Appearance Before the Standing Committee on Citizenship and Immigration

Re: National Identity Card

Wednesday, February 19, 2003
Delta Pinnacle Hotel
1128 West Hastings Street
Vancouver

Richard S. Rosenberg, Vice-President
Electronic Frontier Canada

and

Professor
Department of Computer Science
University of British Columbia
Vancouver, BC V6T 1Z4
e-mail address: rosen@cs.ubc.ca

EXECUTIVE SUMMARY

The organization that I represent today, Electronic Frontier Canada, has been in existence almost nine years. On its Web page, the following statement of purpose appears: [1]

> "Electronic Frontier Canada (EFC) was founded to ensure that the principles embodied in the Canadian Charter of Rights and Freedoms remain protected as new computing, communications, and information technologies are introduced into Canadian society."

It is inevitable that in the aftermath of crises such as September 11, concern for the security of the nation will (seem to) overweigh individual privacy rights. This government has introduced a number of bills that raise serious privacy issues and in the context of such legislation as well as the Canada Customs and Revenue Agency (CCRA) database on foreign travel activities and the Lawful Access Discussion Paper, the current proposal for an ID card strikes many that the government is clearly over-reacting.

Simply put, Canadians neither need nor desire a National Identity Card. It is being advertised as a solution to identity theft and as means to improve the chances of identifying and apprehending terrorists. In addition, the convenience of a single piece of identification for facilitating the multitude of transactions that Canadians must deal with is also being promoted as an advantage. Finally, warnings are being issued that without an ID card , Canadians will have difficulty entering the United States

Five reasons against a National ID card have been proposed by the American Civil Liberties Union and these apply to Canada as well:

- Reason #1: A national ID card system would not solve the problem that is inspiring it.
- Reason #2: An ID card system will lead to a slippery slope of surveillance and monitoring of citizens.
- Reason #3: A national ID card system would require creation of a database of all Americans. [Read Canadians for present purposes]
- Reason #4: ID cards would function as "internal passports" that monitor citizens' movements.
- Reason #5: ID cards would foster new forms of discrimination and harassment.

Current examples around the world, as well as historical ones, reveal the detrimental and occasionally deadly effects of National ID cards, or "papers." The crucial issue of a self-contained card or a card based on a centralized database must be carefully evaluated.

The call for a discussion and debate on National ID cards is premature. Parliament has not done its homework. This submission, and many others I am sure, have raised a host of serious questions about the need, purpose, and dangers associated with an ID card. As Dr. Brands' contributions demonstrate much turns on technical issues associated with the implementation of an ID card system. The use of the word system cannot be overemphasized.

If there remains a serious interest in National ID cards after this series of hearings, then the House must undertake a serious study of associated technical, political, and social issues. However, challenges mounted here, including the results of studies in other countries as well as historical evidence, should provide convincing reasons to terminate further consideration. Indeed, the U.S., the primary target of international terrorism on September 11, has decided, yet again, not to proceed with the introduction of a National ID card system.

BRIEF ON BEHALF OF ELECTRONIC FRONTIER CANADA ON A NATIONAL IDENTITY CARD

I. INTRODUCTION

The organization that I represent today, Electronic Frontier Canada, has been in existence almost nine years. On its Web page, the following statement of purpose appears: [1]

> "Electronic Frontier Canada (EFC) was founded to ensure that the principles embodied in the Canadian Charter of Rights and Freedoms remain protected as new computing, communications, and information technologies are introduced into Canadian society."

EFC has often taken a position against government intervention in Internet activities. Probably most significant, is the continued resistance it has offered against attempts by governments to regulate content on the Internet. In fact, we are probably best known for our unwavering support of freedom of expression. Almost exactly four years ago I appeared before the Standing Parliamentary Committee on Industry to present EFC's views on Bill C-54 (later Bill C-6), Personal Information Protection and Electronic Documents Act. We supported the role of government in protecting the privacy rights of Canadians in the marketplace. However, on this occasion we urge government not to intrude on those privacy rights by introducing a National Identity Card (ID card).

I am sure that this Committee has heard many arguments on this issue; nevertheless, it is my intention to review the recent history of attempts to introduce ID cards in a number of countries, and the associated arguments challenging these attempts. It is inevitable that in the aftermath of crises such as September 11 concern for the security of the nation will (seem to) overweigh individual privacy rights. This government has introduced a number of bills that raise serious privacy issues and in the context of such legislation as well as the Canada Customs and Revenue Agency (CCRA) database on foreign travel activities and the Lawful Access Discussion Paper, the current proposal for an ID card strikes many that the government is clearly over-reacting.

Simply put, Canadians neither need nor desire a National Identity Card. It is being advertised as a solution to identity theft and as means to ensure, with as much certainty as possible, that terrorists can be identified and apprehended. In addition, the convenience of a single piece of identification

for facilitating the multitude of transactions that Canadians must deal with is also being promoted as an advantage. Finally, warnings are being issued that without an ID card , Canadians will have difficulty entering the United States. It should be noted that in spite of efforts shortly after September 11 to introduce a National ID card in the U.S., no such system has been implemented and none is on the horizon. Furthermore, many conservatives and liberals voiced public opposition to this idea. For example, the conservative columnist for *The New York Times*, William Safire expressed his opposition as follows: [2]

> "However, the fear of terror attack is being exploited by law enforcement sweeping for suspects as well as by commercial marketers seeking prospects. It has emboldened the zealots of intrusion to press for the holy grail of snoopery - a mandatory national ID. . . The plastic card would not merely show a photograph, signature and address, as driver's licenses do. That's only the beginning. In time, and with exquisite refinements, the card would contain not only a fingerprint, description of DNA and the details of your eye's iris, but a host of other information about you. . . With a national ID system, however, it can all be centered in a single dossier, even pressed on a single card - with a copy of that card in a national databank, supposedly confidential but available to any imaginative hacker."

Why then should Canadians be required to carry an ID card? In what follows, I will attempt to survey, necessarily briefly, a variety of positions on the introduction of National ID cards, concluding that only under very special technical conditions can they be effective for certain purposes. However, it must be emphasized that in principle ID cards can be dangerous devices inimical to the basic tenets of a democratic society. They contribute to the loss of anonymity because they will encourage law enforcement officials to demand their presentation any where and anytime. It is also inevitable that their purposes and applications will expand, so-called "function creep," not because it is necessary but because it is possible. Witness the history of the Social Insurance Number (SIN) in Canada. The availability of an apparent unique identifier resulted in a host of mundane uses beyond any initial expectations and Parliament seemed to be unable or unwilling to curtail such extraneous applications.

Thus, we will consider the comments and advice of privacy advocates, online civil liberties groups, privacy commissioners, representatives of technical and professional societies, academics, and politically motivated organizations. Many of these will no doubt make their own contributions to your deliberations but seeing their views in one document should combine their individual messages into a coherent, forceful, and persuasive argument.

II. SETTING THE CONTEXT: MEMBERS OF PARLIAMENT SPEAK

On November 22, 2002, Immigration Minister Denis Coderre, made the following remarks: [3]

> "Let's have a national debate for policy-making purposes. Do Canadian people feel that we should have a national ID card?" said Coderre. Coderre said the card would be based on the Maple Leaf card now issued to landed immigrants in Canada. The Maple Leaf cards contain biometric information such as fingerprints. He said the cards would make it easier for Canadians to travel, especially to the U.S.

And so we are engaged in this debate, one that some countries have experienced and others will no doubt soon have. This Committee subsequently issued a statement inviting comments on the possible adoption of a National Identity Card. Among the points identified for discussion are the following, some of which raise very difficult questions: [4] (Note that the numbering has been added in order to refer to the points more easily)

(a) What should be the guiding principles for a national strategy on identity documents?
(b) Which level(s) of government should be responsible?
(c) Do we need to create a new national identity card, or can the security features of existing "foundation" documents be strengthened?
(d) What has been the experience of other countries with national identity cards?
(e) Should everyone in Canada be required to carry a secure identity document at all times? Or should the identity document be *voluntary* for some (e.g. Canadian citizens and permanent residents) and *mandatory* for others (e.g. refugee claimants, foreign students, or other temporary residents)?
(f) What information should be imbedded in the cards, who should be able to access that information, should the information be stored centrally, and what safeguards would be required to prevent misuse?
(g) What technologies are available for enhancing document security and what issues are raised by the use of particular technologies, such as biometrics? (Biometric identifiers include fingerprints, iris scans and facial scans.)

