PUBLIC INTEREST ADVOCACY CENTRE
LE CENTRE POUR LA DEFENSE DE L'INTERET PUBLIC
ONE Nicholas Street, Suite 1204, Ottawa, Ontario, Canada K1N 7B7
Tel: (613) 562-4002. Fax: (613) 562-0007. e-mail: piac@piac.ca . http://www.piac.ca

Submission to the House of Commons Standing Committee on Citizenship and Immigration

"Identity Theft as a Justification for a National Identity Card"
Public Interest Advocacy Centre

November 4, 2003

The Public Interest Advocacy Centre (PIAC) is a national, non-profit organization which has been representing the interests of ordinary consumers in matters to do with financial institutions and services, public utility regulation (telecommunications, energy, transportation), broadcasting, Internet access, consumer privacy, and consumer protection generally, since its formation in 1976. PIAC is run by a distinguished Board of Directors from across Canada, and has organizational members who themselves represent millions of Canadians. PIAC has developed a strong reputation nationally for its effective consumer advocacy in these areas.

These submissions related to the narrow issue of identity theft in the debate over a National Identity card. For the record, PIAC opposes such a card as unnecessary, costly and a violation of civil liberties in Canada. PIAC leaves the submissions regarding the larger issue of the National Identity card to the numerous other groups and individuals who oppose the concept of such a card.

Executive Summary

It has been suggested that a national identity card would help to reduce the incidence of ID theft in Canada. There are many problems with such a conclusion. Such a "universal identifier" would invariably face immense pressure towards function creep – it could become a "super-SIN". Once in the hands of thieves, this information will aid, not impede, identity theft. There is a strong likelihood that business will not alter credit-granting systems to accommodate it. Yet, even were business and government to do so, their information practices would put National ID card data at risk – possibly increasing the prospect of identity theft. Consumer credit data will continue to be traded, this time with the added "gold" of National ID card information. A National ID card will not bring necessary legal reform, or additional funding to law enforcement agencies. Police will continue to be ineffective in controlling identity theft without increased resources and legal powers. Canadians can also not count on their privacy laws to protect them from identity theft. Finally, biometrics is a highly invasive technology that will not guarantee document integrity. Perversely, excessive trust in the

technology could aid ID thieves.

There are instead many practical measures that can be taken now to combat identity theft. None of these requires the introduction of a National ID card.

In conclusion, the case has not persuasively made that a National ID Card would necessarily limit identity theft in a manner that represents an acceptable trade-off between privacy and security, or indeed in any appreciable way at all.

Citizenship and Immigration Minister Denis Coderre has recently introduced the concept of the National ID card into the public debate. Minister Coderre has taken a more or less positive stance towards the need for such a card. Minister Coderre has also linked the issue of biometrics to the debate over the National ID card. Finally, Minister Coderre has, to a large extent, justified the need for a national ID card, with biometrics, due to the problem of identity theft.[1]

The only difficulty with this logic is that it is flawed. Identity theft will not be seriously curtailed by the introduction of a National ID card. Biometrics may barely dent it and indeed has the potential to make some cases of identity theft far worse. Identity theft is a security state's straw man for introducing invasive measures designed to reduce personal privacy.

Scope and Nature of Identity Theft in Canada

PIAC has recently completed an extensive report on identity theft in Canada for Industry Canada.[2] The report concludes that there are eight main causes of identity theft in Canada:

- pre-approved credit offers and credit card "cheques";
- easy credit;
- electronic access to personal information;
- sloppy government and business information practices;
- lack of consumer control of their credit bureau files;
- abuse of Social Insurance Numbers, drivers' licence numbers, ("function creep");
- weak ID theft laws and uncoordinated law enforcement;
- inadequate protection by privacy laws.

On reviewing this list it is enlightening to note how few of the above points would be

[1] See the remarks of Minister Denis Coderre, Minister of Citizenship and Immigration, at the forum: "Biometrics: Implications and Applications", Ottawa, October 8, 2003, (http://www.cic.gc.ca/english/press/speech/bio-forum.html) and similar remarks entitled: "Document Integrity And Biometrics: Exploring The Options For Our Future" at the Kiwanis Club, Ottawa, Ontario, September 19, 2003 (http://www.cic.gc.ca/english/press/speech/biometrics.html).

