

National ID Cards: Protection or Invasion?

I. Introduction

For some time, national identification (ID) cards have been the subject of debate. Proponents believe that national ID cards will enhance national security, protect Americans against terrorists, and deter illegal immigrants from entering the country. Opponents believe that national ID cards will not effectively protect Americans from terrorists or illegal immigrants, but will invade our privacy and compromise our civil rights.

The debate over whether the U.S government should implement a national ID system is not a new one. Thirty years ago, a task force of the Social Security Administration rejected extension of the Social Security Number to a corresponding ID card. In 1973, a Health, Education and Welfare Committee debated a similar issue, and subsequently decided that a national ID was not a good idea at the time. In 1976, the Federal Advisory Committee on False Identification similarly rejected the concept of a national identifier, and in 1981 the Reagan Administration followed suit. In 1999, Congress repealed a provision in the Immigration Reform and Immigrant Responsibility Act of 1996 that would authorize the inclusion of Social Security Numbers on drivers' licenses (EPIC, 1).

While there has not been a substantial initiative to develop a national ID system in many years, the tragic events of September 11 changed the thinking of many Americans regarding national security measures. Subsequently, there has been renewed interest in the development of a national ID card. In late September 2001, Oracle CEO Larry Ellison proposed development of a national identification system and offered his company's technological resources to develop it. Ellison's proposal has again sparked this controversial debate, and there are strong positions involving basic ethical principles on both sides of the argument. This paper will explore the dilemma faced by public administrators in their consideration of whether the benefits of a national ID system will outweigh the consequences.

II. Ethics Overview

In order to frame the ethical dilemma involved with the national ID card issue, it is best to first discuss the concept of ethics in general and why they are important for public administrators.

Ethics is essentially the philosophical study of morality – what we do and how we act. Ethics deals with concepts of moral duty and obligations. Ethics presupposes that we are free individuals and want to do what is “right”, and also that we are capable of making informed and conscious decisions without excessive influence from other people.

There are two main categories of ethics: 1) descriptive; and 2) normative. Descriptive ethics make statements about “what is” – for example, “It is the responsibility of the Federal Bureau of Investigation (FBI) to protect our nation’s security”. Normative ethics question what “ought to be” – “Do FBI employees violate our privacy rights when they are protecting our nation’s security?” Ethics involve concepts of good, bad, rightness, and wrongness. In ethical discussion, rightness and wrongness typically refer to actions, while good and bad are descriptive of intentions and motives. The study of ethics does not rely on law, religion, or politics. This is mainly because law and religion, for example, appeal to a higher authority to determine the right action to take. In the case of law, the right decision is contingent upon what decision will conform with the law – which decision is legal (and in the cases where the law is unclear, an interpretation of the law is sought through the courts). It is important to point out that just because an action is legal, that does not mean that the action is ethical. A historical example of this concept is civil rights. While at one time segregation was legal, it was determined to be unethical because it violated many ethical principles – among them, dignity, fairness, respect, and tolerance. In cases such as this, the person making the decision on how to act is merely concerned with conforming to a standard or legal requirement – they are not focused on doing what is ethically right.

Another important distinction to make regarding ethics is the difference between ethics

and morals. While morals can be classified on an individual or cultural basis, ethics are meant to be universal in nature. A succinct characterization of this distinction was stated by Dr. David L. Perry in his June 2000 presentation to the Leadership of Santa Clara University entitled “Ethics in Public Service”. In his written remarks, he stated “ Perhaps most ethical principles should be considered *prima facie* binding on us: i.e., universal (not relative to cultural or individual beliefs) and timeless, but not absolute. Ethical principles will often reinforce each other in opposition to selfishness and cruelty” (5).

Once the concept of ethics is defined, it is important to note that there are two approaches to ethical decision-making. The first approach is classified as *teleological*, meaning that the focus is on the consequences of our actions. The second approach is classified as *deontological*, meaning that the focus is on the actions themselves – deciding whether an action is right or wrong regardless of the consequences.