Brief answers follow with the remainder of this document offering supporting material.

(a) Because the implementation of an ID card is largely rejected, no "guiding principles" will be offered.
(b) Again, in the context of this document this question need not be answered.
(c) We do not need a new ID card and existing documents can be improved, if a clear need can be demonstrated.
(d) See the next section for some interesting items.

(e) It is not necessary for everyone in Canada to carry "a secure identity document at all times."
(f) Given the position expressed in this document, this question will not be addressed but some comments about security will be included.
(g) In the course of arguing against the ID card, some of the technologies mentioned here will be discussed.

More recently, Minister Coderre has urged his colleagues on the Commons Committee "to consider whether the card's personal information should be compiled in a government database." [5] Such a database could presumably have considerably more information available about an individual than a card and could be accessible in part via the card. Such a powerful system just raises the stakes in the assault on individual privacy because arbitrarily large amounts of diverse information can be accessed about any individual. Do we want to take such a drastic step for such a minimal return?

III. EXPERIENCES OF OTHER COUNTRIES

The intention in this section is to examine a few countries which either have introduced, are planning to introduce, or have decided not to introduce a National ID card. It is to be hoped that lessons learned in these cases are relevant to the Canadian situation. In Belgium, an 1856 law required that all inhabitants be registered with local authorities. "All cities, towns and villages had to open a register and keep track of people's addresses and the composition of their families." [6] These are the words of Rudi Veerstraeten, Counselor and Consul, Embassy of Belgium in a statement made before the U.S. House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Oversight Hearings on National Identification Cards ("Does America Need a National Identifier?"), November 16, 2001. Mr. Veestraeten goes on to describe the Belgian identity card [1985], which contains the following data on the front side:

- Name and first name
- Nationality
- Date and place of birth
- Mention male/female
- Signature of the bearer
- Address

- Card number
- Date of issuance
- Valid until (date)

The card bears a sticker on the back side. On this sticker are mentioned some additional data, if the bearer wishes to do so:

- Card number (for security purposes)
- Marital status and name of spouse
- Number of the National Register

This extra information can only be mentioned upon explicit approval by the bearer of the card.

Finally, for the present purposes, the main issue of concern is the following:

> Most Belgians do not oppose these mentions, but they have a right to do so. The card is automatically issued to every Belgian citizen over 12 years of age; every Belgian over 15 years of age has the obligation to carry it at all times, while walking, driving a car or riding a bus.
>
> **A police officer can ask to see the identity card of any person found in a public space. Although such request on behalf of a law enforcement agency does not need to be motivated, it mostly occurs only when there is a particular reason for a police officer to do so (suspicious behavior, events, security reasons)**. [emphasis added]

Do Canadians want to move towards a society in which police officers can ask to see identification without necessarily having to justify their request. It seems that Europeans are more willing to move in this direction. Another example is the Netherlands. Earlier this year, a Bill was submitted in the Netherlands, with the following requirement: [7]:

> In future police will be authorized to require anyone in the Netherlands older than 12 to show proof of his or her identity. Failure to do so can result in a prison sentence of up to two months or a fine of up to 2,250 Euro. Police will be given powers to request proof of identity for the purpose of carrying out all their regular tasks, specifically the investigation of criminal offences, maintenance of public order, and providing assistance. Those responsible for carrying out administrative supervision will also be given the same powers, in order to improve law enforcement.

Of course, being required to show identification means that it must be carried at all times. One of the main concerns with respect to the adoption of National ID cards is the loss of anonymity, a basic component in the web of privacy rights. The right to be unidentified, to be one of the crowd,

to be undistinguished as one walks among others in urban areas, and elsewhere, is a much valued, if rarely contemplated, state of being.

In 1987, the Australian government attempted to introduce a National ID card, which failed as a result of a major opposition campaign. Simon Davies of Privacy International described this campaign in some detail. [8] Two kinds of arguments were used, the first of which is characterized as intangible, i.e., difficult to refute and somewhat hysterical, namely,

- A fear that the card will be used against the individual
- A fear that the card will increase the power of authorities
- A feeling that the card is in some way a hostile symbol
- A concern that a national ID card is the mechanism foretold in Revelations (the Mark of the Beast).
- A fear that people will be reduced to numbers - a dehumanising effect.
- A rejection of the card on the principle of individual rights
- A sense that the government is passing the buck for bad management to the citizen

The second type of concerns are characterized as "tangible concerns that tend to create a more powerful long term campaign focus." Among these are the following:

- Any card system needs rules. How many laws must be passed to force the citizenry to use and respect the card?
- A card or numbering system may lead to a situation where government policy becomes "technology driven" and will occur increasingly through the will of bureaucrats, rather than through law or public process
- Practical and administrative problems that will arise from lost, stolen or damaged cards (estimated at up to several hundred thousand per year)
- Will the system create enough savings to justify its construction? If the system fails, can it be disassembled?
- To what extent will the system entrench fraud and criminality? What new opportunities for criminality will the system create?
- What are the broader questions of social change that relate to this proposal ? How will it affect my children?

The Australia Card "was to be carried by all Australian citizens and permanent residents (separately marked cards would be issued to temporary residents and visitors). The would contain a photograph, name, unique number, signature and period of validity, and would have been used to establish the right to employment. It would be necessary for the operation of a bank account, provision of government benefits, provision of health benefits, and for immigration and passport

control purposes." It should be noted that prior to the launch of the anti-Card campaign about 70% of Australians supported its introduction. Let me conclude this very brief review of the Australian anti-card campaign with two early critiques: [8]

> One of the fundamental contrasts between free democratic societies and totalitarian systems is that the totalitarian government relies on secrecy for the regime but high surveillance and disclosure for all other groups, whereas in the civic culture of liberal democracy, the position is approximately the reverse. [Professor Geoffrey de Q Walker, now dean of law at Queensland University]
>
> Is it realistic to believe that the production of identity cards by children to adults in authority to prove their age will be "purely voluntary"? The next generation of children may be accustomed to always carrying their Cards, to get a bus or movie concession, or to prove they are old enough to drink, so that in adult life they will regard production of an ID card as a routine aspect of most transactions. [Australian data protection expert Graham Greenleaf, one of the pioneers of the anti ID card push]

Finally, Privacy International gathered comments from people around the world expressing their experiences with National ID cards. Consider the following selections: [9]

> **Greece**: In my country the Cards are compulsory. If police for example stop you and ask for identification you must present them the ID or you are taken to the police department for identification research.
>
> **Brazil**: They are compulsory, you're in big trouble with the police if they request it and you don't have one or left home without it. The police can ask for my identity card with or without a valid motive, it's an intimidation act that happens in Brazil very, very often. The problem is not confined to the police. Everybody asks for your id when you are for example shopping, and this is after you have shown your cheque guarantee card. We also have other similar cards. Nobody trusts anybody basically.
>
> **Singapore**: [M]any people in his country were aware that the card was used for purposes of tracking their movements, but that most did not see any harm in this. If that question is put to Singaporeans, they are unlikely to say that the cards have been abused. However, I find certain aspects of the NRIC (ID card) system disconcerting. When I finish military service (part of National service), I was placed in the army reserve. When I was recalled for reserve service, I found that the army actually knew about my occupation and salary! I interpreted this as an intrusion into my privacy. It might not be obvious but the NRIC system has made it possible to link fragmented information together.
>
> **Korean**: One professor reported that the national card was used primarily as a means of tracking peoples activities and movements. If you lose this card, you have to report and make

another one within a certain period. Since it shows your current address, if you change your address then you must report that and make a correction of the new address. If you go to a military service or to a prison, then the government takes away this identity card. You get the card back when you get out. You are supposed to carry this card everywhere you go, since the purpose is to check out the activity of people. There are fines and some jail terms if you do not comply. If you board a ship or an airplane, then you must show this card to make a record. You need to show this card when you vote

Portugal: One man studying in the United States reported an obsession with identity in his country. I keep losing my ID. card, and people keep asking for it. It seems like it's needed for just about everything I want to do, and I should really carry it around my neck or have it tattooed on my palm. The information on it is needed for everything. Many buildings, perhaps most, will have a clerk sitting at a "reception desk" who will ask you for your id. They will keep it and give it back to you when you leave.

