

# 4

## **National Identification Smart Cards: Implications of a Mandatory Implementation**

Derrick D. Dickey and Bader Al-Hinai

### **Introduction**

Behind Winston's back the voice from the telescreen was still babbling away about pig-iron and the overfullfillment of the Ninth Three-Year Plan. The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it, moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized (Orwell, pg 1).

This scenario from George Orwell's novel *1984* is a disturbing look into what the future may hold. The concept of Thought Police and round-the-clock surveillance is detrimental to the privacy and liberty that we enjoy. The potential for such horrors may not be far off. In the above passage by George Orwell, replace "telescreen" with "smart card" and our worst privacy and liberty apprehensions become reality. The technology is available, and with geopolitical events steering societies to reduce privacy for the sake of security, never in the history

of the world has the opportunity been ripe for the implementation of such a system.

In the near future, probably within our lifetimes, we will see the implementation of National Identification (ID) cards in the form of smart cards. These Identification cards will be much more comprehensive than the current ID system used in America. The smart card will contain driver's license information, social security number, and a personal data sheet. It will also function as a credit card as well as a debit or check card. In addition, smart cards will store your membership data and provide you with security clearance depending on your occupational situation. Insurance information, medical records, and shopping preferences are also included to save time and improve service at restaurants and retailers. "Smartcards could let citizens participate in electronic voting, gain access to their health records, complete tax returns and claim benefits. At the same time, the ability of such cards to reduce online fraud would also serve to drive e-commerce" (A Sense of Identity, 2002). Finally, retinal imaging and fingerprint data would be stored on the card to authenticate the user.

Imagine carrying all of this information on a single card in a wallet. At which point most people ask, why store all of that data? What purpose does it serve? What impact does this National ID card have on the privacy of the individual? For our initial purposes, let us examine a more practical version of the National ID card.

If a National ID were implemented, the ID card would be mandatory and government issued. This means that it will include information important to the government and its various agents such as law enforcement and healthcare providers. The ID card would contain driver's license, passport, social security number, insurance information, and medical records. For authentication purposes, your retinal image and fingerprints will also be included. From this point forward, this is the model used in this reading when referring to National ID cards.

The clash of technological advances and societal norms has never been more prevalent than now, especially evident in the field of Biometrics. The field itself is not a new scientific avenue, but rather it has grown to take on a new meaning and area of study. Due to this shift in meaning and the wide array of applications associated with it, the following working definitions will suffice for our understanding. The International Biometrics Group defines biometrics as, "The automated use of physiological or behavioral characteristics to determine or verify identity." The Texas A & M department of Statistics defines biometrics as "the emerging field of technology devoted to the identification of individuals using biological traits, such as those based on retinal or iris scanning, fingerprints, or face recognition." As technology advances and security and privacy concerns continue to rise, biometrics will become a topic of debate among the laypeople.

A smart card is defined as, "a small electronic device about the size of a credit card that contains electronic memory, and possibly an embedded integrated circuit" (Smart Card Definition, n.d.). Smart cards are currently being used in a variety of scenarios around the world. A familiar use is inside your cellular phone. Smart cards, or subscriber identity module (SIM) chips as they are often called, store data that tells

the provider that the phone making the call belongs to owner X and records their activity, which is then reported back to the provider. In England and Australia, smart cards are being used as train passes and are scheduled to completely replace paper tickets. "London Underground (LU) has embarked on a GBP 1.2 [billion] smart ticketing project that will be rolled out to the Tube's 350,000 annual season ticket holders next year, and may also add banking services and loyalty schemes" (Tudor, 2002). Currently, paper season tickets no longer exist in London. Credit card companies are also readily adapting the smart card concept by enabling users to protect their credit by storing special authorization information that often requires the use of biometrics for authentication.

