Public Attitudes towards a National Identity "Smart Card:" Privacy and Security Concerns

Starr Roxanne Hiltz Hyo-Joo Han Vladimir Briller
roxanne.hiltz@worldnet.att.net *hxh8518@njit.edu* *vladimir.briller@njit.edu*
Department of Information Systems, College of Computing Sciences
New Jersey Institute of Technology, University Heights, Newark, NJ 07102

Abstract

Tracking technologies use pervasive information systems to scan and record the location of individuals and to transfer information about them to and from a central database. One potential application is a "smart" national identity card (NID). National polls have shown a strong majority of Americans favor an NID in recent months. This study uses a telephone poll with 400 respondents and semi-structured interviews with 29 New Jersey adults to explore in depth the concerns and opinions that explain the "surface" opinion that is elicited with a single question. The results indicate that most people actually have very mixed feelings, with strong reservations about privacy and civil rights implications and also the security of the information on the card itself from theft or misuse.

1. Introduction

Pervasive tracking devices contain a chip with unique personal identifying information, are read by scanning devices, and the information thus obtained may be stored in a centralized data base for later retrieval. The chip is often embedded in something that usually has another purpose, such as a mobile telephone with Global Positioning System (GPS) tracking; an EZ- Pass transponder on the windshield of a car, used for automatic toll collection in states from West Virginia to Massachusetts; or a possible "national identity smart card." The scanning device may be built into a walkway, a roadway, or a hand-held "wand." The information could be stored only temporarily and used only for billing or similar transactions. For example, EZ-Pass data might be kept only for 60 days past a billing date, and never stored longer or used for any other purpose, such as identifying people who speed through the toll plazas; or the data could potentially be kept for years and used for a variety of purposes, such as trying to track the movements of criminal suspects.

Such devices raise issues for users and potential users, related to the tradeoff among concerns for security, privacy, and convenience. As part of a five year program of research for the New Jersey Center for Pervasive Information Technology, a joint undertaking of Princeton University, Rutgers University, and New Jersey Institute of Technology, a team at NJIT is studying acceptance and potential impacts of a variety of possible pervasive tracking devices. This paper describes a study of the attitudes of New Jersey residents towards a possible National ID "smart card," based on both a telephone survey of a sample of 400 households, and 29 semi-structured interviews that explored attitudes in depth.

2. Background on the issue of a National ID "smart card."

National identity schemes are used in over 100 nations, and may combine the functions of social security cards, driver's licenses, immigration documents, and other identification documents. In recently proposed versions, the national ID card or device would be a "smart" one containing a microchip that stores and accesses information, probably including biometric data about the person, such as fingerprints or retina scans. People would be required to have the card scanned in specific circumstances, such as when boarding an airplane or when stopped by the police. At that point, "authentication" would take place, as the information on the card is compared with the person, e.g., a live finger scan with a fingerprint recorded on the card. If there is a match, the card would be linked to a database to record the location and time of the scan (this is the "tracking") and to determine whether there is anything on file that raises suspicion about the cardholder (There could also be a process of data matching, in which information in the database is compared to other databases in order to build more information about the person.)[1]. Almost from the day the planes hit the World Trade Center and the Pentagon, members of Congress, security experts and

high-tech executives such as Oracle's Larry Ellison, have endorsed the idea of some new form of identification system as a critical weapon in the fight against terrorism. Many people believe the cards, linked to comprehensive national databases, would be invaluable in preventing terrorists from operating under assumed names and identities. A number of national polls following 9-11 showed that about 70% of the American public expressed support for the idea of a National ID card for the U.S. [6]. More recent polls show much more evenly split opinions among Americans. Civil liberties groups have raised alarms about national identity cards on the grounds that they could substantially increase police power and would greatly facilitate information sharing among government agencies [8].

Identity cards have existed in Hong Kong, for instance, for half a century, but digital technology is now greatly expanding the uses of such a card --- making it a potentially indispensable tool of daily life, but also raising fears about privacy and the use of personal data. Hong Kong's previous National ID Card was a laminated card that looks like a driver's license and includes a photo, biographical data and the cardholder's residency status. But the chip embedded in the new "smart" card has room for much additional information, including medical and financial data and driving records [4]. Likewise, the U.S. military has adopted a smart ID card that tracks each soldier through the "doorways he passes through, the computer he accesses, the doctor he sees…" [6]. The Immigration and Naturalization Service already has a voluntary biometric ID system, INSPASS, which is intended to allow its holders to move through border checkpoints quickly.