[2] The complete report is available on PIAC's website at: http://www.piac.ca/ID_theft.htm. (Full report in English only, sommaire exécutif disponible en français au: http://www.piac.ca/volID/somm-ex.pdf).

directly affected by the introduction of a National ID card.

Easy and Unsolicited Credit

Easily obtained credit and unsolicited credit from financial institutions and other businesses is a business model that is well ingrained in our consumer culture. Even assuming the new National ID card would be mandatory, would companion financial services legislation be passed (at both the federal level and provincial levels) which would *require* all lenders to physically verify a potential debtor's identity against the National ID card for all credit extensions or offers? Such a duty would be highly disruptive to modern consumer credit transactions.[3] It would all but eliminate pre-approved credit offers (which might actually prove beneficial). Were the National ID card voluntary, or if there were no card verification requirement to obtain credit, there would always be lenders willing to run a higher risk (for a greater return) and lend without seeing the card. Since an ID thief only needs credit for a short period during which the victim is unaware, even one such high-risk lender will provide a window out which ID thieves can abscond with cash or credit.

In PIAC's report, we instead suggest tackling this cause of ID theft by tightening up present notice requirements to debtors: forbidding unsolicited credit offers and requiring creditors to take simple steps to avoid issuing credit in ID theft-prone manners. The first simple step which creditors can take is address verification. Incredibly, lenders routinely skip this step. California law sensibly requires it. Second, lenders can use tested and effective authentication measures. Simple physical identity checks (e.g., requirement to attend in person, hand signature on credit card) are most effective. Careful merchants, for example, always check the consumer's signature on receipts with the signature on the credit card.

The next step, where a merchant or creditor is suspicious, is to demand to see additional information (that is, photo ID). Presumably, the National ID card would become the default accepted photo ID. Again, however, the question remains: should this verification step be mandatory? What are the inconveniences to commerce to try to implement it for all transactions? What is the likelihood that some businesses or lenders will not comply or if the step is voluntary, will have a policy of not checking the National ID card?

It could be argued that such a step would provide a routine double-check. However, what if this were legislated and all lenders and businesses actually did it? Would there not be an incredible pressure on financial institutions and businesses to keep a record of the ID check? Would that not mean that suddenly all financial institutions and other

[3] The Interim Privacy Commissioner's concerns include the following comment: "It is also said that an identification card would help combat identity theft. Again, how that would work is not at all clear. A comprehensive infrastructure of electronic card readers and trained personnel would be very complex technically, and very expensive to deploy. And the system would still rest at some point on foundation documents like birth certificates and drivers licences, so an identity thief who surreptitiously obtained foundation documents could still apply for a card in someone else's name." See "News Release: Interim Privacy Commissioner questions merit of a national ID card", September 18, 2003 (http://www.privcom.gc.ca/media/nr-c/2003/02_05_b_030918_e.asp).

businesses amassed huge amounts of National ID card information? Would that not be an even larger security risk and also be a potential privacy nightmare – where businesses could immediately create consumer profiles with this new unique identifier, the National ID card?

PIAC has argued strenuously in its Report that such verification of individual identity should not involve the *collection* of additional personal information; rather, simple checking of the information should be sufficient.[4] The more personal information recorded, the more susceptible it is to abuse. Yet businesses, for risk management and liability purposes, will routinely gather and keep this information, even if not required to do so.

In addition, much commerce now is electronic, meaning limited opportunity for a National ID card to provide authentication of identity. New authentication services, such as digital signatures in the online context, are now emerging, but are not yet widely used. PIAC supports the use of digital signatures but not the linking of electronic signatures to a portable National ID card, which can be double-swiped or stolen.

Electronic Access to Personal Information

A major factor in the phenomenon of ID theft is nearly ubiquitous access to personal information due to electronic storage and access technology, and interconnected networks. Remote access to databases of personal information, whether in the public domain or revealed through computer hacking, facilitates the stealthy work of ID thieves. No National ID card will remove or alter this electronic architecture. Indeed, the National ID information will now be added to the data cloud surrounding us. PIAC, based on past experience of function creep of key government identifiers and private credit information such as credit card numbers, finds it extremely unlikely that effective legislation could be enacted to forbid electronic storage or linking of National ID card information.