IV. CONCERNS OF THE LEFT AND THE RIGHT

The American Civil Liberties Union (ACLU) is the largest association in the U.S. dedicated to the defense of constitutional rights. As such it is not surprising that privacy is high on its agenda and that the introduction of a National ID card is an anathema. Shortly after September 11, many proposals emerged from high profile technology figures such as Scott McNealy, CEO of Sun Microsystems and Larry Ellison, CEO and founder of Oracle Corporation, as well as from government officials at state and federal levels. The conversion of state drivers' licenses to federal ID cards received considerable attention but in the end the enthusiasm waned and once again nothing happened. However, as the debate raged, The ACLU published an advocacy paper, "National ID Cards: 5 Reasons Why They Should Be Rejected." [9] and these are given, in brief, as follows:

- **Reason #1: A national ID card system would not solve the problem that is inspiring it.** A national ID card system will not prevent terrorism. It would not have thwarted the September 11 hijackers, for example, many of whom reportedly had identification documents on them, and were in the country legally.
- **Reason #2: An ID card system will lead to a slippery slope of surveillance and monitoring of citizens.** A national ID card system would not protect us from terrorism, but it would create a system of internal passports that would significantly diminish the freedom and privacy of law-abiding citizens. Once put in place, it is exceedingly unlikely that such a system would be restricted to its original purpose.

- **Reason #3: A national ID card system would require creation of a database of all Americans**. What happens when an ID card is stolen? What proof is used to decide who gets a card? A national ID would require a governmental database of every person in the U.S. containing continually updated identifying information.
- **Reason #4: ID cards would function as "internal passports" that monitor citizens' movements**. Americans have long had a visceral aversion to building a society in which the authorities could act like totalitarian sentries and demand "your papers please!" And that everyday intrusiveness would be conjoined with the full power of modern computer and database technology.
- **Reason #5: ID cards would foster new forms of discrimination and harassment**. Rather than eliminating discrimination, as some have claimed, a national identity card would foster new forms of discrimination and harassment of anyone perceived as looking or sounding "foreign."

In contrast to the "liberal" ACLU, the Cato Institute is definitely conservative; nevertheless, it shares the ACLU's deep antipathy towards ID cards. Shortly after September 11, the following appeared in the Institute's TechKnowledge Newsletter [10]

> "What *is* new about the various national ID card proposals is that they have become more technologically sophisticated. The prospect of massive computer databases or registries, software data collection systems, digital fingerprinting, handprint scans, facial recognition technologies, voice authentication devices, electronic retinal scans, and other "biometric" surveillance technologies have suddenly become realistic options for government identification purposes. If Americans are concerned about the recent proliferation of traffic surveillance cameras on roadways and sidewalks, then they ain't seen nothin' yet. But while the technologies may have changed, the fundamental problems with national ID cards have not. The most serious problem with national ID mandates remains the troubling ramifications for civil liberties. As former California Rep. Tom Campbell, currently a Stanford University law professor, has recently argued, "If you have an ID card, it is solely for the purpose of allowing the government to compel you to produce it. This would essentially give the government the power to demand that we show our papers. It is a very dangerous thing."
>
> While proponents of national ID cards will contend that such concerns are overblown, there is no denying that a national ID card could become the equivalent of a domestic passport that citizens are required to produce for the most routine daily tasks. . . The other serious problem with national ID cards is more practical: They probably won't work. For example, who will be issuing these cards? If everyone is required to have one, then that means there will be a lot of bureaucrats responsible for collecting and filing our personal information. Beyond logistical questions about how that process will work and how much it will cost, it raises concerns about potential fraud and abuse."

The U.S. organization most involved with privacy rights is the Electronic Privacy Information Center (EPIC). Concerned about attempts to convert drivers' licenses into *de facto* National ID

cards, EPIC joined with other organizations, both liberal and conservative, in sending a letter to President Bush in February 2002. Among their concerns were the following: [11]

- **A national ID would not prevent terrorism**. An identity card is only as good as the information that establishes identity in the first place. Terrorists and criminals will continue to be able to obtain -- by legal and illegal means -- the documents needed to get a government ID, such as birth certificates and social security numbers
- **A national ID would depend on a massive bureaucracy that would limit our basic freedoms**. A national ID system would depend on both the issuance of an ID card and the integration of huge amounts of personal information included in state and federal government databases.
- **A national ID would be expensive and direct resources away from other more effective counterterrorism measures**. The costs of a national ID system have been estimated at as much as $9 billion.
- **A national ID would both contribute to identity fraud and make it more difficult to remedy**. Americans have consistently rejected the idea of a national ID and limited the uses of data collected by the government. In the 1970s, both the Nixon and Carter Administrations rejected the use of social security numbers as a uniform identifier because of privacy concerns. A national ID would be "one stop shopping" for perpetrators of identity theft who usually use social security numbers and birth certificates for false IDs (not drivers' licenses). Even with a biometric identifier, such as a fingerprint, on each and every ID, there is no guarantee that individuals won't be identified - or misidentified - in error. The accuracy of biometric technology varies depending on the type and implementation. And, it would be even more difficult to remedy identity fraud when a thief has a National ID card with your name on it, but his biometric identifier.
- **A national ID could require all Americans to carry an internal passport at all times**, **compromising our privacy, limiting our freedom, and exposing us to unfair discrimination based on national origin or religion**. Once government databases are integrated through a uniform ID, access to and uses of sensitive personal information would inevitably expand. Law enforcement, tax collectors, and other government agencies would want use of the data. Employers, landlords, insurers, credit agencies, mortgage brokers, direct mailers, private investigators, civil litigants, and a long list of other private parties would also begin using the ID and even the database, further eroding the privacy that Americans rightly expect in their personal lives. It would take us even further toward a surveillance society that would significantly diminish the freedom and privacy of law-abiding people in the United States. A national ID would foster new forms of discrimination and harassment. The ID could be used to stop, question, or challenge anyone perceived as looking or sounding "foreign" or individuals of a certain religious affiliation.

I would like to draw the Committee's attention to these last two points in particular. Given that Minister Coderre has specifically identified the ID card as a means to combat the growing incidence of identity theft, the argument presented above must first be answered. The notion of an

internal passport creates that fearsome image of a policeman in trench coat and fedora confronting a trembling individual, demanding to see his papers, an image associated with black-and-white movies set in Europe during the Second World War. For additional details, see the Epic report, "Your Papers, Please," [12]

V. TECHNICAL AND PROFESSIONAL CONCERNS

In this section, we will consider the concerns of such professional organizations as the Institute of Electrical and Electronics Engineers (IEEE), the Association for Computing Machinery (ACM) and the Committee on Authentication Technologies and Their Privacy Implications of the Computer Science and Telecommunications Board of the National Academies of the U.S. Prior to September 11, the IEEE issued a brief position statement against Universal Identifiers [

- The concept of an identifier that is both unique to an individual and "universal" in the sense of being always used by that individual to identify himself or herself in interactions with society, is fraught with danger. While such an identifier could provide convenience to the individual in assembling a detailed, intimate understanding of his or her interactions with society, similar convenience could well accrue also to many other parties and thus simultaneously be very attractive to many forms of painful misuse at the expense of the individual's privacy and security.
- IEEE-USA believes that individuals and society will be better served by a family of identifiers instead of by the use of a single identifier. A family of identifiers would allow different identifiers to be used, as appropriate to the security needs, privacy desires, and other tradeoffs of different transactions or situations. For example, person A might want to give a certain identifier to some other person B, so that B could also use that identifier to access certain information; but A might want different identifier(s) for other uses.
- The chosen identifier must be defined so as to be algorithmically suitable for its intended function. Such definitions would need to assure at the least that the identifier itself can be mathematically proven to have been accurately used and unchanged (such as with one or more "check digits"). The definitions must be extended to include additional levels of error correction and security as may be required for different intended functions.

The argument in favour of a "family of identifiers" is well taken and the Committee should certainly consider this proposal, which is rather close to the current situation in Canada.

The ACM includes as members most academic and research oriented computer scientists in the U.S. and Canada. Professor Ben Shneiderman, of the University of Maryland represented the U.S. Public Policy Committee of the ACM at the Subcommittee on Government Efficiency, Financial

Management and Intergovernmental Relations, Oversight Hearings on National Identification Cards, referred to above. Professor Shneiderman reminds us of the basic inadequacy of National ID cards, [14]

> "From a practical standpoint, a National Identity card system would not have prevented the tragic terrorist acts of September 11. Evidence suggests the suspected hijackers made no effort to conceal their identities. In fact, several of the suspected terrorists possessed state-issued ID cards with their pictures and names."