In Business Ethics: A Philosophical Reader, Thomas White discusses the teleological and deontological approaches to ethics. As stated in this book, a teleological approach to ethics claims that an action is considered ethical based on the extent to which actions benefit or cause detriment to others. This approach is best characterized by the philosophical school of thought called Utilitarianism, which was proposed by Jeremy Bentham and later revised by John Stuart Mill. Thomas White wrote, “Utilitarianism therefore contends that something is morally good to the extent that it produces a greater balance of pleasure over pain for the largest number of people involved, or as it is popularly described, “the greatest good of the greatest number” (4).

A deontological approach to ethics, as presented by Immanuel Kant, is based on the notion that “...some actions are considered inherently good; others are bad” (6). In the deontological approach to ethics, an action cannot be considered right – regardless of the good that comes from it – if the action itself violates an ethical principle. Kant claims that “the only thing inherently good is a good will, that is, one that follows reason’s guidance and actions from

a sense of duty...because it is the right thing to do” (7). In Kant’s deontological school of thought, an action is ethical only if that action could successfully be applied to a universal scale; i.e., that the action would be morally permissible if it could be considered a law of nature. Regardless of whether a teleological or deontological approach (or combination of both) is taken to consider an ethical question, it is evident that there are many factors involved and points to consider before a well-reasoned decision can be reached.

III. Introduction to Ethical Dilemmas

With this general ethics background in mind, we can now proceed to a discussion of an ethical dilemma. An ethical dilemma is present when a decision-maker is confronted with a situation where any alternative action taken will produce undesirable ethical consequences (namely, will violate one or more ethical principles). For the purposes of this paper, we will examine a particular ethical dilemma from the perspective of the public administrator.

The fundamental role of a public administrator is to serve the public by the best means possible. Fulfilling this role applies to the effective and efficient use of resources, maintaining a sense of duty to the public at large, and adhering to a sense of duty to one’s organizational superiors. Often, these priorities and duties will be in conflict – that is, a decision to fulfill a sense of duty applicable to one service sector (for example, the public at large) will contradict a duty to another sector (for example, one’s superior). In addition to this type of scenario, a public administrator may also encounter a conflict between principles of ethics. This type of conflict arises when a decision must be made, and regardless of the action chosen, there will be an inevitable violation of one or more ethical principles. Some examples of ethical principles are justice, honor, loyalty, and respect. Many decisions faced by public administrators are not clear-cut; that is, in the best interest of serving the public, an ethical principle may have to be sacrificed in order to fulfill another ethical principle. The greatest challenge in this type of situation is to determine which principle is more important in regards to the problem at hand. This can be extremely difficult to determine, and potential resolution of the ethical dilemma

requires a great deal of examination and evaluation. One method by which to handle an ethical dilemma is to use an established ethical decision-making framework. A discussion and application of this type of framework in regards to national ID cards is below.

IV. Application of Terry Cooper's "Ethical Decision-Making Model" to Ethical Dilemma Regarding National ID Cards

In an attempt to fully discuss and seek resolution of the dilemma concerning national ID cards, Terry Cooper's "Ethical Decision-Making Model" presented in his book The Responsible Administrator will be used. This Model, or framework, has four main components: 1) defining the ethical issue; 2) identifying alternative courses of action; 3) projecting possible consequences; and 4) state of resolution (20).

A. Definition of the Ethical Issue

1. Background on National ID Cards

First, it is important to note that the ethical dilemma involved regarding the use of national ID cards can also be related to the dilemma faced with the possibility of implementing a nationwide identity system that does not have a physical component. The concepts involved, regardless of whether an actual card is used or an alternative national system identifier is put in place, are interchangeable and will be treated as such in this paper. The debate concerning implementation of either type of system (though the concept is typically proposed by development of an ID card) involves the same ethical principles. In effect, the phrase "identity system" may be a more appropriate way to characterize the issue of national ID cards, since regardless of whether a card is used, many components – such as legal, technological, administrative, and social – will be interwoven.

