NATIONAL IDENTIFICATION SCHEMES (NIDS):
A Remedy Against Terrorist Attack?[13]

Andrew Clement
Faculty of Information Studies, University of Toronto clement@fis.utoronto.ca
Robert Guerra
CPSR rguerra@privaterra.com
Jeff Johnson
CPSR; UI Wizards, Inc. jjohnson@uiwizards.com
Felix Stalder*Openflows; Surveillance Project, Queen's University felix@openflows.org*

Abstract The terrorist attacks of September 11, 2001 on the World Trade Center and the Pentagon have rekindled public debate about National Identification Schemes (NIDS) in the US, Canada, and other countries. While much of the debate has focused on the tradeoffs between security protection and the potential loss of privacy and other civil liberties, this paper examines the prior question of whether a NIDS would actually be effective in preventing terrorist attacks of the kind the world recently witnessed. It examines currently proposed NIDS and finds none that identify how it would contribute to reducing the threat of major terrorist attack. By relying on unfocused measures of questionable effectiveness, NIDS may actually create a false sense of security that leaves us more vulnerable than before. We therefore risk impairing our vital liberties with little gained in return. In this light, the oft-cited trade-off between liberty and security may be irrelevant, or worse, a distraction that prematurely concedes and obscures a dangerous presumption.

Key words: national identification schemes, security, smart cards, biometrics, civil liberties

[13] This paper is based on the Computer Professionals for Social Responsibility (CPSR) *National Identification Schemes (NIDS) and the Fight against Terrorism: FAQ (Frequently Asked Questions)* (Clement, et al., 2001). The authors are grateful for the contributions of Ian Bicking, L. Jean Camp, Paul Czyzewski, Susan Evoy, Harry Hochheiser, Peter Hope-Tindall, Chris Hibbert, Alessandro Lofaro, Lenny Siegel and other participants in the [CPSRnatIDfaq] discussion list. For more information, please see CPSR's website at **http://www.cpsr.org**

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35609-9_29

K. Brunnstein et al. (eds.), *Human Choice and Computers*

1. INTRODUCTION

The extraordinary ferocity of the attacks of September 11, 2001 on the World Trade Center and the Pentagon have lead to demands for extraordinary security measures. In the U.S. and Canada, one of the most prominent proposed measures has been the introduction of a National Identification Scheme (NIDS). Much publicity has been given to the offers of the CEOs of two major technology vendors to donate key components of a NIDS.[14]

In November, the US Congress held hearings on "Does America Need A National Identifier?", followed by similar hearings convened by the California State Assembly Judiciary Committee. Reflecting the perception that the drivers' license is the most likely candidate for basing a national scheme upon (Hoescht, 2001), the American Association of Motor Vehicle Administrators has announced that it plans to create a de facto national identification card for the US.

In Canada, the proposals have been more modest, but are heading in a similar direction. So far the only public step has been to upgrade Canada's notoriously unreliable paper-based Immigrant Card. However, the Toronto *Globe and Mail* newspaper reported that 80% of Canadians would submit themselves "to providing fingerprints for a national identity card that would be carried on your person at all times to show police or security officials on request" (October 6, 2001). This suggests that the public assumes that diminished liberty would be compensated by improved security, an assumption that we question.

Similar measures are being considered in the U.K. A public opinion poll following the September 11 attack "showed 86% in the UK backed the introduction of some form of ID card." (Travis, 2002) In February 2002 the UK Home Office, announced a consultation exercise on NIDS, with David Blunkett, the home secretary, clearly preferring "a compulsory entitlement card which would replace passports and driving licences and give access to public services." (Travis, 2002).

These proposals are only the latest round in a recurring pattern, and as in the past, have stimulated sharp debate about the pro's and con's of NIDS, with much attention given to the obvious threats to civil liberties (Turley,

[14] Among the most vocal promoters of a national ID card in the wake of the September 11 terrorist attacks were industry leaders such as Larry Ellison, CEO of Oracle, who proposed a system based on a large database provided by his company (Ellison 2001). Sun's CEO Scott McNealy proposed a system based on the distributed intelligence of smart devices using Sun's Java to execute authentication algorithms (Coffee 2001). While both offered to provide the technology for free, the ensuing maintenance and upgrading contracts would have turned their "gifts" into very lucrative businesses.