Furthermore,

> "Proponents of the National Id system suggest that cards will authenticate the identity of individuals. **However, the positive identification of individuals does not equate to trustworthiness or lack of criminal intent.**" [Original emphasis]. . . A national ID system requires a complex integration of social and technical systems, including humans to enter and verify data, plus hardware, software and networks to store and transmit. Such socio-technical systems are always vulnerable to error, breakdown, sabotage and destruction by natural events or by people with malicious intentions.

In a more technical sense, the creation of a database with 300 million records poses very serious problems, greater than those arising from the necessary database one-tenth the size required for Canada. Nevertheless, technical problems are real and they do raise constant and urgent questions about the effective operation of such large systems. Professor Shneiderman's remarks in this context are instructive and must be addressed by advocates of ID card systems. It is important to recognize that the card itself is only a small part of a very large and complex system. We turn again to Professor Shneiderman:

> "We must ask whether there is now a secure database that consists of 300 million individual records that can be accessed in real time? The government agencies which come close are the Internal Revenue Service and the Social Security Administration, neither of which are capable of maintaining a network that is widely accessible and responsive to voluminous queries on a 24 hour by 7 days a week basis."
>
> "Can records on everyone in the United States or even all foreign visitors be organized and maintained in one database? Compiling the necessary database to support the system would require a massive data-collection effort beginning with the interconnection of databases held by local, state and national government networks and some private entities. Determining what information to include in the database will no doubt prove to be controversial."

> "Once the problem of gaining access to the amount of information required is solved, there still would be challenges in creating a system that could communicate with all of the varied computer networks that would house components of individual identification. The difficulty of communicating with intra-federal, intergovernmental, and private sources of information in real time environment is unprecedented."

In 2001, the Computer Science and Telecommunications Board, a unit of the U.S. National Research Council, launched a study of issues associated with the implementation and use of a very large National ID card system. The study, published the following year, focused on the use of "authentication technologies and their privacy implications." [15] The following disclaimer sets the boundaries of this study:

> "There are numerous questions about the desirability and feasibility of a nationwide identity system. This report does not attempt to answer these questions comprehensively and does not propose moving toward such a system or backing away. Instead, it aims to highlight some of the significant and challenging policy, procedural, and technological issues presented by such a system. . . "

Given the stature of this board, it is wise to pay attention to its findings and recommendations. It raises a number of policy questions that must be considered and answered before undertaking the implementation of any National ID Card system.

- What is the *purpose of the system*? Possibilities range from expediting and/or tracking travel to prospectively monitoring individuals' activities in order to identify and look for suspicious activity to retrospectively identifying perpetrators of crimes.
- What is the *scope of the population* that would be issued an "ID" and, presumably, be recorded in the system? How would the identities of these individuals be authenticated?
- What is the *scope of the data* that would be gathered about individuals participating in the system and correlated with their national identity? While colloquially it is referred to as an "identification system," implying that all the system would do is identify individuals, many proposals talk about the ID as a key to a much larger collection of data. . .
- *Who would be the user(s)* of the system (as opposed to those who would participate in the system by having an ID)? One assumption seems to be that the public sector/government will be the primary user, but what parts of the government, in what contexts, and with what constraints? In what setting(s) in the public sphere would such a system be used? . .
- What *types of use* would be allowed? Who would be able to ask for an ID, and under what circumstances? Assuming that there are datasets associated with an individual's identity, what types of queries would be permitted (e.g., "Is this person allowed to travel?" "Does this person have a criminal record?")? . .

- Would participation in and/or identification by the system be *voluntary or mandatory* ? In addition, would participants have to be aware of or consent to having their IDs checked (as opposed to, for example, allowing surreptitious facial recognition)?
- What *legal structures* protect the system's integrity as well as the data subject's privacy and due process rights, and determine the government and relying parties' liability for system misuse or failure?

The Standing Committee would be well advised to read this rather short report if it intends to pursue this issue. The computer technologies which continue to develop, raise serious questions of security, of detailed description of access, of purpose, of facilitated "function creep," and more, much more. The authors of the report go on to urge more analysis especially of "both desirability and feasibility:"

- Given the potential economic costs, significant design and implementation challenges, and risks to both security and privacy, there should be broad agreement on what problem(s) a nationwide identity system would address. Once there is agreement on the problem(s) to be solved, alternatives to identity systems should also be considered as potential solutions to whatever problem(s) is identified and agreed upon.
- The goals of a nationwide identity system must be clearly and publicly identified and deliberated upon, with input sought from all stakeholders; public review of these goals prior to selecting a proposed system is essential.
- Proponents of such a system should be required to present a very compelling case, addressing the issues raised in this report and soliciting input from a broad range of stakeholder communities.
- Serious consideration must be given to the idea that--given the broad range of uses, security needs, and privacy needs that might be contemplated--no single system may suffice to meet the needs of potential users of the system.
- Care must be taken to explore completely the potential ramifications, because the costs of abandoning, correcting, or redesigning a system after broad deployment might well be extremely high.

VI. CANADIAN PRIVACY COMMISSIONERS SPEAK

Although the Committee is aware of the views of the George Radwansky, the Privacy Commissioner of Canada, Ann Cavoukian, the Information and Privacy Commissioner of Ontario, and David Loukidelis, the Information and Privacy Commissioner for British Columbia, they are

included in this submission for completeness and to confirm that major professionals in the area of privacy protection in Canada, are strongly opposed to a National ID card, and associated system.

George Radwansky delivered his annual report to parliament on January 29, 2003. From the outset, he launches a major critique of government policies that compromise the privacy rights of Canadians. More specifically, he is concerned that laws and policies ostensibly motivated by security concerns will find their primary use by law enforcement officials engaged in traditional activities. Thus security interests have been used to restrict the basic privacy rights of Canadians, actions that will not soon disappear. Mr. Radwansky emphasizes the following issues: [16]

> "Specifically, I am referring to: the Canada Customs and Revenue Agency's new "Big Brother" passenger database; the provisions of section 4.82 of Bill C-17; dramatically enhanced state powers to monitor our communications, as set out in the "Lawful Access" consultation paper; a national ID card with biometric identifiers, as advanced by Citizenship and Immigration Minister Denis Coderre; and the Government's support of precedent-setting video surveillance of public streets by the RCMP."

Although Mr. Radwansky has much of compelling interest to say about all these actions, for purposes of this submission, I would like to focus on his comments about the National ID card. The section on **Identity cards** reads as follows: [17]

> It is a matter of very considerable dismay that Citizenship and Immigration Minister Denis Coderre, presumably on behalf of the Government, is pressing for a "debate" on establishing a mandatory national identity card, complete with biometric identifiers, for all Canadians.
>
> Given the Government's current behavior on other privacy matters, it is difficult to avoid fearing that this means that it wishes to introduce such a card.
>
> That would be another huge blow to privacy rights. In Canada, we are not required to carry *any* identification – let alone to identify ourselves on demand – unless we are carrying out a licensed activity such as driving. Introducing a national identity card, even if it were "voluntary" at first, would push us toward becoming the kind of society where the police can stop anyone on the street and demand, "Your papers, please."
>
> The notion of the Government of Canada fingerprinting or eyeball-scanning every citizen for such a card is, of course, all the more abhorrent.
>
> **I can find no justification for a national identity card, especially since it is absolutely useless as an anti-terrorist measure.** As the perpetrators of the September 11 attacks demonstrated, terrorists are not necessarily previously identifiable as such. Every citizen would be able to obtain and display an identity card, regardless of his or her possible terrorist proclivities, but of course it wouldn't list occupation as "terrorist." And short-term visitors to Canada wouldn't have such a card at all.

> Rather than a "debate" about a grave and needless intrusion, Canada needs clear acknowledgement by the Government that the fundamental privacy right of anonymity as we go about our day-to-day lives is too important to abrogate for no apparent reason. [emphasis added]

Mr. Radwanski's argument is clear and forceful and consistent with the basic premises of this statement.

In a letter to Prime Minister Jean Chrétien and the leaders of the other Canadian political parties, which coincided with the delivery of the Privacy Commissioner's report to parliament, David Loukidelis briefly expressed his concern, as follows: [18]

> "I note with concern suggestions in some quarters that a national identity card should be introduced. In a free and democratic society, citizens are generally free to circulate without carrying any identification, let alone a national identity card. I propose to make my concerns about this known in more detail to the appropriate Committee of the House of Commons."