As mentioned previously, the debate over whether a national identity system should be put in place had begun many years prior to the terrorist attacks of September 2001. The reasons that a national ID system has not yet been put in place - in addition to the ethical arguments surrounding the issue - are because such a system would be complicated to develop

and difficult to implement. Due to the increasing threats to our nation's security, however, many people feel that these developmental problems should be overcome in order to mitigate against terrorist attacks. An extensive evaluation of this subject was presented in IDs – Not That Easy: Questions About Nationwide Identity Systems, written by the Computer Science and Telecommunications Board (CSTB). In this publication, the CSTB discusses the purpose and many factors to consider in implementing a national ID system. The CSTB classifies a national ID system as "...a component of a large and complex nationwide identity system, the core of which could be a database of personal information on the U.S. population...[the system] might involve the detection of abnormal or suspicious patterns of behavior that accompany the planning and/or execution of a terrorist act" (1).

2. Public Administration Implications

In considering whether the implementation of a national ID system would be ethical, it is important to first examine the context in which the system would be put in place. This context involves state and federal agencies, laws, and regulations.

Agencies Involved

It is conceivable that many different state and federal agencies could be involved in the development, maintenance, and use of a national ID system. Currently, the Department of Defense already has a "Common Access Card" in use for its employees as an identification system. Of course, state Department of Motor Vehicles (DMVs) already have a de facto ID system in place – the drivers license. In addition, the Social Security Administration issues each American citizen a Social Security Number which is used for many different purposes. Government officials at the Department of Justice are reportedly working on "a nationally standardized ID system that could include such security features as digitized fingerprints or encoded magnetic strips" (Leinwand, 2). Since proposals for national ID cards are typically relative to the increasing effort to protect our nation against terrorism, the public administrator to consider this ethical dilemma will be employed with the Office of Homeland Security.

The reason that the Office of Homeland Security (OHS) would likely be the potential agency to administer a national ID system is because of the relation this type of system would have to the federal government's national security initiatives. The OHS and the related Homeland Security Council were established, within the Office of the President, in October 2001 by an Executive Order. As stated in the Executive Order, the mission of the OHS is to "develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks" (White House, 2001). Among the duties of the OHS listed in the Executive Order are to "work with executive departments and agencies, State and local governments, and private entities" in the accomplishment of this mission. The reason that this coordination between agencies, departments, and groups is especially important is because it is entirely possible that prior to the terrorist attacks, departments such as the Immigration Department, Federal Aviation Administration, FBI, and U.S. Customs may not have seen a crucial need to "cross-check" their information. For example, a passenger engaged in a U.S. Customs check may be on the FBI's Most Wanted list but allowed to go through because this information was not shared between departments. One of the duties of the OHS is to prevent situations such as this. In consideration of this coordination and information sharing directive of the Executive Order, it would not be inconsistent for a public administrator at the OHS to put a national identifier system in place, because this system would facilitate information sharing between departments, perhaps by sharing access rights to a central database.

In addition to requiring coordination and integration with other federal agencies and departments, the Executive Order requires the OHS to "ensure that all executive departments and agencies that have intelligence collection responsibilities have sufficient technological capabilities and resources to collect intelligence and data relating to terrorist activities or possible terrorist acts within the United States" (2001). A national ID system could certainly be characterized as a technological means by which to provide and exchange intelligence and data.

Legal/Legislative Factors

In implementing a national ID policy, it would be necessary to pass laws that would define the rights, obligations, authorities, use, and privileges associated with such a system. This national ID system would need to be developed from the aggregation of numerous databanks and ID requirements. Also, if a national ID system were put into effect, it would have to comply with existing laws. There are five main laws that would have to be reviewed to ensure this: 1) The Immigration Reform and Control Act of 1986; 2) The Illegal Immigration Reform and Immigrant Responsibility Act of 1996; 3) The Personal Responsibility and Work Opportunity Reconciliation Act of 1996; 4) The Health Insurance Portability and Accountability Act of 1996; and 5) The Federal Aviation Administration and other databank and ID requirements (Sobel, 4).

The Immigration Reform and Control Act of 1986 requires employees to prove to employers that they are U.S. citizens or have permission from the government to work. The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 has stringent penalties for “fraudulent use of government-issued documents”. The Personal Responsibility and Work Opportunity Reconciliation Act of 1996 mandates the creation of a federal databank to track newly hired employees. The Federal Aviation Administration requires airlines to request government-issued photo identification from passengers for flights within the U.S. There are other databank and ID requirements which are used in a national ID system. As mentioned, requirements of the Department of Transportation and Social Security Administration mandate drivers licenses and Social Security ID documents, respectively (5).