2001; Etzioni, 2002). Before we pin our hopes on a NIDS as a remedy to terrorist threat and assess what civil and economic costs we are and are not willing to pay for it, we must examine the prior issue of whether it could even be effective as a safeguard. This is the central issue we address here.

In its recent report raising a range of serious questions about national identification systems, *IDs – Not That Easy*, the National Academy of Sciences Committee on Authentication and Technologies and Their Privacy Implications (2002) noted "that serious and sustained analysis and discussion of the complex issues presented by national identity systems are needed. Understanding the goals of such a systems is a primary consideration." While it is beyond the scope of this paper to consider all the possible goals of a NIDS, it does address the fundamental question raised by the Committee: "What is the purpose of the system?" This paper seeks to contribute to the longstanding NIDS debate by exploring the new aspects surrounding the presumed protections against severe terrorist assault. In particular, it focuses on the requirements for a NIDS to be effective in preventing an attack by a small number of modestly resourced but highly disciplined people like those who conducted the September 11 atrocity.

This paper is organized as follows: first we examine the structure and scope of current NIDS proposals. Then we look at NIDS in the context of the Sept. 11 attack. The most substantive part of the paper assesses the potential of NIDS to live up to their claimed promises, as well as the security risks they pose in their own right. In the conclusion, we re-examine the tradeoffs between security and civil rights as well as the need for an informed public debate.

2. STRUCTURE AND SCOPE OF PROPOSED NIDS

Many different national identification schemes (NIDS) have been proposed. A key feature in all of them is that people in a particular country would be required, or at least expected, to present an officially issued ID card in order to obtain particular services or pass security checkpoints. Traditionally, NIDS have been used or proposed for handling routine administrative transactions between government agencies and citizens, with benefits claimed in the areas of convenience, cost savings, or fraud reduction. NIDS could combine the functions of a driver's license, the social security registration, and so on. Until recently, NIDS have rarely been suggested as a way to protect against terrorist attacks, partly because of inherent difficulties in achieving the required levels of security. Suddenly, in the wake of the terrorist attacks on September 11, 2001, preventing terrorism is being touted as a principal use of NIDS.

Current proposals for National IDs fall into several categories depending on whether people carry a physical card, and if so, what data are on it versus in a database. Many of the current proposed security oriented schemes involve the use of biometric data – recorded measures of human physiography and behaviour, most notably finger or retinal scans.

1. **Unique ID number; no card:** This familiar scheme assigns each person a unique ID number, like a Social Security number, that they then use to identify themselves. All personal information is stored in government databases. There is either no card, or the card is just a piece of paper that is irrelevant to identification transactions.

2. **Unique ID code on card and in database(s); biometrics and other data in database:** The card has a unique ID number, like a debit card number, which is required for use as a database key. Other data about the person is stored in databases of government agencies.

3. **Biometric data on card only; no ID number; no database**: The card contains an encoding of the person's fingerprint or retina-scan, as well as a photograph and other data. At authentication locations (e.g., airport security gates) the biometric measure stored on the card is compared with a new scan of the person's fingerprint or retina. The biometric data is kept only on the cards; there are no government databases storing it. No explicit unique ID number is required for such a scheme. Civil Rights lawyer Alan Dershowitz advocates a voluntary version of this scheme. Sun Microsystems CEO Scott McNealy agrees, and promotes a ava-based smart ID card.

4. **Unique ID code and biometric data on card; ID code, biometrics and other data in database:** A unique ID is assigned, after checking a biometric database to ensure that a prospective cardholder had not previously registered with a different identity. This is the scheme being pushed by Larry Ellison, the CEO of Oracle, a database company.

5. **Biometric data in database only, no card:** In this scheme, a database is created with each person (supposedly) uniquely identified through biometric measurements, but no ID number are assigned. Data is read from individuals' bodies at security points (or elsewhere) and compared with the biometric database for a match. In addition to the usual biometric measures, face-recognition technology is being considered, despite the fact that it currently is much less reliable than other biometric identification techniques.

Current proposals also vary as to whether possession of an ID card would be mandatory or voluntary. Some proposals make it voluntary for citizens, but mandatory for visitors and immigrants, as called for in the USA-PATRIOT Act. In a mandatory scheme, everyone is required to carry and present a card when asked; not doing so is an offence. In a voluntary scheme, those who do not have a card will be subjected to additional background checks while those with a card can more easily obtain services or pass security checkpoints (e.g. The INS Passenger Accelerated Service System (INSPASS) in operation since 1995 to expedite immigration inspection processing at selected points of US entry). However, because of the suspicion that would be raised by not having a card and the extra checking required to clear such people, it is very likely that a voluntary scheme would develop irresistible pressures to turn it into a mandatory one.