Finally, the views of Ann Cavoukian are also on record in a letter sent to the Committee on February 10, 2003. Let me just briefly highlight her concerns, as follows: [19]

1) **The requirement, scope and proposed use of the ID card:**
   The discussion of a national ID card has, to date, been lacking in any specific details as to its purpose and scope. As a result, the need for a national ID card system has yet to be justifiably demonstrated. While there are several possible uses one could propose for an ID card, Canada already has a number of tools in place that effectively address these issues.
2) **The enrollment requirements of the ID card system**
   The concept of a mandatory card system raises troubling privacy issues. A fundamental question yet to be answered is who would be required to register for the ID card and whether the production of the ID card, when requested by various authorities, would be a voluntary or mandatory obligation. Informational privacy revolves around the right of an individual to exercise choice and reasonable control over the collection, use and disclosure of his or her personal information. Obliging citizens to carry this card would significantly limit the control an individual has over the uses of his or her personal information, and the degree to which it may be disclosed to others.
3) **The effectiveness of a national ID card**
   It is important that government continually evaluate and assess the effectiveness of current public safety and security measures. Although new security initiatives may have implications for individual privacy, these implications may be within acceptable limits if the initiatives can be shown to be truly effective in promoting public safety. This case has not

> been made for a national ID card. To date, the government has provided little evidence that the creation of a national ID card would minimize terrorist activity.

Thus, Privacy Commissioners, whose obligations are to represent the privacy interests of Canadians in their jurisdictions, unanimously oppose the federal government's proposals.

VII. OTHER CONCERNS

A number of experts and relevant organizations have not yet been heard from. In order to include as wide a range of voices as possible in opposition to the introduction of a National ID card, this section will include brief observations from some leading scholars. Their views are reasoned, impassioned and informed; the included samples should encourage a more thorough examination of their works.

Colin Bennett

Colin Bennett, a professor at the University of Victoria, is one of Canada's leading scholars of privacy issues. In 1997 he presented a relevant paper at a meeting of the Canadian Political Science Association [20] His paper is quite long with many important observations, ideas, and warnings; for the present purposes, the following selections are taken from the Introduction:

> Around one hundred countries have official, compulsory national identity cards that are used for multiple purposes [21]. Some others, such as France, Italy and the Netherlands, have voluntary cards. In other countries (including Canada, Britain and the United States) the drivers license has become a *de facto* form of identification. Cards issued for specific "sectoral" purposes can over time be used for more widespread purposes and acquire some of the features of compulsory forms of identification. Identity cards vary in terms of their compulsory nature, their contents, their security features, the kind of database support, the forms of personal identifier used, as well in terms of the accompanying rules about who may have legitimate access to their contents and under what circumstances.
>
> These technologies have also, however, been regarded as a bad idea for a range of civil libertarian, practical and economic reasons [22]. The superficial attraction of modern card technology is attributable to their capacity to be used for multiple purposes. This multi-functionality raises dangers of the matching and linkage of those different data. For the privacy advocate, the clear segmentation of the data on the card is dictated by the privacy

> principle that information collected for one purpose should not be used for another. Even single purpose cards, however, are susceptible to the process of "function creep." The temptation to construct the card technology in such a way that it may be used for other applications may be inexorable.
>
> Identity cards are not just technologies, they are also *policy instruments*. . . As I have shown briefly above, these instruments may be used for a number of substantive and procedural ends. As policy instruments, their development will be influenced by the same range of forces that need to be considered in the comparative analysis of any policy choice. The fact that the manifestation of this instrument is confined to the individual's pocket does not alter the larger set of relationships that still need to be politically determined and that raise a complex range of social, economic, political, legal and technological issues.

Roger Clarke

Roger Clarke is a consultant , academic, and privacy advocate in Australia. In an important paper written in 1997, Mr. Clarke surveys the uses of ID cards around the world, offers detailed arguments about their dangers, and provides a multitude of issues that must be taken into account in determining whether or not they should come into use. The following are samples of Mr. Clarke's concerns as contained in the abstract of his paper: [23]

> Multi-purpose identification schemes in general, and national identification schemes in particular, represent the most substantial of information technologies' threats to individual liberties. This is because they concentrate information, and hence power; and because it is simply inevitable that, at some stage, even in the most apparently stable and free nations, power will be exercised against the interests of individuals, and of the public generally. . . Chips are being proposed as a means of identifying people as well. They present an opportunity to devise and implement highly repressive identification schemes; and many corporations and countries are in the process of harnessing those potentials. Chips also offer great scope for designing schemes that are privacy-sensitive, and that balance privacy interests against other social and economic interests and law and order concerns. Unfortunately, that scope has to date been almost entirely overlooked or ignored. This paper argues that the simplistic approaches being adopted by the proponents of identification schemes are in the process of destroying public confidence, and hence of undermining the intended return on investment.

Now, Mr. Clarke recognizes that chip-based ID cards can be used in a way that respect individual privacy and the associated hard-won rights of the past several years. Mr. Clarke includes the following options in 'privacy-sensitive' design:

- 'electronic signature cards' rather than 'id cards';

- no central storage of biometrics;
- two-way device authentication;
- less identity authentication, and more eligibility authentication;
- fewer identified transaction trails, and more anonymity and pseudonymity;
- multiple single-purpose ids, rather than multi-purpose ids;
- separation between zones within multi-function chips; and
- role-ids as well as person-ids.

Finally, one last, important, point must be noted, namely a class of ID cards that Mr. Clarke characterizes as electronic signature cards. Such cards are characterized by the definition, "private keys used variously for message-encryption and for digital signatures may be stored on a personal card, but **no central storage of private encryption keys** must be permitted to develop."

Stefan Brands

Dr. Brands is an adjunct professor at the School of Computer Science at McGill University, the author of *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy*, (MIT Press, 2000), formerly with Zeroknowledge Systems, and now with Credentica. This section consists of comments sent to me by Dr. Brands a few days ago when he became aware of my appearance before this Committee.

> **Re: Comment regarding ID cards**
>
> This comment is in response to the plans of the Committee of Citizenship and Immigration to hold extensive hearings on a national ID card. I am an adjunct professor at the McGill School of Computer Science in Montreal, Canada, and the author of a widely acclaimed MIT Press book on secure electronic identity management. . . The opinions in this e-mail are solely my own, and do not necessarily reflect the opinions of anyone else.
>
> A naïve implementation of a national identity card for Canadians would pose grave threats to privacy. I will not get into the privacy issues here, but instead am writing on a more constructive note. Namely, it is entirely feasible to build a national ID card system that simultaneously addresses the security needs of government and the legitimate privacy needs of individuals. The key to using ID card technology in a privacy-friendly manner is to avoid architectures that rely on inescapable systemic identification of card holders. Over a decade of research by respected cryptographers has resulted in highly practical technologies for electronic identity cards that address the complete spectrum of security, liability, and privacy risks for all parties involved. These technologies restrict, by their very design, the flow of information to only those parties that have a legitimate need to see it.
>
> Most decision-makers are completely unaware of the existence of such technologies, since they are not yet available by way of off-the-shelve commercial products. IT specialists

working on behalf of the mainstream IT industry will not tell you about privacy-friendly solutions, since they invalidate much of the current commercial offerings of the IT security industry. As an unfortunate result, in most debates on national ID cards (and there have been many around the world in recent years) the issue of privacy-friendly solutions hardly ever comes up, simply due to a fundamental lack of technological awareness.

However, an all-or-nothing debate on a national ID card that lacks insight into state-of-the-art scientific knowledge serves neither government nor its citizens, and will only lead to the total abandonment of the initiative or to the adoption of a privacy-invasive solution (at the cost of many millions of tax-payer dollars).

Should government continue pursuing a national ID card, I strongly recommend that a serious study be conducted of privacy-enhancing solutions and how they can address the needs of both government and Canadian citizens.

Kind regards,
Dr. Stefan Brands
McGill School of Computer Science
sbrands@videotron.ca
www.xs4all.nl/~brands

An expanded description of Dr. Brands' work is given in APPENDIX B, to this report.

Katie Corrigan

Ms. Corrigan is the legislative counsel on privacy at the American Civil Liberties Union. In what follows I will present a few of the remarks she made before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Oversight Hearings on National Identification Cards, referred to above. In brief, Ms. Corrigan predictably bases her concerns on threats to privacy, with little positive effect on security. Consider the following: [24]

We ask Congress to use a three-prong analysis to promote safety and to reduce the likelihood that new security measures would violate civil liberties.