There are many technical issues to be solved in order for such a scheme to reliable and secure. For example, Neumann and Weinstein, in the "Inside Risks" column of the Communications of the ACM [5] note, "The belief that "smart" NID cards could provide irrefutable biometric matches without false positives and negatives is fallacious. Also, such systems will still be cracked, and the criminals and terrorists we're most concerned about will find ways to exploit them, using the false sense of security that the cards provide to their own advantage -- making us actually less secure as a result!" Such issues need to be kept in mind, but are not the focus of this study.

What this study is concerned with is going beyond the simple "one question" type national polls that find that people are "in favor" or "opposed" to such a scheme, by obtaining much more detailed and in depth thinking of the public about the issues involved with any tracking device, and specifically with a possible National ID smart card. What kind of information is the public willing to have included if there were to be such a card, and when do they think it should or should not be required to be shown? What are the advantages and disadvantages perceived about such a technology? And most importantly, how does opinion about such a device relate to the strength of general concerns about privacy and about security?

3. Privacy and Computer Technology

There is a long history in America of concern about invasion of privacy, especially as it relates to new technologies and business practices. For instance, consider the following statement:

> "Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual…the "right to be let alone." Instantaneous photographs and newspaper enterprise have invaded the sacred precinct of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."

This reads like an editorial in a current newspaper, and certainly applies to new pervasive tracking technologies; but it appeared in an 1890 edition of the Harvard Law Review, written by Samuel Warren and Louis Brandeis [10]. The phrase "the right to privacy" stems from this article and has become so well known that many educated people believe it was granted in the Bill of Rights of the United States Constitution. In fact, not only doesn't the phrase appear in the Bill of Rights, but the word "privacy" does not even appear in the U.S. Constitution [2].

In a 1974 article, Richard B. Parker defines privacy in a manner that is much more precise in terms of how pervasive tracking devices violate this perceived, though not constitutionally protected, right, based on who can "sense" us:

> Control over when and by whom the various parts of us can be sensed by others. By "sensed," is meant simply seen, heard, touched, smelled, or tasted. By "parts of us," is meant the parts of our bodies, our voices, and the products of our bodies. "Parts of us" also includes objects very closely associated with us [7].

Louis Brandeis wrote in his famous dissent to the 1928 Olmstead v. U.S. case, that privacy is our most valued entitlement; as a means of safeguarding privacy, every government intrusion upon it must be condemned. We

will see that this kind of thinking is prevalent among New Jersey citizens interviewed about the possible introduction of a smart national ID card; but concerns about security, in the wake of 9-11, are also very salient.

Scholars who have examined the issues of computers and privacy have been most concerned with two areas: databanks and the Internet. For example, in Privacy *and the Computer: Why We Need Privacy in the Information Society*, Lucas D. Introna makes reference to a 1971 survey by the Royal Commission on Privacy. More than 90% of those surveyed felt that a national databank was the most disturbing example of the government intruding upon the individual's right to privacy [3]. A "smart" NID that tracked and recorded location frequently would obviously result in extreme intrusions into personal privacy.

Citing a Harris Poll that showed that approximately 2/3 of Internet consumers consider privacy violations a serious matter, Wang, Lee and Want [9] describe some of the violations that are primarily feared by online users, including: improper monitoring (surveillance of consumer's Internet activity without his knowledge or permission (tracking sites visited); and improper storage (storing customer information in a non-secure manner, potentially (permitting outsider access to information). Each of these concerns would only be magnified by a smart NID with tracking and a database.

4. Research Methods

4.1. The Sample Survey

The topic of this survey was technology and security. The first author designed some of the questions. This survey was conducted on behalf of New Jersey Institute of Technology (NJIT) by Global Strategy Group, Inc., between January 20 and 22, 2002, among 400 New Jersey adults. It used Random Digit Dialing (RDD), from a list of residential phone numbers. Because women and older people tend to answer phones, the introduction is randomized to ask for the oldest/youngest male/female over the age of 18 in the household, in alternate calls. There was a three-callback minimum (up to 16 callbacks), to increase the chances of including the harder-to-reach. The number of interviews conducted in the north, central, and south regions of the state was established by a quota and based on census population figures in New Jersey counties. The respondents were 52% female and 16% non-white. Estimated sampling error is plus-or-minus 4.9%. Note that overall, 67% of New Jersey adults in this poll thought that requiring a National Identity card is an excellent or "very good" idea; this is similar to results for national polls.