In addition to the above-mentioned legislation, privacy laws would also have to be reviewed to ensure that the new ID system was not in violation of privacy rights. Privacy issues in regards to a national ID system are discussed in the previously mentioned CSTB book. In this publication, the CSTB states, “the minimization principle is often used as a guideline when building systems sensitive to privacy concerns. It relates to the kind and quantity of information collected from and/or about individuals and emphasizes the need to collect only the minimum

amount necessary for the desired transaction. Minimization also implies that disclosure of information should be limited to the purpose(s) for which it was collected (9).

In taking privacy laws and concerns into consideration, the public administrator would have to ensure that the national ID system did not collect information that was not necessary to fulfill the purpose of having such a system in place. Specifically, personal information that would not provide insight as to a person's security risk or terrorist affiliation (such as credit history, purchasing preferences, etc.) should not be included.

In the Privacy Act of 1974, "Congress intended the guidelines to ensure that each user has a legitimate purpose, information remains accurate, and security measures protect data from unauthorized access. Further, Congress sought to confer privileges upon every citizen to retrieve, control, and correct their personal information and initiate a civil suit for intentional violations by federal agents (Black, 7). It is clear that emphasis on privacy rights mostly focus on the potentially unauthorized use of personal information.

Intent of Congress

Another important consideration of a public administrator must be that regulations are consistent with the intent of Congress as stated in existing legislation. Legislation was signed into law in response to the terrorist attacks that may provide some insight as to what the intent of Congress would be regarding a national ID system. In November 2001, the President signed into law the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" (USA PATRIOT) Act. Certain provisions of the Act prohibit states from issuing "a license to operate a motor vehicle transporting in commerce a hazardous material" unless DOT has first determined that the applicant "does not pose a security risk warranting denial of the license." The legislation also requires the Department of Justice (DOJ) to perform, upon the request of a state, a background records check of any hazmat license applicant. The records check is to include criminal history records, immigration records, and international databases where appropriate. This information will be provided to DOT and form

the basis of DOT's determination regarding a particular driver. While a rule has not yet been issued by the Department of Transportation putting this law into effect, it may be inferred that Congress intends to take any necessary precautions to mitigate against potential use of hazardous materials in terrorist attacks. The concepts involved implementation of a criminal records background check for drivers is not inconsistent with requirements of a national ID system. In either case, the obtainment, exchange, and use of personal information by a federal agency will be required.

Regulations

A crucial component of any public administrator's decision-making process is the involvement of interested stakeholders. These stakeholders include the public, inter-agency personnel, other federal agency personnel (such as the Immigration and Naturalization Service, Social Security Administration, Department of Transportation, Bureau of Vital Statistics, and the General Services Administration, to name a few), state and local agencies (such as state Department of Motor Vehicles), Congress, and interest groups (for example, the American Civil Liberties Union, Electronic Privacy Information Center, American Association of Motor Vehicle Administrators). In order to implement such a complex system, all of these stakeholders would have to be involved in the public policy making process to ensure that all concerns are addressed and issues discussed.

Upon review of the factors for a public administrator to consider related to national ID cards, it does not appear as though such a system would be contradictory to existing law, Executive Orders, or Congressional intent. With the completion of this evaluation, the next step for the public administrator would be to examine the ethical principles involved with such a decision.

3. Ethical Arguments Supporting National ID Cards

While the issue of national ID cards has met a host of criticism from privacy and civil rights groups, there has also been widespread public support of such a system. In a *National*

Journal online poll from February 2002, 50% of the 861 adults surveyed supported a national ID card system (2002). Well-known liberal attorney and Harvard Law professor Alan Dershowitz has publicly supported national ID cards. Larry Ellison, CEO of Oracle, has publicly offered the technological resources of his company for free in order to implement such a system. In order to examine this ethical dilemma, it is important to consider the particular ethical principles involved. What follows is a discussion of ethical principles that are supported by a national ID system, as advocated by national ID card proponents.