The topic of National ID cards has been broached by a large number of governments around the world and, in some cases, is in the process of being implemented. What does it mean for a government to issue mandatory National ID cards? If we look at American society this concept is already in place. Nearly everyone has a driver's license, state identification card, or at the very least a social security card. Very seldom does anyone think of this policy as the passive implementation of a National ID card system. The system is reinforced by a variety of non-government agencies within the nation. When you apply for a job, credit, or savings account, identification, possibly in multiple forms, are required. Without formally issuing a mandate, the government has established a mandatory identification system. On a much larger scale, a passport functions as an international identification card. When traveling abroad, an individual's identity is subject to confirmation at any point in time.

Before a National ID can be issued, it is necessary to examine the privacy concerns raised by the nature of the technology as well as the concerns of citizens. What impact will the National ID card have on the individual's privacy? The evolution of the social security card demonstrates the need for concern. The original purpose of the social security number was to allow the federal government to track individuals' earnings and determine how much to deduct and place into the social security fund. Since its inception, the social security number has strayed far from its original goal. Social security numbers have now become attached to almost any important record in a citizen's life. They are used for everything from job applications, to student numbers at universities, to e-banking verification. These corollary uses do nothing more than distribute your unique identifier to the world. This chain of events should generate concern. As the comprehensiveness of the National ID card grows with time, the greater the opportunity for exploitation and the escape from strict standards of usage.

It is also necessary to examine the ethical considerations involved with a mandatory National ID card. When examining a large population group, ends-based ethical thinking is most appropriate "End-based thinking, known to philosophers as utilitarianism, is best known by the maxim Do whatever produces the greatest good for the greatest number." (Kidder, 1996) The typical approach to this is a cost-benefit style analysis. The driving force behind the National ID smart card is to increase National security due to recent terrorist activity

around the world. In order to increase security, it is imperative that authorities have access to files of any individual at a moment's notice. At any given time, authorities could be viewing your ID card contents, mining data to "improve your life." There would be no problems if authorities could be trusted to use data only for its proper and legal intents and purposes. However, over time, as more individuals view your information, the chance of it being misused increases. It is necessary to balance the prospective breach against the potential for loss of life or lives saved.

From a technology standpoint, the attitude towards smart cards is much less negative. Smart cards were designed to store encrypted data. They can also be secured using a lock and key methodology using retinal image scanning and fingerprint scans, as well as through standard data encryption techniques. Fingerprints have been used for quite some time now and have developed to the point where making copies to overlay on your fingerprints will not work. Technology has advanced to a level where the actual print itself is no longer the desired goal. New advances in optics and iris scanning are improving the ability to identify individuals, by increased accuracy over longer distances and greater optical efficiency. To use the card, one of the above technologies would be put to use depending on the security level of the transaction. The user's data would remain secure, as long as the card remained with the cardholder. Even if a card were stolen, the difficulty and skill required to fool the biometric identification would be immense, but still possible.

The ability of the card to provide its own verification is promising; however, in order to take advantage of some features, other institutions will need access to the authenticated data. For Instance, when an individual goes to the bank, before a transaction can take place, the bank must verify their digital signature. This proposes the use of a centralized database for storing public records of every individual. This aspect of the smart card system provides for the greatest chance for privacy violations. The same security concerns arise that are being dealt with on a daily basis. It only takes a single hacker to tap into the database to destroy the National ID card system. It is understood that protective measures, such as encryption of sensitive data, would be taken to prevent such an attack, but as technology improves, so does counterproductive technology. Many opponents would question the need for a central database system as opposed to a distributed database system where each ID function is handled by the involved agency or business. This defeats the purpose of a comprehensive card and decreases security for the individual and the group as a whole. As more individuals access the data, the greater probability that information will leak.