From the point of view of a "user", there are at least two distinct processes in a functioning NIDS:

First is a one-time *registration* process in which everyone is required to present themselves to the authorities along with their existing identification documentation, such as birth certificate or citizenship papers. If the authorities believe the documentation is valid, they create an individually identified entry in a database and issue the person a card that, in most systems, would be linked to this entry. In recently proposed schemes, this would be a "smart" card containing a micro-chip that stores and accesses information and possibly biometric data about the person.

The second process is *authentication.* This occurs whenever the cardholder is required to show the card to verify his or her identity. A first check is made to ensure that the card actually belongs to the person presenting it. This is done by comparing the information on the card with the person, for example by visual comparison of the cardholder with the photograph on the card, or by digital comparison of a live finger scan with the finger print recorded on the card. If there is a satisfactory match, the unique ID or biometric signature is used as a link to a database. A second check then determines whether there is anything on file that raises suspicion about the cardholder. If not, the person can proceed.

There is also a third, behinds-the-scenes, *data-matching* process, in which authorities analyze and compare information in the NIDS databases to determine whether information about a person is present in more than one database, in order to augment what is known about that person. Usually this is done without the person's knowledge between the registration and authentication steps. Closely associated with this is the controversial process of *profiling*, in which people are flagged as suspicious not because of any individual acts but due to their category memberships (e.g. race, religion, ethnic origin, political affiliations, etc.) (Shattuck 1996).

The various proposed identification schemes differ in how well they support each of the three processes: registration, authentication, and data-matching. For example, card-only schemes enable registration and authentication, but not data-matching.

3. CAN A NIDS DO WHAT IT PROMISES?

3.1 Securely Identify Everyone?

The strong claim for the security value of a NIDS rests on the assumption that individuals can be uniquely and reliably identified. Using biometric data such as fingerprints and retina scans can help in verifying that the card actually belongs to the cardholder. However, this is not 100% reliable. There is always a margin of variation between the original sample obtained during registration and any subsequent sample used at the point of authentication. In general, the tighter tolerances are set to avoid falsely authenticating an impostor, the more that cardholders will be falsely assessed as not matching their rightly possessed cards, and vice versa when tolerances are loosened. In a security oriented scheme that aims to ensure that no one slips through by pretending to be the cardholder, the range of tolerance must be set so narrow that there will be significant numbers of people who will not appear to be legitimate cardholders when in fact they are. (Clarke, 2001)

Using biometric data to identify people also encounters the problem that for any biometric measurement we use, some people will not be able to provide that data. Some people lack hands and therefore have no fingerprints. Some people have hands but their fingerprints are too poorly defined to be readable. If we adopt a fingerprint-based system, how do we accommodate such people? Similarly, using retina scans would exclude people whose retinas cannot be scanned for various reasons, e.g., they have cataracts. Would such people face a lifetime of suspicion by authorities? For example, would they be unable to fly on airplanes?

More fundamentally, however, biometric identification is just one step in the overall NIDS process. The security provided by the overall system is governed by its weakest link. The issuance of a high-security ID card is based on the presentation of low-security documents. Anyone with a convincing passport or birth certificate would be able to obtain an ID card. This is already a problem with present NIDS in Europe and elsewhere. All biometrics help to do is to make sure that the cardholder is really the person identified by the card and, if they are, enable checking that persons

information in a database. Using biometric data does nothing to ensure that the information the person presents when obtaining the card is correct.

