

National Identification Schemes (NIDS) and the Fight against Terrorism: Frequently Asked Questions

This set of Frequently Asked Questions (FAQ) provides background on why NIDS are an unsuitable measure to increase security against terrorist attacks.

Authors:

- **Andrew Clement**, Professor, Faculty of Information Studies, University of Toronto
- **Felix Stalder**, Director, Openflows; Post-doc Surveillance Project, Queen's University
- **Jeff Johnson**, Computer Professionals for Social Responsibility (CPSR), UI Wizards, Inc.
- **Robert Guerra**, Board Member, CPSR
- Additional Contributors: **Ian Bicking**, **L. Jean Camp**, **Paul Czyzewski**, **Harry Hochheiser**, **Lenny Siegel**

Status: v1.2 (27.11.2001)

([Jeff Johnson's Analysis](#)) [[Cal. Judiciary Summary](#)] [[Related Links](#)]

Introduction

The terrorist attacks of September 11, 2001 on the World Trade Center and the Pentagon have restarted public debate about National Identification Schemes (NIDS) in the US, Canada, and other countries. The extraordinary ferocity of the attacks seems to demand extraordinary measures of protection. However, none of the proposed NIDS clearly states which problem it tries to solve and how exactly it contributes to reducing the danger of terrorism.

This set of Frequently Asked Questions (FAQ) provides background on why NIDS are an unsuitable measure to increase security against terrorist attacks.

In brief, we question that NIDS can provide additional security against terrorist attacks like those that occurred in New York City and Washington. However, they do endanger our civil liberties. Even more, by relying on the wrong approach to security, NIDS may actually create a false sense of security that leaves us more vulnerable than before.

Questions Answered (below)

1. [What is a national identification scheme \(NIDS\)?](#)
2. [How does a NIDS work?](#)
3. [Would a NIDS have prevented the Sept. 11 attacks?](#)
4. [Would the use of biometric data increase security?](#)
5. [How secure is a high-tech ID card?](#)
6. [Is there a trade-off between civil liberties and security with NIDS?](#)
7. [How would a NIDS threaten civil liberties?](#)
8. [OK, NIDS are not perfect, but don't they at least improve security somewhat?](#)
9. [Wouldn't a voluntary NIDS improve security while preserving civil liberties?](#)
10. [Who wants NIDS, and why?](#)
11. [What public support is there for NIDS?](#)

12. How can NIDS proposals be stopped?

13. What questions should be posed to NIDS proponents?

1. What is a national identification scheme (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, social security registration, immigration documents, and other government-issued identification. Until recently, NIDS have not 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 possible use of NIDS.

NIDS can either be mandatory or voluntary. In a mandatory scheme, everyone is required to carry and present a card when asked; not doing so is an offense. 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.

2. How does a NIDS work?

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 which, 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, such as finger prints or retina scans.

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 card 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 can also be a third process, data-matching. This occurs whenever 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.

3. Would a NIDS have prevented the Sept. 11 attacks?

The overwhelming majority of the hijackers were in the US legally and had no record 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.

A NIDS offers no 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).

4. Would the use of biometric data increase security?

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. 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.

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. All biometrics help to do is to make sure that the cardholder is really the person identified by the card and, if they are checked against a central database, then biometrics can ensure that a person does not hold more than one card.

However, biometric data cannot ensure that the information the person presents when obtaining the card is correct.

5. How secure is a high-tech ID card?

This depends widely on the specifics of the system, but no system can ever be 100% secure. While smart cards are among the most secure technologies available, virtually all existing smart card systems have been compromised. Leading security experts point out that as more and more smart cards are put into operation, more and more people know how to break them.

If the card is used to check the information against a central 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 system might 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 a thousands of people, hundreds of organizations and dozens technologies. Each of these elements introduces a specific set of vulnerabilities. Securing the entire system against attacks and abuses will be close to impossible.

6. Is there a trade-off between civil liberties and security with NIDS?

NIDS would allow individuals to be easily tracked. However, knowing the identity of people will not prevent crime. If the identity of the person who will commit the next crime were known then prevention would be trivial: simply find the person and stop them from acting. However, since crime and acts of terror cannot be predicted, being able to track individuals will not increase security.