In the end, the government will establish their mandatory National ID card. Before doing so, the government should focus on the needs, fears, and concerns of its citizens. The first goal of the government should be to alleviate fear about the technology itself. This will be a difficult task considering the number of individuals not born into the information age and the digital world. There will be many opponents of using the smart card because they may not understand the technology, or they are not technologically inclined. Through educating

individuals about the authentication methods being used and both the strengths and weaknesses of the cards, citizens will more readily accept the idea of putting their life on a smart card. It is very probable that the fear group will be small, in comparison to the privacy advocates. Once again, education will be the key to winning this group over. Education will help alleviate the fear of the unknown and change usually associated with new technologies. It would be in the best interest of the government not to hide any potential flaws or potential for privacy leaks. Hidden information is what fuels the advocates and protesters. Knowledge is the key to driving society forward.

### **Omani National Registration System: A Case Study for a U.S. Implementation**

Currently Oman, one of the Gulf countries in the Middle East, is implementing the National Registration System. The Omani National Identification smart card system is a revolutionary idea that will soon catch on with other nations. Currently the United Arab Emirates is working to implement a smart card National Identification system. If the international trend continues to expand, more pressure will be placed on the United States to implement such a system as well.

The Directorate General of Civil Status runs the system. The National Identification card contains a smart card chip with Public Key Infrastructure (PKI) capabilities. This provides a satisfactory level of encryption to protect the citizen's data contained on the card. Every citizen and foreigner in the country will be assigned an identification smart card, which contains an invariable and unique civil number, issued to everyone in the civil register. Omani law states:

Any Omani who is above 15 years of age shall make an application for an identity card. This shall be obligatory for males and optional for females...Every foreigner who is resident in Oman shall obtain a residence card (Directorate General of Civil Status).

This system will maintain information pertaining to: birth, marriage, divorce, death, residency, and nationality. The benefit of the electronic identification card is the ability to contain large amounts of data in a small computer chip. The identification card uses biometric recognition for authentication of the cardholder, which can be verified by portable terminals. The identification card also allows for quick and easy uploading of data into electronic government forms. The information contained in the card is as follows but not limited to civil information, biometric recognition, Drivers License information, and Passport and Visa information. In the future, information contained in the card could be banking, health, and voting information.

The objective of civil register in using a national identification card is to generate an accurate database of the Omani population. It provides accurate information about social events such as birth, marriage, divorce, and death. The Ministry also provides easy access to the system for other ministries to enhance the standard of decision-making and carry out any required studies.

Scholars and researchers have long been interested in demographic studies and census as they are of great concern to countries. They

supply information to plan future development projects. By keeping civil status records on events as birth, death, marriage, and divorce major sources of information and statistics become available to relevant centers and institutions. This includes the individual's personal information such as their place of origin, where they live, marital status, number of people in the family, and their educational, economical, and social status. It also includes relevant information pertaining to passports and driver's licenses.

As quoted above, every Omani male, 15 years of age or older must obtain one of these ID cards. This is roughly the age Americans generally acquire their first "public use" identification card; social security cards issued at birth are supposed to be private. Already some similarities exist for the rolling of a National ID smart card system in the United States. However, in Omani law there are a few provisions, allowing the public agencies to collect your information freely without repercussions. This first scenario involves the collection of data by lodging establishments. Article 49 of Omani Civil Status Law reads, "Managers of hotels and similar furnished places prepared for lodging of the general public shall enter in their records particulars included in the card of anybody who lodges at such places" (Directorate General of Civil Status). This is an interesting provision to Omani law. It allows government agencies to track the status of individuals as they move around the country or even the city for that matter. It does this indiscriminately through establishments. Uploading National Identification data profiles of citizens can be constructed based on lodging selection and purchases made while in residence of a particular lodging in a particular region, city, or lodging.

Another interesting provision in Omani law is Article 53 of Civil Status Law states that:

Any person has the right to apply for obtaining an official duplicate of the entries and documents in relation to himself or to his ascendants, descendants, or spouses... Anybody who has obtained an official copy as mentioned hereinabove shall be prohibited from using it for any purpose other than that for which it was issued... (Directorate General of Civil Status).

This provision allows for gross misconduct of identity fraud. For example, if there was a pair of identical twins, one brother could potentially acquire the proper papers of the other brother and defraud the Identification system. Granted, biometric data is kept on the electronic identification card, but if the cardholder is a twin, the data would be easier to obtain.