3.2 Prevent a September 11 Attack?

The key test for a security oriented NIDS proposal is whether it would have prevented the September 11 attacks. It is most likely that the answer is no. The Immigration and Naturalization (INS) has determined that all 19 of the hijackers entered the United States on legal visas (Council on Foreign Relations, 2002), and had no record of offence with the FBI or other security agency. In other words, they could have obtained a legitimate ID card and the authentication checks prior to boarding the plane would have not have revealed anything that would have aroused the suspicions of authorities. As HCI expert, Ben Shneiderman notes in his testimony on behalf of USACM at the Congressional Hearings on National Identification Card Systems:

> **[T]he positive identification of individuals does not equate to trustworthiness or lack of criminal intent.** (emphasis in original) (Shneiderman, 2001)

From terrorist training documents captured in the UK, it appears that the terrorists favoured a simple but effective strategy of 'blending in'. They eschewed sophisticated communications technologies such as encryption and instead focused on passing as 'normal' citizens. To escape attention, they were even advised to talk about sports with their acquaintances and avoid getting traffic tickets. This low-tech strategy, which worked in the 2001 attack, is likely to continue to foil a security apparatus that relies on the routine screening of millions of people to detect anomalies in behaviour.

In other words, no NIDS regardless of the strength of its biometric authentication, offers security against terrorists who have no record of prior misconduct and are not worried about being identified after the attack (possibly because they will be dead).

3. NIDS AS SECURITY RISK ITSELF

While smart cards are among the most secure technologies available, virtually all existing smart card systems have been compromised. As more and more smart cards are put into operation, more and more people know how to break them and have an incentive to do so.

If the card is used to check the information against a database, then the security of this database becomes crucial. It must be accessible nationwide in order to support security checkpoints all over the country. Therefore it will have to be on some network, probably the Internet or telephone system. The

security necessary to prevent people from breaking into such a sensitive networked system would be nearly impossible to achieve. For this reason, a NIDS creates security risks that would otherwise not exist.

Furthermore, if high-tech security cards can be compromised, it becomes impossible to distinguish a fake card from a legitimate one. A smart card may be more difficult to forge, but if successful, forgeries would be perfect.

Last but not least, a system as complex and comprehensive as a NIDS relies on the cooperation of thousands of people, hundreds of organizations and dozens technologies. As existing systems illustrate, notably the notoriously unreliable criminal information databases, each of these elements introduces a specific set of vulnerabilities. Securing the entire system against attacks and abuses will be close to impossible.

4. CONCLUSION

National identification schemes have in North America been given a major impetus in the aftermath of the September 11 terrorist attack. While there are significant technical developments, notably in biometric techniques, that can improve components of identification schemes, and further that these may improve security in small scale or low threat applications, there is no scheme that stands a good chance of protecting against the recurrence of that type of attack

Fully integrated identification schemes effective in warding against attack are extraordinarily difficult if not impossible to achieve. While there are many points of weaknesses in these proposals, the fundamental flaw they all share is that someone with apparently authentic documentation and no record of suspicious activity will pass smoothly through the most rigorous of screenings. They will operate freely until they commit their first, and perhaps final terrorist act. Because intent to commit a crime cannot be assessed reliably, identification alone will not increase security. With no more sophistication and resources than were displayed in the recent attacks, any organization that can recruit and hold people with "clean" identities can defeat any identification scheme. Once a small but disciplined group of people is bent on suicidal attack, a NIDS will offer no protection.

However, every proposed NIDS would involve extensive tracking of individuals. As the U.S. Courts and Congress as well as the Canadian Supreme Court have repeatedly recognized, people under constant surveillance are not free. Furthermore, a NIDS would also make everyone vulnerable to the problem of incorrect data in the database, which could victimize innocent people through no fault of their own. If other government

databases are any indication, a system as large as a NIDS would contain a significant amount of incorrect data.

NIDS, then, do not provide additional security against terrorist attack, but compromise civil liberties. Furthermore, given the hidden systemic weakness of any NIDS, such a highly visible system might well produce a false sense of security. By relying on flawed security, we might end up also compromising our security through a NIDS.

These various shortcomings are rather obvious for most people involved in these issues. Nevertheless, ID card schemes resurface again and again. Why? At least part of the answer can lies in the fact that there are powerful actors, notably high-tech industry, law enforcement and politicians (Stalder and Lyon, in press), who would profit from the introduction of ID cards independent of their actual usefulness in any specific context. So far, while proclaiming the apparent benefits, these promoters have not said how their schemes would actually work, nor what costs would be incurred.

The potential risks to civil liberties have meant that normally there is little public support for NIDS, in 'Anglo-American' countries at least. In the past 20 years, NIDS have been proposed at various times in the US, Canada, Australia and the UK. Each time politicians have dropped the schemes in the face of strong public opposition. But in the wake of the September attacks, there are signs of a shift in public attitudes in favour of NIDS.