4.2. The semi-structured interviews

The questions in the interview guide first probe initial knowledge and attitudes about a "smart" National ID card. Then, a short "tutorial" type of explanation of what the "smart card" might contain and how it would work is given, since it was observed in pilot studies that many people had only a very vague idea about what was meant by a "national identity smart card." (This explanation is included in the Appendix). This was followed by a set of open-ended questions, most of which are provided in Section 6 on results of the interviews. Interviewers were instructed to be sure to cover all of the listed topics, but to also use extensive probing to draw out the opinions of respondents and the reasons for them. It was designed by the first author, and modified based on pilot interviews.

All of the interviews were conducted and transcribed by students in the CIS 350 Computers and Society class at NJIT, as one of the available term project choices. The interviews were then coded using NVivo qualitative analysis software. A rough "quota" sampling guideline was used. Each student interviewed four people. At least two were supposed to be over 25, and not students. They were to try to include two males and two females, and to obtain as many of the interviews as far away from NJIT and Newark as possible, to spread the interviews around the state. This is a small, non-random sample designed to explore the reasons for opinions, not to estimate the proportions of people who hold certain opinions.

The 29 interviewees average 33.6 years age, and all are U.S. citizens. Seven were identified as female, nineteen as male, and the gender of three was not recorded. The racial makeup of the group is not typical of the USA at large, but does reflect New Jersey's diverse population: 41.4% White, 31.0% African-American, 24.1% Asian, and 3.4% Hispanic. The occupational pattern is highly skewed toward the professions: only two homemakers are included, along with one retired person. The groups most over represented are students and educated professionals, especially in the computer-related fields.

In this paper, some highlights of the results of the telephone survey will be presented, and excerpts from the semi-structured interviews will be used to illustrate the kinds of thinking that underlie the different points of view about the desirability of a National ID smart card.

5. Correlates of Support for a National ID

After beginning with explicit questions about the effects of September 11 on concerns about terrorism and concerns about different kinds of threats to security (such as computer viruses and violent crime, as well as terrorism), respondents to the telephone survey were asked: "For each of the following ideas to promote safety and security, please tell me if you think it is an excellent

idea, a good idea, only a fair idea or a poor idea for promoting safety and security." The dependent variable of interest in the telephone survey is degree of support for a National ID card, as measured by the item below, shown with frequency distribution of the answers:

Require national identity cards
33% Excellent idea
34% Good idea **67% Net Excellent/Good idea**
16% Only a fair idea
15% Poor idea **31% Net Only a fair/Poor idea**
2% Don't know/Refused

The other 54 questions from the telephone survey were used for a factor analysis (oblique solution primary pattern matrix) and produced a total of 15 factors. The major factor loadings of items on the first and strongest factor (larger than 0.60) are shown below; all of these items come from the same section of the questionnaire. This factor can be considered to measure support for government monitoring and tracking vs. concern for privacy issues.

Factor 1. Government monitoring vs. privacy concerns

22. Require everyone in the United States to submit DNA, either through a hair or blood sample (0.677).
23. Make it easier for the government to wiretap phone lines (0.759).
24. Make it easier for the government to listen in on cellular phone conversations (0.703).
25. Allow government security agencies more access to individual's e-mail (0.698).
27. Increase the use of computer programs that create profiles of people considered a risk based on their behavior, including those who travel to unfriendly countries or use cash for purchases of things such as airline tickets or cars (0.651).
28. Allow government security agencies to compile a database on individual Americans based on their participation in groups or organizations that are believed to support criminal or terrorist activities (0.691).

The Pearson's correlation coefficient between this monitoring factor and support for a national ID card is 0.463, significant at the 0.001 level. In other words, support for a national ID card is related to support for many other government activities that would monitor Americans much more closely and keep a national database not only on individuals, but also on groups.

Surprisingly, there were no other correlations with support for a national ID card that were stronger than 0.10; anything smaller is substantively insignificant, even if it is statistically significant. In other words, many other types of variables, which might be presumed to be related to support for a national ID, actually were not, including demographic factors such as age or gender, life style factors such as use of the Internet, and questions or factors measuring degree of security concerns.

6. Concerns about a National ID Card: Results of the Semi-Structured Interviews

This brings us to the key question: why are some people concerned about potential government abuse of tracking/monitoring information, while others are not? And are there "limits" or "lines that should not be crossed" in government surveillance with devices such as a National ID card? The semi-structured interviews, conducted from February through April of 2002, were designed to explore these issues in more depth.