Sloppy Government And Business Information Practices

Mass data losses are now becoming weekly news in Canada. These "data spills" of personal information typically occur when unsecured computers with unencrypted personal information are stolen from businesses or government. However, unauthorized access from outside the organization (hacking) or from within also augment the problem. The aggregation of personal data, often cross-referenced to financial information or key identifiers like SINs, create a real threat of sudden, massive identity theft.

[4] Note the U.S. *Patriot Act*, under regulations made pursuant to s. 326, requires banks and other financial intermediaries to set up a "Customer Identification Program". They must ask to see personal identification and ask for date of birth, address and "taxpayer ID number" (usually a SSN). There is no requirement, however, that banks or others keep copies of such documentation. However, banks are permitted to keep copies of identification, and although the American Bankers Association recommends against it, "the man who wrote the rule said that it would be "prudent" to do so": *Privacy Journal*, "ID Requirements in Banks", June 2003, Vol. 29, No. 8, p. 5.

It is difficult to imagine how a National ID card could curtail the damage from such a data spill. In all likelihood, the unique identifier on the National ID card would be linked to the information in databases that would remain vulnerable to loss.

PIAC in its report urged both businesses and government to take security measures commensurate with the sensitivity of their information holdings. PIAC has also called for immediate, mandatory disclosure of security breaches to individuals. Neither of these strategies requires a National ID card.

Consumer Control Of Their Credit Bureau Files

Consumers have notoriously little control over their financial profile as presented to the outside world in their credit report. Credit information is regularly communicated to and from credit bureaus by credit grantors without the knowledge of the individual subject. Such access facilitates identity theft by permitting thieves to open credit accounts with ease once personal information about the victim is known.

Credit bureaus stand in a unique position in the battle against ID theft: consumers regularly discover ID theft after being denied credit due to a deteriorating credit rating. Consumers also must immediately deal with credit bureaus to halt further fraud. Credit bureaus stand at the cross-roads of ID theft.

Yet there are many measures which could counter much ID theft which are not regularly undertaken by credit bureaus: credit “freezes” of a customer’s credit file; notification of unusual patterns of credit applications; notification of significant inaccuracies in a credit file. At present the consumer carries the burden of obtaining and reviewing his or her credit report to check for fraud.

PIAC has called for credit bureaus to do more on behalf of consumers to combat identity theft. Some credit bureaus have claimed that a national unique identifier (which could be a National Identity card) could reduce ID theft by permitting the credit bureaus to cross reference name and address information. However, even were consumers to feel comfortable with the credit bureau possessing an even more powerful piece of information such as a National ID card, this would not reduce the core of ID theft perpetrated through the credit system. It would not halt further credit being granted once an ID thief persuaded a credit grantor to grant further credit – only a credit freeze or notification of the transaction to the consumer could do that.

Social Insurance Numbers, etc. and Function Creep

In 1998, the Auditor General of Canada stated that the SIN had become a “de facto national identifier for income-related transactions, contrary to the government’s intent”. A similar fate surely awaits the National ID card.

Function creep is the term that has been given to the use of a unique identifier, often government-issued, for purposes other than those for which it was issued. Canada’s present law regarding the Social Insurance Number forbids a business or government

from requiring an individual to divulge his or her SIN (except for tax or employment purposes). However, the law permits others to ask for the SIN. Most individuals comply and provide their SIN for various authentication purposes in the course of routine financial transactions. Most of the time, this is simply to speed the process or to obtain better service. Indeed, it appears some customer service is simply unavailable unless the individual is willing to divulge a SIN or driver's licence number.

Should a similar permissive legal regime be allowed to govern the use of a National ID card, it will be demanded routinely by businesses and government. It will very likely be regarded as an ideal unique identifier – without the stigma and sensitivity of a SIN. This would be a mistake, however. A unique identifier in the hands of an identity thief is a powerful thing. Unless businesses were forbidden to rely upon the National ID card to identify individuals and qualify them for services, the National ID card information, once stolen by an identity thief, could immediately be used to enter into any number of electronic or other non-in-person transactions. Unless businesses were forbidden from asking for the National ID card information, it will enter the stream of commerce and, like all other personal information, be vulnerable to theft or disclosure through negligence or inadvertence.