Considering a National ID smart card system has already been discussed in the aftermath of September 11, a push from a governing body such as the European Union would probably guarantee an implementation. As noted previously, Omani law allows potential security and privacy threats to be casually exercised. With the growing concern in America over Identity theft and e-commerce applications, a National ID smart card system would be subject to much scrutiny. On the other hand, increasing pressure to ensure National Security may be

enough to push through a mandatory smart card resolution without proper planning and provisions.

We have seen a National ID smart card system in place in Oman and the implications of its use. The system in place is much more concise than the theoretical smart card systems described at the beginning of our discussion. The Omani government has left open the opportunity for expanded capabilities of the card. When the United States implements such a system, it will likely mirror the system established in Oman. It is important to keep in mind that cultural differences and differing governing bodies exist between the two nations. In some instances, a direct comparison will not make sense. If an implementation mirroring their system were to occur, discrepancies arising from these differences would need to be addressed.

However, the bottom line still reads as a gross violation of citizen's privacy if a National ID smart card system is implemented. As freely as information travels, it seems silly to think that the government condensing your driver's license, passport, biometrics, and civil info is a violation of privacy. The difference is that this is a mandatory government program requiring the submission of this private and personal information. From a logistics standpoint, the data would need to be stored in a centralized location and maintained by the government. With a concentration of personal information such as this, the security issues are remarkable. The ease, with which hackers are able to break into systems, makes the centralization of such a large quantity of data a liability.

Hackers aside, privacy laws exist to protect citizens against the required centralized database of the National ID card system. The most notable of these laws is the Federal Privacy Act of 1974. The law regulates the collection, protection, use, and diffusion of personal information by federal government agencies (Kiefer). "Essentially, the law directs that information maintained in a system of records must be protected from unauthorized disclosure, used for stated purposes, and maintained in accurate form" (Kiefer, pg 26). In theory, the Privacy Act of 1974 should sufficiently protect Americans from dangers such as identity theft or government misuse. When we examine the National ID system in relation to this act, several concerns arise. One aspect of information security not directly spelled out in the Privacy act is the ability to hold someone accountable for failing to provide the above-mentioned protections (Kiefer). Once a citizen's information enters the centralized database, who becomes responsible for the security of the data? Liability will be difficult to place because the information will be shared freely among numerous government agencies and departments. Granted the government already has access to a good portion of citizens' information, now numerous agencies would have access to the big picture of every individual. This is enough access to create personas, habits, tendencies, and items of this nature, of every individual and "assist" their lives in any manner seen fit.

Another flag raised relates to protection from unauthorized disclosure. The National ID card system grants permissions to a large number of government organizations. The majority of those offices do not need access to all of the individual's information stored on their National ID card. Since the only way to make such a system successful

is a centralized database, cost will dictate that all agencies have complete access at all times. The cost to segregate system components outweighs any potential privacy and security benefits. The protection of our information becomes an issue of cost, which does not sit well with most people.

Even the small privacies granted by the Privacy Act of 1974 are in jeopardy with the implementation of the US Patriot Act. "The Act overrides existing state and federal privacy laws, allowing law enforcement to compel disclosure of any kind of records, including sensitive medical, educational and library borrowing records, upon the unsupported claim that they are connected with an intelligence investigation" (Nicoll, pg 29). Even more incredulous is the permissibility of black bag searches under the U.S. Patriot Act. Not only does it allow law enforcement officials to investigate American citizens for criminal matters without establishing probable cause, it also entitles them to execute black bag/secret searches without notifying the individual that is the target of the search (ACLU). Imagine the convenience for law enforcement and government officials to carry out random investigations and searches if our personal and private information is centralized in their database. Such thoughts conjure up images of Sandra Bullock in the film *The Net* and the doom foretold by Orwell in *1984*. Now we are beginning to venture towards the unethical prospects embedded in such a system.