6.1. Level of Knowledge

Most people did not have a very good idea of how a National ID smart card might work. Here are a few of the responses to the question, "What have you heard about or read about in terms of what you think a national identity card would contain, and how it would work?" The following are sample comments from some of the respondents.

> *Actually, I don't know too much about it, except that it would be...uh... like have a memory on it I guess. Like similar to a credit card.*

> *Well, I heard that it was supposed to be an identification that would contain all about the individual. But I'm not sure of the information that would be contained in the card.*

> *And do you know how it would work?*

> *No, actually I don't know. But the only thing I heard was that it would look like a credit card. I heard that the military uses that.*

6.2. Opinions behind the opinions: acceptance of a National ID card

Respondents were asked, "Before we start discussing the possible nature and uses of such a card in detail, how would you say you now feel, off the top of your head, about a law requiring its use in the United States: On balance do you support or oppose the introduction of a national identity card scheme? "

A slight majority of respondents in these interviews indicated some support for such an idea, many

mentioning its apparent usefulness in combating terrorism and increasing security, but usually there were mixed feelings expressed, whether they said that overall they were in favor or opposed or undecided. Most of the reasons and explanations given relate to reservations about and discomfort with the idea of such a card. For example:

> *I don't oppose it but I don't feel comfortable about it. I'm not for it, I should say. I don't want it to contain my personal information and I'd like my privacy. I don't want someone to be able to swipe a card and find out about my whole entire life.*
>
> *I have both views i.e. I support and at the same time oppose the introduction of this ID card… In view of the incidents of September 11 and the fact that I got directly affected, on one hand, I would say that maybe if we had these cards before, maybe we could have identified these people before and prevented the incident. So on this basis I support the introduction of the ID card. On the other hand is the issue of privacy. How far do you go? How much information should be there on that card? What if it fell into the wrong hands? There are people who go through the hassle of their identity being stolen, like their credit cards etc. Now, this card would have even more information. So from this respect, I oppose this ID card.*

6.2.1.Perceived Disadvantages. When asked about the major disadvantages of the NID, the most frequently voiced concerns were about privacy, both in terms of "criminals" or unauthorized persons getting access to the information on the card in some manner, and also concern about government abuse:

> *I just see all your rights being taken away and basically your freedom of moving will be hindered.*
>
> *It would be like the X-files, where we would all be born with a little computer chip that can track us. Its like some biological study, we are all going to be tracked, tagged. See who goes where, I don't like it.*
>
> *It's definitely taking away from your privacy. It's like all of your life is on one computer chip. It's not really fair. It's dehumanizing people.*
>
> *Probably the privacy issue. What if it fell into the wrong hands? Similar to credit card theft. Even though online stores offer secure sites, there are still ID thefts occurring. So if it fell into the wrong hands, it would be too much information about you. Not necessarily a thief, but the government. I support the US government to a point. They take care of things like keeping the citizens safe with law enforcement. But at the same time it can be used against citizens. No government is above that. So the disadvantage is mainly privacy issue.*

An African-American interviewee expresses particular concern about abuse of the information by law enforcement officials who might engage in new kinds of profiling:

> *I think it would lead to, not that we don't already have these problems, but I think it would lead to selective enforcement of random stop laws and you know selective punishment… I think a lot of people would be profiled for whatever reason, and I would especially be concerned if all or most of law enforcement had access to that information. You know could they could use it to whatever end they wanted and we might not always be able to monitor that…Who's going to monitor the people who have access to all that information, how they use it?*
>
> *What if you go somewhere without your ID? Does that mean you're a bad guy or a terrorist? Would you be in trouble or harassed by police? Sometimes we forget!*

Several interviewees also mentioned doubts that the technology available today could really make a NID secure against "faking" by organized criminals:

> *I mean ok, there is the whole domestic terrorism thing, but the fact is any card can be faked. You can get a fake one, just like you can get a fake passport or fake ID. So if you have someone who is going to suicide bomb themselves, I don't think that is going to stop that. I don't really see any benefits.*

6.2.2. Perceived Advantages. The most frequently mentioned advantage was as a tool in decreasing terrorism.

> *I think it would make things a lot safer for people.*
>
> *I think it would do a lot to preventing terrorist activity like you saw on September 11… Security has been so bad in this country that I think that it would do a lot, to help make the United States a little more secure in terms of who is riding, taking planes or who is coming in and out of the country, who is getting access to areas, places that they shouldn't be.*