First, any new security proposals must be genuinely effective, rather than creating a false sense of security. Second, security measures should be implemented in a non-discriminatory manner. Individuals should not be subjected to intrusive searches or questioning based on race, ethnic origin or religion. Finally, if a security measure is determined to be genuinely effective, the government should work to ensure that its implementation minimizes its cost to our fundamental freedoms, including the rights to due process, privacy and equality.

> A national identification card does not pass these basic tests. A national ID card would substantially infringe on the rights of privacy and equality of many Americans, yet would not prevent terrorist attacks. The ACLU strongly opposes the creation of a national ID card, whether the card is embodied in plastic, or whether the "card" is intangible – a sort of "virtual reality" card consisting instead of a government-mandated computerized database containing information about most people in the United States linked by a government-issued identifier.

Prevent Genocide International

This is the global education project of Genocide Watch. A paper was presented in late 2001 at the Yale University Genocide Studies program. [25] This organization is concerned with the use of the National ID card to store ethnic, racial, or religious information, with purposes revealed, as follows:

> National ID cards of all kinds are controversial. In recent years in the United States, Britain, Canada and Australia proposals for introducing national ID cards and registry systems have raised debate about governmental control and privacy issues. Classification of ethnic, racial or religious groups on ID cards, however, is a distinctively different issue. Group classification on ID cards or other official personal documents (passports, residence permits, etc.) force a person to be affiliated with a governmentally-defined group and expose persons to profiling and human rights abuses based upon their group identity. In times of crisis such classifications facilitate the targeting of persons on the basis of group affiliation, making individuals readily identifiable for possible detention, deportation, or death.

Examples abound of countries that have used ID cards to contain such information. For example group classifications are contained on the ID cards of Israel (Nationality);China, Ethiopia, Kenya, Vietnam, and Russia (Ethnicity); Dominican Republic, Malaysia, Singapore, South Africa, and some State Driver's Licenses only in the U.S. (Race/Color); Afghanistan, Brunei, Egypt, Jordan, Turkey, Greece, and Lebanon (Religion); and Myanmar, Indonesia, and Sri Lanka (Multiple Categories). There is more but it is clear that the existence of a National ID card may permit or even encourage the state to include information related to concerns that go beyond the intended primary purposes of the card.

VIII. CONCLUSIONS

Let me clearly state in conclusion, that Electronic Frontier Canada (EFC) is opposed to the introduction of a National ID card, both in principle and in practice. Such cards will not work for the purposes enunciated by Minister Coderre, namely identity theft and ease of crossing into the U.S. In addition, they will not deter terrorism as the mere possession of a card cannot supply the information needed to apprehend suspected terrorists. Among other concerns are the potential loss of a major right in democratic societies, the right to be anonymous, the "right to be let alone." The existence of an ID card would see an increase in the demand to see the card by law enforcement officials, wherever and whenever they see fit. Let me reiterate the five reasons against a National ID card proposed by the American Civil Liberties Union: [26]

- Reason #1: A national ID card system would not solve the problem that is inspiring it.
- Reason #2: An ID card system will lead to a slippery slope of surveillance and monitoring of citizens.
- Reason #3: A national ID card system would require creation of a database of all Americans. [Read Canadians for present purposes]
- Reason #4: ID cards would function as "internal passports" that monitor citizens' movements.
- Reason #5: ID cards would foster new forms of discrimination and harassment.

Current examples around the world, as well as historical ones, reveal the detrimental and occasionally deadly effects of National ID cards, or "papers." The crucial issue of a self-contained card or a card based on a centralized database must be carefully evaluated. As Roger Clarke warned, "no central storage of private encryption keys must be permitted to develop."

Finally, the call for a discussion and debate on National ID cards is premature. Parliament has not done its homework. This submission, and many others I am sure, have raised a host of serious questions about the need, purpose, and dangers associated with an ID card. As Dr. Brands' contributions demonstrate much turns on technical issues associated with the implementation of an ID card system. The use of the word system cannot be overemphasized.

If there remains a serious interest in National ID cards after this series of hearings, then the House must undertake a serious study of associated technical, political, and social issues. However, challenges mounted in the present submission and no doubt in many others, including the results of studies in other countries as well as historical evidence, should provide convincing reasons to terminate further consideration. Indeed, the U.S., the primary target of international terrorism on

September 11, has decided, yet again, not to proceed with the introduction of a National ID card system. In this context, Canada should follow suit.

REFERENCES

[1] Electronic Frontier Canada Web site at the URL: http://www.efc.ca/ .

[2] William Safire, "Threat of National ID, *The New York Times*, December 24, 2001. Available at the Web page with URL: http://www.nytimes.com/2001/12/24/opinion/24SAF1.html Archival material can only be obtained with payment.

[3] "Minister Calls for Debate on National ID Cards," CBC.CA News, November 22, 2002. Available at the Web page with URL: http://cbc.ca/cgi-bin/templates/print.cgi?/2002/11/14/id_card021114

[4] "A National Identity Card: Points on Which the Committee Invites Comments," House Standing Committee on Citizenship and Immigration. Available at the Web page with the URL: http://www.parl.gc.ca/InfoComDoc/37/2/CIMM/PressReleases/CIMMpr5-e.htm

[5] Bill Curry and Anne Dawson, "Coderre Seeks Public's Input on National ID Card," *National Post*, February 07, 2003. Available at the Web page with URL: http://www.nationalpost.com/search/site/story.asp?id=1314AF91-7E8E-4950-928A-3F4CEF41c28c

[6] Rudi Veestraeten, Counselor and Consul, Embassy of Belgium, "Identity Cards and National Register in Belgium." House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Oversight Hearings on National Identification Cards (or Card Systems), November 16, 2001. Available at the Web page with URL: http://reform.house.gov/gefmir/hearings/2001hearings/1116_nationa._id/veestraeten_testimony.doc

[7] "Netherlands, ID Checks to Be Introduced," *Statewatch News*, January 2003. Available at the Web page with URL: http://www.statewatch.org/news/2003/jan/05neths.htm

[8] Simon Davies, "Campaigns of Opposition to ID card Schemes," Privacy International, No date given. Available at the Web page with URL: http://www.privacyinternational.org/issues/idcard/campaigns.html

[9] "National ID Cards: 5 Reasons Why They Should Be Rejected." American Civil Liberties Union, 2002. Available at the Web page with URL: http://archive.aclu.org/features/National_ID_Feature.html

[10] Adam Thierer, "National ID Cards: New Technologies, Same bad Idea," The Cato Institute, *TechKnowledge Newsletter*, Issue #21, September 28, 2001. Available at the Web page with URL: http://www.cato.org/tech/tk/010928-tk.html

[11] Letter to President Bush, Electronic Privacy Information Center, February 11, 2002. Available at the Web page with URL: http://www.epic.org/privacy/id_cards/presidentltr2.11.02.html

[12] "Your Papers, Please," Electronic Privacy Information Center, February 13, 2002. Available at the Web page with URL: http://www.epic.org/privacy/id_cards/yourpapersplease.pdf

[13] "Against Use of Universal Identifiers (UIDs)," IEEE-USA Position Statement, February 15, 2001. Available at the Web page with URL: http://www.ieee.org/organizations/pubs/newsletters/npss/0601/against_UID.htm

[14] Professor Ben Shneiderman, "National Identification Card Systems," House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Oversight Hearings on National Identification Cards (or Card Systems), November 16, 2001. Available at the Web page with URL: http://reform.house.gov/gefmir/hearings/2001hearings/1116_nationa._id/shneiderman_testimony.doc

[15] *IDs—Not That Easy: Questions About Nationwide Identity Systems*, National Research Council, Washington, DC: National Academy Press, 2002. Available at the Web page with URL: http://books.nap.edu/html/id_questions/

[16] George Radwansky, "The Annual Report to Parliament, 2001-2001," The Privacy Commissioner of Canada, January 2003.Available at the Web page with URL: http://www.privcom.gc.ca/information/ar/02_04_10_e.pdf

[17] **Ibid**., p. 13.