It is not only the system itself that becomes unethical, but the approach taken by the government to secure our privacy that pushes ethical boundaries as well. Many individuals who are unfamiliar with U.S. privacy laws would welcome the implementation of a National ID system. A safe prediction would say that most Americans would welcome such a system if posed in the same manner as the US Patriot Act was proposed and passed. "A Pew Survey of Americans after the terrorism attacks shows that about 70 percent of citizens feel a national ID card is needed" (Hunt, 2002, pg 21). Spinoza addresses such an issue in his ethics as a means to an end:

If we remove a disturbance of the mind, i.e. an emotion, from the thought of an external cause, and join that disturbance of the mind to other thoughts, then the love or hatred towards the external cause, as well as the waverings of the mind that arise from these emotions, will be destroyed (Spinoza, pg 290).

However, this approach is deceitful and will only cause harm in the end, if applied to our society. Although Spinoza touches on some psychological principles, the public in our time is much more educated and would see through such a façade. If examined more closely it becomes apparent that Spinoza is getting at something more profound than the mindless diversion of subjects for personal gain. If thought of in terms of privacy of an individual's information a completely different interpretation arises. It proposes the disconcerting of the public's mind as a method for gradually removing their rights without conscious realization of the act. The National ID card system as a means to increase safety and well-being camouflages the removal of the disturbance of losing privacy. As Spinoza says, "...the waverings of the

mind that arise from these emotions, will be destroyed" (Spinoza, pg 290). Further more, by convincing Americans the U.S. Patriot Act and a National ID card system are mandatory for our well-being they are using Spinoza ethics once more as a weapon. "In so far as the mind understands all things as necessary, so far it has a greater power over the emotions, or, it suffers less from them" (Spinoza, pg 293). The government passing off a National ID card system for our safety and protection is playing on our survival instincts. When humans understand something to be necessary, they condition themselves to endure it with minimal impact.

It seems that this inborn conditioning process has already begun. The authors conducted a survey to determine attitudes on a National ID card system and its impacts on the lives of individual citizens. It was a small study with a sample size of 60. The majority of respondents were college students. One question of particular importance provided some surprising feedback. The statement reads: "If you chose five or higher for any of the above statements, are you comfortable with the government having access to the above information?" "The above information," refers to survey questions asking if individuals would use their National ID card for everything from bus pass to banking activities. The Likert style survey provided answers ranging from one (strongly disagree) to seven (strongly agree). The results were rather surprising. The verdict rendered was a split decision. 17 respondents said they were comfortable and 17 respondents said they were uncomfortable with the government having access to that information. The rest of the respondents did not meet the criteria to answer the question. The split decision illustrates that the psychological tweaking by the government has already been taking place. For half of the respondents to have no concern for their privacy is a startling revelation, considering the threats of identity theft, spam, and other evils of the digital revolution. A follow-up study should be completed with a larger sample size, however, a statement has been made in response to the above stated survey question.

### **Conclusion**

A mandatory National ID smart card system will have its day. The time and place is not here and not now. The number of privacy implications is insurmountable. The implementation of a National Identification smart card challenges the fabric of our Democratic society. Our government was founded on a system of checks and balances to protect the inalienable rights and freedoms of the people. With the implementation of a mandatory National ID card system in conjunction with the U.S. Patriot Act, there are no checks or balances in place to protect the inalienable rights and freedoms of the people. Supporters of the system will claim the previously defined privacy acts will protect the people. It has been demonstrated that the U.S. Patriot Act overrides the majority of provisions in the previous and currently existing legislation. The government is granted free reign over every American's personal information. They have the ability to play god on a small scale. This amount of control by a government begins to lean towards a Totalitarian state or Dictatorship.

Just as the original restrictions on the use of the Social Security card have been all but eliminated, limits on a national I.D. number or card would be ignored or legislated away. There would be an irresistible temptation to use the data for purposes for which it was never intended, including government surveillance. Former Senator Alan Cranston has described the national I.D. card as “a primary tool of totalitarian governments to restrict the freedom of their citizens” (ACLU).