The second most frequently mentioned potential advantage is convenience, in terms of needing only one document for all identification purposes:

> *I guess it would cut down on what you would have to carry on your person for identification purposes. This card would be all of this wrapped into one. Information like driver's license, passport etc. could be stored on this. So for simple everyday things like cashing a check, renting a car, going into a store where you would need identification, traveling abroad, this card would be useful.*

The third most frequently mentioned advantage is in terms of cutting down on identity theft or other kinds of crimes or illegal activities, including illegal immigrants:

> *In this case, I think it would cut down on a lot of theft mainly Identification theft. Everyone's thumbprint and retina is unique. So it would cut down on ID theft and other possible crimes.*
>
> *I think it would be good for tracking any kind of people that have a criminal record, sex offenders.*
>
> *(We could) catch more illegal immigrants floating around.*

6.3. What should be included on an NID?

A checklist was supplied in terms of what sorts of information a NID should contain, if it is implemented, and comments were solicited, especially for those who opposed a particular type of information. The results are summarized in Table 1.

Table 1. What should be included on an NID?

	Willing	Not willing	Don't know
Date of birth	26	3	0
Photograph	28	1	0
Fingerprint	23	4	2
Eye scan	18	8	3
DNA details	12	15	2
Criminal records	21	7	1
Religion	9	19	1
Medical history	12	6	0

Note that religion stands out, as something that it is felt is "none of anybody's business." Some of the strong comments against including religious affiliation include the following:

> *That might just be used as a tool to discriminate against folks.*
>
> *Because it's against the constitution of the United States. We have a freedom of religion and that shouldn't be public display on any card, it's your free will.*
>
> *I don't think this is anybody's business. It's a personal freedom to have religion or not.*

DNA details are also thought to be "too personal" by many people. There is a real distinction drawn between the "traditional" biometric identifier, the fingerprint, and DNA, which is considered to be something that is "inside" of you. Although eye scans are also "new," they are not felt to be so intrusive.

The medical history question was not included in the first round of interviews, but was added subsequently because it was spontaneously mentioned by several interviewees, as something they thought would be useful to include.

6.4. When should use of an NID be required?

Table 2 summarizes feelings about the circumstances under which one should have to produce a NID for scanning, should it be implemented:

Table 2. When should Use of an NID be required?

	Favor	Oppose	Don't know
To enter an airport	27	2	0
To get a driver's license	22	7	0
To buy a gun	24	5	0
To take a train	13	10	5
To go through a tunnel	8	13	7
To obtain hospital care	9	16	4
To enter the U.S. from abroad	23	2	4
To make a cash withdrawal from an ATM	12	15	2
Whenever you are stopped by the police, e.g., for a traffic violation	15	10	4

Being required to have a NID scanned, if it is to be implemented, is strongly supported for uses that clearly relate to issues of national security in most respondents' minds, such as entering an airport, buying a gun, or getting a driver's license. (The ability of 9-11 terrorists to obtain drivers licenses illegally has received much publicity.) There is considerable disagreement about other kinds of uses, with most feeling that scans for tunnels or trains or ATM's would cause unacceptable delays and

inconvenience. By contrast, use to obtain hospital care was opposed because most people felt that anybody who needs it should be able to obtain hospital care in an emergency, regardless of whether they are illegal immigrants or not.

6.5. How About an Implanted Chip?

From a purely "rational" point of view, it would make sense to implant a small chip under the skin, rather than have it on a card that can easily be lost. However, for most respondents (18 against, 5 willing), this is "going too far" in the direction of dehumanization. Below are some of the statements expressing opinions against an implanted chip:

> *I don't want anything like that in my body right now.*
>
> *To me it's taking it beyond to a sci-fi level with the chip implantation.*
>
> *Because like I said that's dehumanizing people. If you have a card, OK, you could take the card with you. If they're putting something inside of you, that's like you're changing yourself. It's not right.*
>
> *I would rather have the card because I could ditch the card and I wouldn't have to scoop this chip out of me wherever it would be hidden.*
> *(Interviewer: I will take that as a definite unwilling.)*
> *Subject: Unwilling, yes. And thank god the ACLU is still alive.*

7. Summary and Conclusions

When asked, most New Jersey residents are currently willing to have a national Identity card scheme that would be required for actions such as taking an airplane which raise national security issues. Support for a NID "smart card" is strongly related to support for other government measures that would track "suspicious" people and groups. However, when discussing such a possibility in some depth, they mention more possible disadvantages and concerns than advantages. They are concerned about loss of privacy, abuse of the information on the card, and the security of the technology itself. They are particularly opposed to implementations that would invade what they perceive as their "personal" sphere, such as the inclusion of information about religious preference or the implantation of a chip in their body rather than on a card that is carried.