Benevolence

Benevolence can be defined as actions which are kind, charitable, and beneficial. Supporters of national ID cards believe that a national identifier would assist in protecting Americans against terrorists, which would obviously be a benefit. In an October 2001 article in the *New York Times*, Alan Dershowitz writes, “[a national ID card offers a] tradeoff: a little less anonymity for a lot more security...A national ID card would be uniform and difficult to forge or alter. It would reduce the likelihood that someone could, intentionally or not, get lost in the cracks of multiple bureaucracies” (1).

Duty

As mentioned in the President’s Executive Order, the mission of the OHS is to take necessary measures to protect Americans from terrorism. Since national ID cards would do this by seeking to identify criminals and potential terrorist suspects, it would be consistent with a public administrator’s duty: to protect the public. In order to effectively do this, proponents of national ID cards argue, they must have the resources necessary to do so. Larry Ellison, CEO of Oracle, maintains that

the single thing we could do to make life tougher for terrorists would be to ensure that all the information in myriad government databases was integrated into a single file...All these separate databases make it difficult for one agency to know about and apprehend someone wanted by another agency. That’s why one of the Sept. 11 hijackers made it through U.S. passport control, even though he had an outstanding arrest warrant in Broward County, Fla (Ellison, 2).

Responsibility

The reasons for supporting a national ID card because it adheres to the ethical principle of responsibility are similar to those arguments that believe that a national ID card would also confer with the ethical principle of duty. In written testimony at the Congressional “Oversight Hearing on National Identification Cards” held in November 2001, George Washington University Law School professor Jonathan Turley points out that “It is important to remember that the Framers gave us a constitutional system that is the most nimble in the world. Whether acting to maximize profits or protection for our citizens, it is a system that is unparalleled in its ability to respond and adjust to new realities” (3). Turley makes clear in his testimony that the idea of national ID cards should not be immediately rejected just because nothing like this has been done before. He believes that the government’s responsibility is to adapt and change with the times to best serve the public. He succinctly stated “As in nature, nations who fail to evolve are the least likely to survive and flourish. We should not be fearful or hostile to new ideas on how to better protect our citizens against new threats” (3).

Promise-Keeping

When taking a position in either the federal, state, or local government, a public administrator must commit to fulfilling their duties to serve (and in the case of OHS, protect) the public. In keeping their oath to protect, the OHS must be willing to make decisions that may not be popular, but may be necessary. As mentioned, the Department of Defense has already implemented an ID system for its employees. Navy Petty Officer Wellington Jimenez responded to inquiries from the *Washington Post* on how he felt about the government’s role in this ID system. He said, “I know the government will have more access to my information, but I know it’s going to be used in the right way. I feel protected” (December 17, 2001).

Dignity

Alan Dershowitz makes a claim that national ID cards will help prevent discrimination. In an October 2001 article in the *New York Times*, he writes,

A national ID card could actually enhance civil liberties by reducing the need for racial and ethnic stereotyping. There would be no excuse for hassling someone

merely because he belongs to a particular racial or ethnic group if he presented a card that matched his print and that permitted his name to be checked instantly against the kind of computerized criminal history retrieval systems that are already in use (2).

This argument basically states that if everyone were to present an ID card, it would not be necessary for law enforcement or other federal/security personnel around the country to “single them out” for further investigation.

Ethical Arguments Against National ID Cards

Not surprisingly, the topic of national ID cards has created an uproar among civil liberty, privacy, and government decentralization advocates. These groups, such as the American Civil Liberties Union (ACLU), Privacy International, and the Cato Institute, have been outspoken on the subject of national ID cards.

Fairness

Opponents to national ID cards believe that it violates the ethical principle of fairness. The ACLU has written numerous papers and articles on this issue. In testimony to the House Committee of Government Reform, Katie Corrigan, legislative counsel for ACLU, states “... minorities would become subject to more and more status and identity checks – not just from their employers, but also from police, banks, merchants, and others... This would mean certain individuals would be increasingly vulnerable to a system that subjected them the stigma of constantly having to prove their citizenship” (3).