[18] David Loukidelis, "Letter to the Right Hon. Jean Chrétien PC MP," January 29, 2003. Available at the Web page with URL: http://www.privcom.gc.ca/media/le_030130_2_e.asp

[19] Ann Cavoukian, "Submission to the Standing Committee on Citizenship and Immigration on the issue of a proposed national identity card," February 10, 2003. Available at The Web page with URL: http://www.ipc.on.ca/scripts/index_asp?action=31&P_ID=14049&N_ID=1&PT_ID=11457&U_ID=6752

[20] Colin Bennett, "Pick a Card: Surveillance, Smart Identification and the Structure of Advanced Industrial States," Paper presented at the 1997 Canadian Political Science Association Annual Meeting, St. John's Newfoundland, June 8th 1997. Available at the Web page with URL: http://web.uvic.ca/~polisci/bennett/research/cpsa97.htm

[21] Simon Davies, "A Case of Mistaken Identity: An International Study of Identity Cards." Toronto: Information and Privacy Commissioner of Ontario, 1995

[22] _____, *Big Brother: Britain's Web of Surveillance and the New Technological Order*. London: Pan, 1996.

[23] Roger Clarke, "Chip-based ID: Promise and Peril." Invited Address to a Workshop on 'Identity Cards, With or Without Microprocessors: Efficiency Versus Confidentiality', at the International Conference on Privacy, Montreal, Canada, September 23-26, 1997. Available at the Web page with URL: http://www.anu.edu.au/people/Roger.Clarke/DV/IDCards97.html

[24] Katie Corrigan, Presentation before the House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Oversight Hearings on National Identification Cards (or Card Systems), November 16, 2001. Available at the Web page with URL: http://reform.house.gov/gefmir/hearings/2001hearings/1116_nationa._id/corrigan_testimony.doc

[25] Jim Fussell, "Group Classification on National ID Cards as a Factor in Genocide and Ethnic Cleansing," Presented on November 15, 2001 to the Seminar Series of the Yale University

Genocide Studies Program. Available at the Web page with URL: http://www.preventgenocide.org/prevent/removing-facilitating-factors/Idcards/

[26] **Op. cit.**, "National ID Cards: 5 Reasons Why They Should Be Rejected."

APPENDIX A: Publications by Richard S. Rosenberg with Specific Reference to Privacy Issues

Books:

The Social Impact of Computers, Second Edition. (San Diego, CA: Academic Press) 1997, 522 pp. (First Edition 1992.)

Computers and the Information Society (New York: John Wiley & Sons) 1986, 397 pp.

Papers:

Is the Enemy Us? – New Threats to Privacy, Freedom of Information and Civil Liberties in the Age of Terrorism. **IFIP WCC2002** (International Federation of Information Processing, World Computer Conference), Montreal, PQ, August 25-30, 2002. In Brunnstein, Klaus and Berleur, Jacques (Eds.). **Human Choice and Computers**, Boston: Kluwer Academic Publishers, 2002, pp. 183-194.

Health Information in Canada: Can Privacy be Protected? ***CEPE 2001*** **IT and the Body** (Computer Ethics: Philosophical Enquiry), Lancaster University, UK, December 14-16, 2001, pp. 184-203.

The workplace on the verge of the 21st century, *Journal of Business Ethics*, Vol. 22, No. 1, October 1999, pp. 3-14.

Privacy protection on the Internet: the marketplace versus the state. **Wiring the World: The Impact of Information Technology on Society**, IEEE Society on Social Implications of Technology, Indiana University South Bend, June 12-13, 1998, pp. 138-147. Also available at the Web page with URL: <http://www.ntia.doc.gov/ntiahome/privacy/files/5com.txt)>.

The workplace on the verge of the 21st century. **ETHICOMP98**, The Fourth International Conference on Ethical Issues of Information Technology, Erasmus University, The Netherlands, 25 to 27 March 1998.

The politics of privacy on the information highway. **Global Networking '97 Joint Conference**, Vol. II, pp. 174 - 183. June 15 -18, 1997, Calgary, Alberta.

The politics of privacy on the global information highway. Culture and Democracy Revisited in the Global Information Society, May 8 - 10, 1997, Corfu, a Working Conference organized by Working Group 9.2: Social Accountability of Computing, **International Federation for Information Processing**.

Other Activities:

Presentation and Chair of Expert Panel for Consultation and Workshop on New Proposals for Lawful Access, Presented by BC Freedom of Information and Privacy Association (FIPA),

Department of Justice, Industry Canada, and Solicitor General of Canada, on behalf of Electronic Frontier Canada and FIPA, November 2, 2002, Empire Landmark Hotel, Vancouver, BC

Expert Witness Hearing, Special Committee on Information Privacy in the Private Sector, Legislative Assembly of British Columbia, Victoria, September 21, 2000.Official presentation available at http://www.legis.gov.bc.ca/cmt/priv_ps/Hansard/ip00921.html

Presentation before The Subcommittee on Communications of the Standing Senate Committee on Transport and Communications to examine the policy issues for the 21st century in communications technology, its consequence, competition and the outcome for consumers, Ottawa, ON, May 16, 2000.

Presentation before the Standing Parliamentary Committee on Industry on Bill C-54 (later Bill C-6) Personal Information Protection and Electronic Documents Act, on behalf of Electronic Frontier Canada, Ottawa, ON, February 9, 1999.[Available at EFC web site, http://www.efc.ca/pages/doc/efc-rosen-c54.09feb99.html. Official presentation available at http://www.parl.gc.ca/InfoComDoc/36/1/INDY/Meetings/Evidence/indyev85-e.html

Visiting Professor, Technical University of Darmstadt, May-June 1998. Gave four lectures on privacy issues at Darmstadt and at the University of Bonn.

Interview and participation in a piece for the CBC National Magazine on threats to personal privacy with Hana Gartner, May 18, 1998.

Invited by Industry Canada to participate in a workshop to review the White Paper, The Protection of Personal Information, January 1998. Ottawa, February 4 -5, 1998.

Invited participant to a U.S. NRC Workshop, What Everyone Should Know About Information Technology, Irvine, CA, January 14-15, 1998.

APPENDIX B: Contribution by Dr. Stephen Brands

Dr. S. Brands
brands@credentica.com

January 24, 2003

To: Entitlement Cards Unit
entitlementcardsunit@homeoffice.gsi.gov.uk

Re: Response to the July 2002 Consultation Paper "Entitlement Cards and Identity Fraud"

1. Introduction

This note is a response to your July 2002 Consultation Paper titled “Entitlement Cards and Identity Fraud.” I am an adjunct professor at the McGill School of Computer Science in Montreal, Canada, and the author of a widely acclaimed MIT Press book on the topic of secure electronic authentication and access management (see http://www.credentica.com/technology/book.html). The opinions in this note are solely my own, and do not necessarily reflect the opinions of anyone else.

The national entitlement card, as currently envisioned by government, poses grave threats to the privacy of UK citizens.[i] I will not address the privacy threats here in detail; without doubt they are well-documented in many of the other responses to the consultation paper. Instead, I am writing you on a more constructive note, namely to inform you that it is entirely feasible to build a national entitlement card system that would simultaneously address the security needs of government and the legitimate privacy needs of individuals.

The key is to avoid security architectures for the entitlement card that rely on inescapable systemic identification of card holders. This can be accomplished by adopting a suitable privacy-enhancing architecture that restricts, *by its very design,* the flow of information to only those parties that have a legitimate need to see it.

2. How to build a privacy-friendly national entitlement card

The solution to building a privacy-friendly national entitlement card is to use proper cryptographic techniques for the certification and disclosure of personal information. According to page 125 of your consultation paper, digital identity certificates are currently being considered for inclusion. However, digital identity certificates have fundamental design flaws that make them highly inappropriate in the context of a national entitlement card. They do nothing to discourage participants from using each other's credentials, and encourage large-scale identity fraud and other devastating abuses of security holes that are inevitably caused by heavily relying on the central storage of information. Furthermore, the actions of card holders can be traced and linked automatically by a multitude of parties, on the basis of the uniqueness of the cryptographic keys that are disclosed whenever their cards communicate with the outside world. Finally, digital identity certificates cannot be implemented efficiently and securely in low-cost smartcards.

Two decades of research by dozens of highly respected cryptographers has resulted in highly practical technologies for digital certification and authentication that address the complete spectrum of security, liability, and privacy risks for all parties involved.[ii] Specifically, my own work of the past ten years has shown how to construct "Digital Credentials" that electronically mimic the key properties of paper credentials, plastic tokens, and other tangible objects. At the same time, Digital Credentials offer security, privacy, efficiency, and functionality benefits that go far beyond those of their traditional counterparts. Digital Credentials are basic cryptographic constructs, much like digital signatures but vastly more powerful.