Disturbing thoughts such as these will continue to grow if such a system is set into place. Freedom should never be contingent on an individual’s perceived safety, it is a two way street. Any person living in a free society understands that to enjoy the benefits there is some degree of uncertainty of the actions of the next person. This uncertainty is the price paid to continue to live in freedom, to enjoy the fruits of Democracy. Economists are fond of saying, “There is no such thing as a free lunch.” Americans understand this concept now and have, arguably, always understood it. Americans value their freedom to live and freedom to privacy above all else. These values set us apart from the rest of the world. Once these are gone, they will fade into eternity as dust, eradicated for the chance to consolidate power under false pretenses.

The quest and need for privacy is a natural one, not restricted to man alone, but arising in the biological and social processes of all the higher forms of life. All animals have a need for temporary individual seclusion or the intimacy of small units, quite as much as for the stimulus of social encounters among their own species. Indeed the struggle of all animals, whether naturally gregarious or not, to achieve a balance between privacy and participation is one of the basic features of animal life (Michael, pg 3).

#### **Works Cited**

- Bennett, Colin J., and Raab, Charles D. *The Governance of Privacy: Policy Instruments in Global Perspective*. Great Britain: Ashgate, 2003.
- Bensen, Miles. “Raising the Standard for Identification -- Step by Step.” 2002. *Newhouse News Service*. <http://www.newhousenews.com/archive/story1a102202.html>
- “Definition of Biometrics.” *Department of Statistics - Texas A & M University*. 22 Nov 2004. <<http://stat.tamu.edu/Biometrics/definition.html>>
- “Civil Status Law.” 2004. *Directorate General of Civil Status*. 22 Nov 2004. <[http://www.civilstatus.gov.om/english/civil\\_status\\_law.asp#6](http://www.civilstatus.gov.om/english/civil_status_law.asp#6)>
- “How is Biometrics Defined?” 2004. *International Biometrics Group*. 22 Nov 2004. <[http://www.biometricgroup.com/reports/public/reports/biometric\\_definition.html](http://www.biometricgroup.com/reports/public/reports/biometric_definition.html)>
- Hunt, Stephen. “National ID debate: Tech Advances, public concern?” *Security*. Jan. 2002: Vol. 39, Iss. 1.
- Kennedy, John B., and Schwartz, Paul M. *Privacy Law: New Developments & Issues in a Security-Conscious World*. New York: Practising Law Institute, 2001.