Weak ID Theft Laws And Uncoordinated Law Enforcement

Presently there is no law in Canada against simple possession of identity documents relating to another person. This leads to a huge gap in the enforcement efforts of police combating ID theft. However, unless a law forbidding such possession is passed to complement the introduction of a National ID card, there will continue to be cases of ID thieves caught with evidence of using others' identity documents who cannot be prosecuted for National ID card fraud. Simple possession of another's passport is an offence: this is required for any National ID card as well, given the likely importance it would assume within Canada.

However, the problem with ID theft goes far beyond updating the law. Police are frustrated by the intense investigation required to track an ID thief. Often such crimes are international in scope, requiring high levels of interagency cooperation that may not be justified by the "small" amounts jeopardized in each identity theft.

Enforcement could be improved by greater resources for police; better coordination amongst police forces and government; the creation of simple ID theft reporting systems (the RCMP "RECOL" website is a welcome recent example); and deterrent sentencing for identity fraud-related offences. These enforcement measures do not require another piece of identification (which can itself be forged) in order to be implemented and reduce identity theft.

Inadequate Protection By Privacy Laws

Canada's personal privacy laws, provincially and federally (especially the *Personal Information Protection and Electronic Documents Act* (PIPEDA)) require safe information practices by businesses and government. However, these acts typically do

not provide real economic sanctions for non-compliance. As a result, it may be that organizations will continue to resist steps to make their personal information handling more secure.

PIPEDA is also unfortunately weak in respect of demands by companies for personal information that is not strictly necessary for the requested service or transaction. Consumers still receive better service in exchange for this superfluous data collection.

As already noted, businesses will face a tremendous pressure to collect National ID card information, it being a unique identifier. This collection will likely become a routine part of consumer transactions, risking data spills, internal fraud, linking to other consumer data (profiling) and unsolicited target marketing.

Security Mechanisms Associated with a National ID Card

Whatever the form of the National ID card, it will more likely than not carry electronic information. Once a card carries such information, there will of necessity be an authentication method associated with the card to show the bearer is the person represented on the card.

Passwords and PINs

The proliferation of password and PIN authentication ignores the inherent limits on an individual's ability to remember several different passwords and PINs associated with different services, without recording them in a manner that would be helpful to ID thieves. Realistically, most individuals will have to use the same password for multiple purposes, or record the different passwords with their associated uses, in order to remember them. Reliance on these methods of authentication, while helpful, is therefore of limited assistance in guaranteeing the security of any National ID card.

Biometrics

Biometrics, which authenticate identity based on the unique physical features of the individual (e.g., fingerprint, retina scan), are also being considered for many applications in which user identity needs to be authenticated. There are, however, serious privacy concerns with such technologies.[5] As for security, there is nothing secure about biometric ID cards unless the papers required to obtain them are equally secure. Reliance on biometrics requires absolute certainty that the right biometric data is associated with the identification document or database. In fact, biometrics could even exacerbate the problem of ID theft, since fraudulently obtained cards would be even more difficult to identify and retract, and victims would likely have even more difficulty obtaining getting redress.[6] A UK expert noted the possibility of "more reliable fake IDs,

[5] See Statement of George Radwanski, Privacy Commissioner of Canada, to the Standing Committee on Citizenship and Immigration (http://www.privcom.gc.ca/speech/2003/02_05_a_030318_e.asp).
[6] Simon Davies. "The Id Card Is The Fraudster's Friend," The Sunday Telegraph, July 7, 2002: http://www.telegraph.co.uk/opinion/main.jhtml?xml=%2Fopinion%2F2002%2F07%2F07%2Fdo0703.xml.

because once someone is able to get a card with false information, there will probably be no means by which that false information can be queried".[7] Finally, while Canadians may tolerate biometrics as an eventual part of passport issuance due to foreign requirements,[8] everyday reliance on such systems in Canada is rightly judged as far too invasive a technology.[9]

[7] Mike Davis, quoted in Sarah Arnott, "Doubts surround national ID cards", vnunet.com(10 July 2003)
[8] See comments of former Privacy Commissioner of Canada Bruce Phillips, delivered to Conference "Frontiers of Privacy and Security", Victoria, B.C., February 14, 2003.
[9] We repeat our comments that credit-granting processes will likely be resistant to introducing a full identity check for every transaction, no matter how secure the technology.