Almost everybody feels that "something" has to be done to obtain more secure identification than the current driver's license or social security number. However, if a national ID with biometric identifiers is to be implemented, the concerns expressed by the interviewees will have to be addressed in order for it to obtain and retain a strong majority of supporters.

This is an exploratory study with many limitations. In particular, the semi-structured interviews were conducted with a small, non-representative sample at a particular point in time and in one state. New Jersey was especially directly affected by the events of 9-11; most people know someone who died or was injured when the World Trade Center collapsed. In order to generalize the results, much more additional data would be needed.

Acknowledgments

The section on computer technology and privacy is adapted from a paper by Bruce Jay Forman [2]. The following students participated in conducting and transcribing the interviews, and contributed to the analysis: Rajakumar Despande, Kim Consolino, Ajay Deshpande, Kritika Iyer, Goce Mitovski, Andrea Noble, Emmanuel Oyatunde, Greg Picaro, Angella Royer, and Kotaro Tsujiuchi. Coding was done by Hyo-Joo Han, Kim Consolino, and Jonas Javier. Hyo-Joo Han had primary responsibility for the analysis of the coded interviews. James DeLorey supervised the telephone survey conducted by Global Strategy Groups, Inc. and was most cooperative in supplying the data and methodological details; Vladimir Briller carried out the statistical analysis of the telephone survey data.

References

[1] Clement, A., Stalder, F., and 7 others, (2002) "National identification schemes (NIDS) and the fight against terrorism: Frequently asked questions," http://www.cpsr.org/program/natlID/natlIDfaq.html

[2] Forman, Bruce. A question of balance: Privacy America. Unpublished draft Ph.D. thesis, NJIT, 2002.

[3] Introna, Lucas D., Privacy and the Computer: Why We Need Privacy in the Information Society, Metaphilosophy, Vol. 28, No. 3, July 1997, pps 259-275

[4] Landler, M., (2002) "Fine Tuning for Privacy, Hong Kong Plans Digital ID" The New York Times, February 18, 2002. http://www.nytimes.com

[5] Neumann, P.G. and Weinstein, L., (2001) "Risks of National Identity Cards", Inside Risks 138, Communications of the ACM 44(12), December 2001. http://www.csl.sri.com/users/nermann/insiderisks.html

[6] O' Harrow, R. Jr. and Krim, J., (2001) "National ID Card Gaining Support," Washington Post, December 17, 2001, p A01.

[7] Parker, Richard B., A Definition of Privacy, Rutgers Law Review, Vol. 27, 1974, pps 275-29

[8] Scheeres, J., (2001) "ID cards Are de Rigueur Worldwide," Wired News, Sept. 25, 2001. http://www.wired.com

[9] Wang, Huaiqing, Lee, Matthew K.O., Want, Chen, Consumer Privacy Concerns About Internet Marketing, CACM, Vol. 41, No. 3, March 1998

[10] Warren, Samuel D. and Brandeis, Louis D., The Right to Privacy, Harvard Law Review, Vol. IV, No. 5, Dec. 15, 1890, pps 193-220.

Appendix

Below is the explanation of a "smart" National Identification Card that was provided to interviewees in the semi-structured interviews. Changes in wording of such explanations would be expected to affect the nature of the opinions expressed about a NID.

There are national identity card schemes in many different countries, and of course there are many possibilities for the information it would contain and the circumstances under which it would be required to be displayed or scanned. Let us assume the following, form, which is similar to that being discussed in the press recently. Suppose it is a device the size of a credit card, only a little thicker, because it contains a computer chip. Let us assume it contains

A digital photograph,

A digitized version of a unique biometric identifier (such as your thumb print or a scan of your eyes),

Some other stored data,

Plus the ability to transfer information to and from computerized scanning devices and a national database.

Let us also assume that at a minimum, the information stored includes your name, address, citizenship, date of birth, and social security number. Third, let us assume that in order to board an airplane, get a drivers license, or enter any secure area, you would have to present the card plus scan the part of your body that was recorded for the biometric identifier, such as your thumb or your hand.