- Kidder, Rushworth M. *How Good People Make Tough Choices Resolving the Dilemmas of Ethical Living*. New York: William and Morrow, 1995.
- Kiefer, Kimberly, Wu, Stephen, Wilson, Ben, and Sabett, Randy. *Information Security: A Legal, Business, and Technical Handbook*. Chicago: ABA Publishing, 2004.
- Michael, James. *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology*. Dartmouth: UNESCO, 1994.
- "NEC to Build Smart Card ID System." *Computer Wire*. 29 Mar 2004
- "Networks Focus; Smartcards;" *Computer Weekly*. 28 Oct 2003.
- Nicoll, C., ed., Prins, J.E.J., ed., Van Dellen, M.J.M., ed. *Digital Anonymity and the Law: Tensions and Dimensions*. Netherlands, Asher Press, 2003.
- Orwell, George. 1984. New York: Signet, 1950.
- Owen-Brown, Michael. "Big Brother's Little helper." *The Advertiser*. 18 Aug 2001: Opinion, pg 29.
- "Smart Card Definition." 2004. The Webopedia Website. 22 Nov 2004. <[http://www.pcwebopedia.com/TERM/s/smart\\_card.html](http://www.pcwebopedia.com/TERM/s/smart_card.html)>
- Raman, Prasanna. "Leveraging Smartcard Power." *New Straits Times – Computimes (Malaysia)*. 1 Sept 2003.
- Roberts, Greg. "Smart Card 'a risk' to Privacy." *The Australian*. 30 Sept 2003: Local pg 8.
- Ross, William G. "Go Slow on National Identification Cards." 2001. *University of Pittsburgh Law School*. 7 Nov 2004. <<http://jurist.law.pitt.edu/forum/forumnew37.htm>>
- Rowan, David. "A Travel Card With A Dark Secret." *The Times (London)*. 8 Oct 2002.
- "A Sense of Identity." *New Media Age*. 11 July 2002.
- Spinoza, Michael de. *Ethics*. Trans. G.H.R. Parkinson. New York: Oxford, 2000.
- "Social Security Numbers." 28 Sept 2004. *Electronic Privacy Information Center*. 22 Nov 2004. <<http://www.epic.org/privacy/ssn>>
- Tudor, Ben. "Time to clarify IT law." *IT Week*. 18 Mar 2002.
- Weich, Ronald, Esq. *Insatiable Appetite: The Government's Demand for New and Unnecessary Powers After September 11<sup>th</sup>, an ACLU Report*. Washington: ACLU 2002.
- Williams, David. *Royal Oman Police*. Oman: Directorate General of Civil Status, 2003.
- Williams, David. *The Sultanate of Oman National Registration System (NSR)*. Oman: Directorate General of Civil Status May 2004.
- "What is a Smart Card?" 2004. *Sun Microsystems*. 22 Nov 2004. <<http://java.sun.com/products/javacard/smartcards.html>>
- "Why Does the ACLU Oppose a National ID Card System?" 1996. *American Civil Liberties Union*. 22 Nov 2004. <<http://archive.aclu.org/library/aaidcard.html>>

**Appendix A: Biometrics and Privacy Concerns Survey**

**Definitions**

**Biometrics.** The automated use of physiological or behavioral characteristics to determine or verify identity. the term "Biometrics" has also been used to refer to the emerging field of technology devoted to identification of individuals using biological traits, such as those based on retinal or iris scanning, fingerprints, or face recognition.

**Smart Card.** Smart card is a small electronic device about the size of a credit card that contains electronic memory, and possibly an embedded integrated circuit.

**National ID.** Mandatory government issue ID card represented in the physical form by a smart card. The card includes the following personal identification information: driver’s license, passport, social security number, insurance information, and medical records. For authentication purposes your retinal image and fingerprints are used.

**Questions**

1. Are you familiar with the term: Biometrics? Yes No
2. If yes to #1, does your definition match the above definition? Yes No
3. Are you familiar with the term: Smart Card? Yes No
4. If yes to #3, does your definition match the above definition? Yes No
5. Are you familiar with the term: National Identification card? Yes No
6. If yes to #5, does your definition match the above definition? Yes No

**Circle the number that best corresponds to your feelings to the statements:**

	Strongly Disagree		Neutral			Strongly Agree	
	1	2	3	4	5	6	7
Mandatory National ID card violates my privacy							
National ID card improves national security							
National ID card improves my personal safety							
Less privacy for better national security is an acceptable trade-off							
National ID card will be issued in my lifetime							

**If possible, I would use my National ID card for the following additional services:**

	Strongly Disagree		Neutral			Strongly Agree	
	1	2	3	4	5	6	7
Bus / Metro / Train / Subway Pass	1	2	3	4	5	6	7
Credit Card	1	2	3	4	5	6	7
Debit / Check Card	1	2	3	4	5	6	7
Banking Activities (securing loans, etc.)	1	2	3	4	5	6	7
Preferred restaurant menu selections	1	2	3	4	5	6	7
Shopping preferences (style, size, color, etc)	1	2	3	4	5	6	7

If you chose 5 or higher for any of the above statements, are you comfortable with the government having access to the above information?    Yes    No

**Demographic Information (Optional)**

Sex:    M        F

Age:    0-17    18-25    26-34    35-42    43-50    50-57    58+

Occupation: \_\_\_\_\_

Computer Literacy Level: None    Novice    Intermediate    Expert  
Professional