A NIDS would make everyone vulnerable to the problem of incorrect data in the database. If the data on the card or in the database is incorrect, then innocent people will be victimized 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 terrorism. With NIDS we compromise civil liberties without increasing security.

7. How would a NIDS threaten civil liberties?

People who are easily and constantly tracked by a central authority are not free people.

Moreover, when everyone is tracked, their associations are tracked as well. In 1965, the National Association for the Advancement of Colored People (NAACP) refused to give the State of Georgia a list of Georgia members for fear that the people listed would be harrassed or harmed. The U.S. Supreme Court backed the NAACP, arguing that we are free to associate without being tracked and watched.

The U.S. courts and Congress have repeatedly recognized that people under constant surveillance are not free.

8. O K, NIDS are not perfect, but don't they at least improve security somewhat?

Given that the systemic weakness of an NIDS are somewhat hidden, such a highly visible system might well produce a false sense of security. By relying on a security measure that is inadequate, we might end up compromising our security through a NIDS.

9. Wouldn't a voluntary NIDS improve security while preserving civil liberties?

This would be even worse than a mandatory system. First, it would make untrustworthy anyone who does not have a card. A lot of energy would be wasted checking people who are only suspects because they don't have a card. Second, less time would be spent checking people who have a card because they apparently have already been cleared.

In effect, it would make life easier for terrorists like those who committed the attacks on September 11 because they could use their ID cards while security personnel would concentrate on those without one.

This structural inefficiency of a voluntary system would create great pressure to make it mandatory over time.

10. Who wants NIDS, and why?

Two groups have been pushing for NIDS for a long time and are now using the war against terrorism to advance their agenda.

The law enforcement community would like a tool to make it easier to identify people on routine checks and to link their databases by using the national ID card as a unique identifier. This has little to do with the fight against terrorism but a lot with expansion of police powers.

Smart-card identification schemes have also been promoted by large information technology vendors. For them, a multi-billion system would be a great business opportunity. The most prominent promoters of the current wave of NIDS in the US have been Scott McNealy, CEO of Sun Microsystems, and Larry Ellison, CEO of Oracle. Both have been peddling their company's products as the basis for the NIDS. While they offered their products for free, the ensuing service contracts would make their "gifts" highly profitable.

Both of these groups stand to benefit from a NIDS even if it does not improve our security against terrorists. So far, failures of proposed smart card NIDS greatly exceed successful implementations.

11. What public support is there for NIDS?

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.

However, in the wake of the September attacks, there are signs of a shift in public attitudes in favor of NIDS. On October 6, 2001, the 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".

However, there has been no public explanation of how such a scheme would work, so one must presume that this support reflects a general assumption that a NIDS would provide protection against another attack like that of September 11.

This apparent public support would presumably be much weaker if people knew that a NIDS would not be effective for preventing terrorism.

12. How can NIDS proposals be stopped?

Because NIDS proposals are based on unfounded premises, they are very vulnerable to public scrutiny. David Parnas and others in CPSR were effective in blunting the SDI proposal by concentrating public attention on the unsupportable claims about the effectiveness of the system. A similar approach could be taken with NIDS. It is quite likely the widespread suspicion of these schemes will return when the dubious advantages and numerous pitfalls are more widely known.

13. What questions should be posed to NIDS proponents?

Given the failures of the security apparatus to protect against the recent attack and the dubious claims made for NIDS, the burden is on proponents to show why they are worth pursuing. Here are some questions to ask of proponents:

- What do we know about the security failures on September 11?
- How would the proposed NIDS be effective against them?
- How would a NIDS catch terrorists that are in the country legally and have no criminal record?
- How much would the implementation of a NIDS cost?
- Couldn't this money be spent more effectively?
- Under your proposed NIDS, how common would misidentifications occur and how would they affect throughput at security checkpoints?
- What alternatives to a NIDS have been considered that would be less threatening to civil liberties?
- What impact would the NIDS have on everyday activities?
- What measures have been considered that would mitigate the privacy and other civil liberty losses?

**This document was found @ <http://www.cpsr.org/issues/privacy/natidfaq>