Autonomy

Opponents of national ID cards adamantly believe that the implementation of such a system will violate the ethical principle of autonomy. These groups claim that a national ID system would allow the government to access information they had no right to access, and that surveillance by the government would infringe on a person’s right to be independent. In her testimony, Corrigan states, “A national ID system would violate the freedom Americans take the most for granted and the one that most defines our liberty: the right to be left alone... As a free

society, we cherish the right to be individuals, to be left alone, and to start over, free from the prying eyes of the government” (3).

In the Boston University Journal of Science and Technology Law, Richard Sobel succinctly defends this argument by stating,

Such a system raises profound ethical and public policy concerns for a free society. By transforming individuals’ identities from the inherent qualities of persons who have and deserve dignity and general protection under the Constitution to attributes represented by numbers, cards, and places in databanks, the process degrades the moral value of political and personal identity as an intrinsic quality of personhood (2).

In these types of arguments, there are frequent remarks of “Papers, please” and references to negative government situations in Nazi Germany, Soviet Russia, and Cuba.

Justice

Opponents of national ID cards make similar arguments relative to the ethical violation of the principle of justice as they did for principles of fairness and autonomy. ACLU attorney Katie Corrigan mentions that a national ID card system may violate rights to due process, since technical glitches or delays in ID procedures may prevent someone from getting on a plane or entering a building, for example. An article in the *Cornell International Law Journal* discusses the injustices that may occur if this type of system was put in place and a myriad of government entities were given access rights to personal information. In the article, R. Brian Black writes, referring to the Privacy Act of 1974, “Congress intended the guidelines to ensure that each user has a legitimate purpose, information remains accurate, and security measures protect data from unauthorized access. Further, Congress sought to confer privileges upon every citizen to retrieve, control, and correct their personal information and initiate a civil suit for intentional violations by federal agents” (7).

Trust

Naturally, the idea of a national ID card also makes mention of trust issues. Opponents of ID cards believe that the ethical principle of trust will be violated if the government or other entities are given access to personal information on a grand scale. Examples are provided of

past misuses of personal information by the federal government, such as Internal Revenue Service Employees accessing the tax records of celebrities or their neighbors. In a Cato Institute report entitled “A National ID System: Big Brother’s Solution to Illegal Immigration”, John Miller and Stephen Moore discuss this situation. They write, “The potential for abuse of a national ID system is greater than it has been of any previous government program. The personal information stored in a national worker registry would have to be widely available to the public – more than 6 million employers, after all, would need access to it” (6). In a similar vein, Privacy International issued a lengthy report in 1996 that warned of ill intentions by government employees. The article states, “...it is generally assumed that at any one time, one percent of staff will be willing to sell or trade confidential information for personal gain” (11).

Respect

Privacy advocates are also up-in-arms over the violation of the ethical principle of respect they feel will be inevitable if national ID cards are put in place. In the book entitled A National ID Card, A License to Live, author Robert Ellis Smith (a frequent contributor to the *Privacy Journal* publication) claims that national ID cards would create disrespectful actions by authorities. Smith feels, as many opponents to the national ID cards do, that requiring law-abiding citizens to display their ID to confirm their identity is degrading and denies the individual of respect. He writes, “We will have granted great powers to police officers to stop citizens engaged in law-abiding activities and demand that they produce identity and ‘give a good account of themselves” (2).

B. Identification of Alternative Courses of Action

Now that the arguments have been presented, it is time for the public administrator to consider all likely actions. Following Cooper’s framework, the OHS representative would now list potential actions regarding the dilemma at hand, without passing judgment on those actions. In relation to national ID cards, the following are possible actions that could be taken: 1) the OHS will implement a mandatory national ID system for all Americans (we will not deal with

international/immigration issues for the purposes of this paper); 2) the OHS will not implement a mandatory national ID system; 3) the OHS implement a voluntary national ID system; and 4) modify existing state drivers license program to implement more uniform system.

