be used for many purposes other than those required by the government. Paradoxically, it could be that a robust nationwide identity system makes identity theft more difficult while at the same time making its consequences more dire. The economic incentive to counterfeit these cards could turn out to be much greater than the economic incentive to counterfeit U.S. currency.^{xxiv}

[32] These concerns, together with the likely massive cost of creating and maintaining a new form of federal identification from scratch, significantly undercut the notion that a new national identity card is desirable. To the contrary, investments in enhancing the

security and integrity of existing forms of identification would be much more productive. The territories and provinces are responsible for registration of births and deaths, and for issuance of related certificates. They are also responsible for driver's licence issuance. The federal government therefore would have to enlist their co-operation in order to create and maintain a new national identity card of any utility. This strongly suggests that any effort to improve forms of identification should take the form of co-operative ventures with the provinces and territories.

A universal identifying number or symbol is not supportable

[33] Identity cards carrying a unique identifier for each individual would unacceptably facilitate state surveillance of Canadians. By "universal identifier" I mean a unique number or other identifier assigned to, and thus representing, a specific individual and no one else. Such identifiers are often a feature of identity card proposals, although it is not clear whether they are contemplated by the Minister's proposal.

[34] One of the gravest problems with universal identifiers is the ease with which the number and nature of their uses will inevitably expand – a well-established phenomenon known as function creep. The uses to which universal identifiers can be applied are easily manipulated and expanded once the technology is operative. Universal identifiers can be characterized as critical elements of what has been called "the continued and voracious expansion of the public and private sector's appetite for more and more refined and integrated personal data at the expense of personal space and individual autonomy."^{xxv} This has been the experience in Sweden with its unique personal identification number^{xxvi}.

[35] To give a Canadian example, if a universal identifier were created, it would permit retrieval of information from databases such as the unacceptably broad and overly intrusive Canada Customs and Revenue Agency ("CCRA") air traveller surveillance database. Governments would have the ability to match personal information across programs and to create a linked or centralized record of an individual's life, including his or her movements and transactions with government or the private sector.

[36] Such a concern is not far-fetched. The ever-expanding number of uses for the SIN is a prime example of such function creep. In its 20th report, the Standing Committee on Public Accounts noted that, over the years, the SIN has become a "gateway to a multitude of federal and provincial programs," despite originally being conceived as a file number for only unemployment insurance, the Canada Pension Plan and the Quebec Pension Plan. The Committee reported that the SIN today is, far from being an entitlement card with limited uses, "a *de facto* universal identifier" for many programs. It reported that no less than 20 federal statutes, regulations and programs now authorize the use of the SIN and that its use has expanded into provincial social programs and the private sector.^{xxvii} Indeed, legislation to sharply constrain public and private sector use of the SIN is long past due, but successive federal governments have ignored long-standing calls to introduce legislation.

[37] Last, as the CCRA air traveller database shows, privacy protection legislation such as the federal *Privacy Act* may not adequately protect against threats to individual privacy and liberty. The *Customs Act* amendments associated with that database

effectively shut out the *Privacy Act* and authorize an unacceptably intrusive and open-ended program of surveillance. Even if legislation is enacted to control uses of a universal identifier, moreover, the effectiveness of such legislation depends on an adequate enforcement regime, including sufficient resources to monitor compliance.

[38] No evidence has been advanced that supports any assertion that a national identity card equipped with a unique identifier is, as s. 1 of the *Charter* requires, demonstrably justified in our free and democratic society. The necessary clear and compelling state interest in such a surveillance tool has not been demonstrated. Nor has it been shown that such an instrument of surveillance would minimally impair our constitutionally-protected privacy rights. A national identity card carrying a unique personal identifier is therefore not supportable and I oppose it.

3.0 CONCLUSION

[39] To paraphrase the late Justice Thurgood Marshall, of the United States Supreme Court, in times of urgency, civil rights and liberties seem too extravagant to endure. We risk losing our rights by acceding to small and almost invariably well-meaning measures whose overall impact only appears with less-than-rosy hindsight. Privacy is not a luxury. It is not, and has never been, an obstacle to good government or a healthy community. It is in fact indispensable to those things. A national identity card that can be used to track us or collate data about us would not make us better citizens. Nor would it make Canada a better place. It would diminish each of us and all of us. I urge the Committee to recommend that the Minister's proposal not proceed further.