However, because there has been no public explanation of how such a scheme would work, one must presume that this support reflects a general assumption that a NIDS would provide protection against another attack like that of September 11. It is quite likely the widespread suspicion of these schemes will return when the dubious advantages and numerous pitfalls are more widely known.

The critical missing ingredients in the NIDS debate are a clear assessment of the recent massive security failure, the risks we currently face and just how a NIDS would be effective in protecting us against these threats. Until there are viable comprehensive proposals that have a good chance of affording us the security we seek, it is at the very least premature to discuss possible diminishment of civil liberties. Citizens generally, and computer professionals in particular, need to be skeptical of the vague and unsubstantiated claims currently made about the benefits of identification schemes. They will certainly be enormously expensive and potentially highly intrusive, but in return may offer only a dangerous illusion of security while actually creating new vulnerabilities. The onus clearly is on their proponents to demonstrate their efficacy and that they have been developed in ways that are sensitive to the complex social/technical issues they inevitably involve.

Given the costs, risks and complexities of relying on a technologically driven NIDS approach, it seems prudent to rely more on enhancing the human and social dimensions of security. At the very least there needs to be an open, informed public discussion of the social and technical alternatives. As the National Academy of Sciences Committee cited earlier concludes: "Proponents of such a system should be required to present a very compelling case, ..." (NAS, 2002)

REFERENCES

Clarke, Roger (2001) Biometrics and Privacy, Notes of 15 April, 2001, http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html

Clement, A., Stalder, F., Johnson, J. and Guerra, R. (2001) *National Identification Schemes (NIDS) and the Fight against Terrorism: FAQ* Computer Professionals for Social Responsibility (CPSR), November 2001. http://www.cpsr.org/program/natlID/natlIDfaq.html

Coffee, Peter (2001) National ID cards are not the answer. *eWeek*, October, 24, 2001 http://www.zdnet.com/filters/printerfriendly/0,6061,2819922-2,00.html

Council on Foreign Relations (2002) Terrorism: Q & A website http://www.terrorismanswers.com/security/borders_print.html

Ellison, Larry (2001) Smart Cards: Digital IDs can help prevent terrorism. *Wall Street Journal*, October 8, 2001

Etzioni, Amitai (2002) You'll love those national ID cards, *Christian Science Monitor*, January 14, 2002 http://www.csmonitor.com/2002/0114/p11s1-coop.html

Hoescht, Tim, (Senior VP, Technology, Oracle Service Industries.) Testimony to the House Committee on Government Reform Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, November 16, 2001 http://www.house.gov/reform/gefmir/hearings/2001hearings/1116_nationa._id/1116_witnesses.htm

IEEE-USA (2001) Position Statement - Against Use Of Universal Identifiers (UIDs) February 15, 2001 http://www.ieee.org/organizations/pubs/newsletters/npss/0601/against_UID.htm

LeBlanc, Daniel (2001). 80 per cent would back national ID cards, *The Globe and Mail*, October 6, p. 1.

National Academy of Sciences, Committee on Authentication and Technologies and Their Privacy Implications (2002) *IDs – Not That Easy: Questions About National Identification Systems*, National Academy Press, http://books.nap.edu/html/id_questions

Neumann, P. and Weinstein, L. (2001) 'Risks of National Identity Cards' *Communications of the Association of Computing Machinery*, 44 147. www.csl.sri.com/users/neumann/insiderisks.html

Shneiderman, Ben, "National Identification Card Systems," Testimony to the House Committee on Government Reform Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, November 16, 2001 http://www.house.gov/reform/gefmir/hearings/2001hearings/1116_nationa._id/1116_witnesses.htm

Shattuck, John (1996). Computer Matching Is a Serious Threat to Individuals Rights. In Kling, Rob (ed.) *Computerization and Controversy: Value Conflicts and Social Choices* 2nd. Edition. pp. 645-651 San Diego: Academic Press

Stalder, Felix; Lyon, David (in press). Electronic Identity Cards and Social Classification. In Lyon, David (ed.) *Surveillance as Social Sorting: Privacy, Risk, and Automated Discrimination.* London, New York: Routledge

Travis, Adam (2002). Compulsory ID cards back on the agenda, *The Guardian*, February 6, 2002, p.5

Turley, Jonathan (2002). National ID: Beware what you wish for, Commentary, *LA Times*, http://www.latimes.com/news/printedition/opinion/la-000001978jan09.story.