C. Projection of Possible Consequences

Under all of these alternative courses of action, the impact will be significant. If a mandatory ID system is put in place, there could be an outcry from privacy and civil rights groups. It is possible that while recent polls indicate that the majority of Americans would support a national ID system if it might help protect them against terrorists, the public may change their mind once a proposal is made (the fear of “Big Brother”). The public administrator would have to be willing to take considerable “heat” from the press and interest groups. It is entirely possible that government employees given rights to access such a system (and there would most likely be thousands) would abuse their privileges, gaining access to information that is not required for the mission they are to accomplish. It is also possible that with the centralization of information into a common database, that identify theft could occur. From an administrative aspect, implementing such a program would be extremely difficult. Intensive and thorough analysis, including involvement of all interested stakeholders (possibly many public meetings) would have to be done prior to moving forward. A program of this magnitude could not, and should not, be taken lightly.

Alternatively, choosing not to implement a national ID system, at least at this time, could prove harmful to the American people. It is entirely possible that some of the September 11 hijackers would have been identified as suspicious if a national identifier was put in place. In addition, air travel and perhaps even using out-of-state checks would be made easier if establishing identity was more efficient and effective.

Without a national identifier in place, law enforcement could be denied a potential aid that would save lives and apprehend criminals that cross state lines. Agency cross-coordination and

integration would improve communications between departments and avoid overlap and information “falling through the cracks”.

Depending on outlook, a national ID system could either serve to reduce harassment and racial profiling or add to it. Perhaps the existence of a national ID would prevent “singling out” of those who appear to be from another country. Or, a national ID may just provide another reason to check someone’s credentials.

While a voluntary ID card may facilitate such things as travel and credit checks, for the purposes of national security, it would do little to establish a person’s identity, since criminals and those who feel it would be an inconvenience or privacy violation would simply elect not to get one.

A last alternative was suggested by the American Association of Motor Vehicle Administrators (AAMVA) - the organization who represents state Departments of Motor Vehicles (DMVs). In this proposal, the AAMVA suggests that instead of a national ID card, a modification should be made to strengthen the existing drivers license standards. The AAMVA believes that uniformity with state DMVs will prevent a person from having multiple identities, and that law enforcement can check a person’s criminal history across state lines, enhancing security. Senator Dick Durbin (D-IL) has supported federal funding to develop such a program. He has introduced legislation that would authorize a study on which various biometric identifier methods (such as iris scans, face scans, fingerprinting) could be researched for potential use in a centralized database that could be shared between DMVs, the Immigration and Naturalization Service, and the SSA (*Washington Post*, April 17, 2002). The same concerns as with the national ID system would inevitably surface, but perhaps since it only involves a few agencies and applies to a drivers license, which is voluntary, the outcry may not be as severe.

D. State of Resolution

It is evident from the discussion of this issue that an initiative with such far-reaching implications would have to be carefully and thoroughly analyzed. The debate on national ID

cards invokes intense feelings on both sides of the issue. From a public administrator's point of view, implementation of such a system would not be a good idea at this point. As part of their duty and responsibility to serve the public, public administrators must sometimes make unpopular decisions. In the case of national ID cards, the backlash resulting from a perceived violation of civil liberties would not justify implementation of this type of system. This is mainly because the benefit and actual mitigation against terrorism resulting from a national ID system is not yet known. From a self-appraisal standpoint, I would take the deontological approach to this issue. Even though benefit could potentially be realized from a national ID system, this is far from certain. Would I want to give authority for the OHS or another federal agency to gain access to my personal records when the result may be tentative? No, I wouldn't. At this point, the ends do not justify the means, because the ends are unknown.

Taking these factors into account, Senator Durbin's proposal to devote federal funds to commission a study on the use of biometric identifiers seems appropriate. The Progressive Policy Institute (PPI) also made feasible recommendations in a February report that would most likely not cause controversy over privacy rights. The PPI recommends that in addition to linking DMV databases, as proposed by the AAMVA, states should be required to issue standardized "smart cards" with encoded biometric data. The PPI also recommends that grants and loans be provided to states to assist in implementation of such a system. The recommendation of this paper is to proceed with Senator Durbin's proposal to commission a study, and then "test the waters" with a uniform national drivers license containing biometric data. This is an innocuous step in the right direction. Since September 11th, Americans may no longer be afforded the right to complete anonymity if the public is to be better protected from terrorists.