---

[i] In short, the system would allow the actions of all card holders to be linked and traced automatically and in real time, not only by the parties directly involved in verifying entitlements but also by a multitude of other parties that users will not be aware of (and that organizations and other verifiers may find highly undesirable). Most card uses envisioned in your consultation paper, however, do not require systemic identification at all. Consider proving eligibility to access products and services, establishing whether a person has the right to work in the UK, allowing people to prove their age when purchasing age-restricted items, allowing employers to check eligibility for work, and supporting telephone or on-line voting; with all of these, identification is necessary only, if at all, at registration time.

[ii] Digital identity certificates, as described for instance in the X.509 standard, do not take any of these advances into account; they were developed in 1978, at the dawn of modern cryptography.

A national entitlement card based on Digital Credentials is entirely feasible, and would offer the following benefits:

Strong security: Digital Credentials offer audit capability for non-repudiation and to assess compliance with regulatory requirements, through secure digital audit trails and digital receipts. They support authentication strengths ranging from weak to military-grade two-factor and three-factor security. Different Credential Issuers can vouch for the authenticity of identity-related information by digitally certifying that information. Organizations can strongly discourage credentials holders from lending or cloning their access rights (even for pseudonymous access) by embedding disincentives that will be disclosed if and only if the legitimate holder commits a fraud; this provides a second security layer on top of the tamper-resistance of the cards themselves.

Negotiable privacy: Digital Credentials accommodate fully adaptable levels of privacy ranging from user-driven anonymity to government/enterprise-mandated identification. In particular, they allow for pseudonymous as well as role-based access (both server-driven for scalability and user-driven for privacy). Digital Credentials provide for automated trust negotiation for the exchange of credential information, ensuring that only the minimum credential information needed to meet the authorization requirements of the service provider is disclosed. In particular, identity-related information can be selectively disclosed in a manner that does not enable identification. Servers can access credential information with varying levels of involvement from the credential database manager and the users themselves.

Information can reside anywhere: Credential information can be held both locally on the card and remotely. Digital Credentials support federation of remotely stored credential information: credential information pertaining to the same entity can be accessed and managed as one logical entity even if it is distributed across different storage locations. They also facilitate roaming, as well as automated sharing and synchronization of credentials between local and remote credential information in accordance with application-specific administrative data.

Secure multi-application smartcards: Smartcards can be used as multi-application devices, without introducing any of the privacy and security problems caused by other technologies. Specifically, different application providers can all share the same secret key stored in a user's smartcard to derive the security benefits of that smartcard. The certificates will have uncorrelated secret keys which cannot be determined by anyone including the smartcard supplier, and all the certificates can be revoked separately. The application software on the user's trusted computer ensures that smartcards attacks are impossible, and that different applications using the same smartcard remain fire-walled.

Efficient smartcard implementations: The storage and computational burden for the entitlement smartcard can be off-loaded almost entirely to a user-controlled device (such as a handheld device with display and keypad, or another chip on the same smartcard that need not be trusted by the system provider), while preserving all the smartcard's security

benefits. Literally billions of digital certificates, which may come from disparate systems that do not trust one another, can be securely managed using a single 8-bit smartcard chip.

Limited-use access rights and credentials: Credential Issuers can issue credentials and access tokens that are valid a limited number of times. A built-in identifier, value token, or self-signed fraud confession will be exposed if and only the credential is shown more times than allowed.

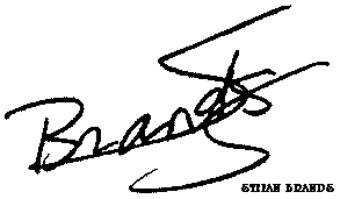
Managed Services: Credential Issuers can certify sensitive information on behalf or organizations without being able to learn that data, and Revocation Authorities can validate certificates (using OCSP or other standards) without being able to learn the identities of the clients of organizations (even when these expressly identify themselves to the organizations they transact with through the certificates themselves). In this manner, organizations can outsource core tasks related to digital authentication and authorization, without having to provide their managed services providers with competitive data or customer information for which they could incur legal liabilities. In fact, even the role of the tamper-resistant smartcard can be outsourced, thereby removing the need for government to securely distribute tamper-resistant devices to card holders; although each and every transaction of a card holder would now require the real-time involvement of a third party that guarantees protection of the user's secret key, that third party cannot learn any details that could lead to a compromise of the user's privacy.

Peer-to-peer support: Organizations can securely give individuals control over some or all of their own credential information by allowing them to store and manage the information locally on their own entitlement card. This information is cryptographically protected to ensure that users cannot modify, discard, pool, lend, or prevent updates of information for which they have no right to do so. In the extreme, one can do away entirely with central databases containing sensitive personal information, by securely distributing each database entry to the card of the individual to whom it pertains. By basing authorization decisions directly on authenticated attributes shown by the requestor himself, trust can be established off-line on first contact, with no prior knowledge of the requestor. This approach provides a superior alternative from the perspective of administratively scalability.

The practicality of the Digital Credentials technology has been well-established. For example, from 1993 until 1999, CAFE and OPERA (two European consortiums co-funded by the European ESPRIT program) implemented and extensively tested an electronic cash implementation for smartcards based on the Digital Credentials technology. Also, the technology has received worldwide acclaim from privacy advocates, security experts, and legal experts; see the selected endorsements for examples.

I would be happy to provide you with further details as well as a prototype demonstration of the technology should this be of interest to you.

Kind regards,



Dr. Stefan Brands
brands@credentica.com

SELECTED ENDORSEMENTS

“minimizing the risks of all the interested actors"

EPIC & Privacy International, in “Privacy & Human Rights 2001; An international survey of privacy laws and developments,” pp 50 - 55.

"shows ways to do digital certificates without giving so much power to the system owner"

Former Chief Privacy Counselor to the Clinton Administration, Dr. Peter Swire, in "Electronic Banking Law and Commerce Report," April 2001, volume 5, number 10.
http://www.law.ohio-state.edu/swire1/EBLCRAprilSwireInterview.doc

“a new standard of privacy in technology"

Information and Privacy Commissioner for Ontario, Canada, Dr. Ann Cavoukian, back cover of "Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy," MIT Press, August 2000, ISBN 0-262-02491-8.

"not "all-or-nothing" certificates”

Federal Privacy Commissioner of the Netherlands, in "Sleutels van vertrouwen", Den Haag, March 2001. ISBN 90 74087 264. Translation from Dutch.
http://www.registratiekamer.nl/bis/top_1_5_35_19.html#1207

"all the characteristics necessary to provide both full authentication of identity and attributes, but allows the subscriber to 'blind' the identity when they choose to do so"

Federal Privacy Commissioner of Australia, in "Privacy Issues in the Use of Public Key Infrastructure for Individuals And Possible Guidelines for Handling Privacy Issues in the Use of PKI for Individuals by Commonwealth agencies", Consultation Paper, June 2001.
http://www.privacy.gov.au/publications/dpki.html

"far-reaching work"

Dr. Marit Köhntopp of the Privacy Commissioner of Nordrhein-Westfalen, Germany. Translation from German.
http://www.koehntopp.de/marit/publikationen/idmanage/usersview

“an important landmark in the evolution of privacy-enhancing technology"

Dr. Ronald L. Rivest (Webster Professor of Electrical Engineering and Computer Science at MIT), foreword to "Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy." MIT Press, August 2000, ISBN 0-262-02491-8.

"security without sacrificing privacy"

Dr. Hal Abelson (Professor at the Artificial Intelligence Laboratory of MIT), back cover of "Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy," MIT Press, August 2000, ISBN 0-262-02491-8.

"a wide range of potential application"

Dr. Ross Anderson (Professor at the Computer Laboratory of Cambridge University), back cover of "Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy," MIT Press, August 2000, ISBN 0-262-02491-8.

"defines the state of the art"

Dr. A. Michael Froomkin (Professor of Law, University of Miami), back cover of "Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy," MIT Press, August 2000, ISBN 0-262-02491-8.

"a superior alternative to conventional approaches to PKI"

Dr. Roger Clarke, privacy expert and IT consultant to the Australian government.
http://www.anu.edu.au/people/Roger.Clarke/II/PKIMisFit.html