February 17, 2003

Victoria, British Columbia

ORIGINAL SIGNED BY

David Loukidelis
Information and Privacy Commissioner
for British Columbia

ACKNOWLEDGEMENT

I am grateful to law student Charles D. Jago for research he did for this submission.

END NOTES

-
- i A. Westin, *Privacy and freedom*, Athenaeum Press, New York, 1967.
- ii John Woulds, former U.K. Deputy Data Protection Commissioner, as quoted in David H. Flaherty, “Defending the Right to Anonymity”, a paper delivered at “Frontiers of Privacy”, Victoria, British Columbia (February 13, 2003).
- iii Dr. Perri 6, “Entitlement cards: benefits, privacy and data protection risks, costs and wider social implications” (paper for the U.K. Information Commissioner) (2003), at p. 52.
- iv A. Westin, above.
- v “Privacy and Computers”, Report of the Task Force Established Jointly by the Department of Communications/Department of Justice (1972) at p. 13 & p. 14.
- vi [1984] 2 S.C.R. 145, *per* Dickson J., at p. 158.
- vii [1988] 2 S.C.R. 417, [1988] S.C.J. No. 82, *per* La Forest J., at para. 15 (S.C.J.).
- viii [1993] 3 S.C.R. 281, *per* Sopinka J., at p. 293.
- ix [1999] 3 S.C.R. 668, [1999] S.C.J. No. 68.
- x At para. 79 (S.C.J.).
- xi At para. 80 (S.C.J.).
- xii At para. 81 (S.C.J.).
- xiii C. Fried, “Privacy” (1967-68), 77 Yale L.J. 475, at pp. 477-78.
- xiv At para. 23 (S.C.J.).
- xv Helen Carter “Used in Europe Since the Last Century” *The Guardian* (4 July, 2002); Justin Thompson “National ID Cards” CBC News Backgrounder (14 November 2002); Commission d’accès à l’information., “Background Paper on Identity Cards” (October 1996)
- xvi A. Dix, Deputy Data Protection Commissioner for Berlin, “Identity Cards in Germany”, paper delivered at “Identity Cards: Putting You in the Picture”, Seminar hosted by the U.K. Data Protection Registrar, (June 21, 1995), at p. 2.
- xvii A. Dix, above, note xvi.
- xviii Constitutional Court Decision on Privacy Rights 91CH0650A Budapest Magyar Kozlony in Hungarian No 30, 13 Apr 91, pp 805-814.
- xix Privacy Commissioner of Canada, Annual Report to Parliament 2001-2002 (January 2003); David Loukidelis, Letter to the Prime Minister on the Subject of the Federal Privacy Commissioner’s Annual Report (29 January 2003); Quebec Access to Information and Privacy Commission, Letter to Joe Fontana M.P., Chairman of the Standing Committee on Citizenship & Immigration, on the Proposed National Identity Card (February 13, 2003); Information & Privacy Commissioner of Ontario, “Submission to the Standing Committee on Citizenship and Immigration on the issue of a proposed national identity card” (February 10, 2003).
- xx Press Release of the Quebec Ombudsman (19 March 1997); Privacy Commissioner of Ontario, Letter from Commissioner Ann Cavoukian to David Tsubouchi, Chair of Management Board of Cabinet, Summarizing the IPC’s Position on Smart Cards (5 April 2001); Office of the B.C. Information and Privacy Commissioner’s Annual Report 1995-1996.
- xxi Bill Currie and Anne Dawson, “Coderre Seeks Public’s Input on National ID Card” *National Post* (7 February 2003).
- xxii A. Bondestam, Director General, Data Inspection Board of Sweden, “Is It A Sin to Use A PIN?”, excerpt from the Proceedings of the XV International Conference of Data Protection & Privacy Commissioners (September 1993), at p. 57.
- xxiii Home Office, “Consultation Paper: Entitlement Cards and Identity Fraud” (October 2002)
- xxiv Stephen T. Kent and Lynette I. Millet, Eds., “It’s Not that Easy: Questions About Nationwide Identity Systems”, Committee on Authentication Technologies and Their Privacy Implications, National Research Council (2002).
- xxv David H. Flaherty, *Protecting Privacy in Surveillance Societies* (University of North Carolina Press, 1989) at p. 403.
- xxvi A. Bondestam, above, note xxii.
- xxvii Twentieth Report of the Parliamentary Standing Committee on Public Accounts (House of Commons, Ottawa, 1999).