

ARTICLE

THE DEGRADATION OF POLITICAL IDENTITY UNDER A NATIONAL IDENTIFICATION SYSTEM

RICHARD SOBEL*

TABLE OF CONTENTS

ABSTRACT	
I. INTRODUCTION	
II. WHAT CONSTITUTES NIDS AND HOW IS IT DEVELOPING?	
III. WHAT WOULD A FORMAL NIDS LOOK LIKE?	
IV. HISTORY OF ABUSES WITH IDENTITY SYSTEMS AND DOCUMENTS?	
V. CRITIQUE OF NIDS: PROBLEMS WITH ID AND DATABANK REQUIREMENTS	
VI. PRACTICAL CONSIDERATIONS	
VII. FUNDAMENTAL CRITIQUE OF NIDS	
VIII. TOWARD A WORLD WITHOUT NIDS	
IX. CONCLUSION	

* Richard Sobel is a Senior Research Associate in the Program in Psychiatry and the Law at Harvard Medical School. Earlier versions of this article were presented as papers, "A National Identification System: Beyond the Ethics of Technology?" at the Panel on Anonymity and Digital Identity, Fourth Annual Ethics and Technology Conference, Boston College, June 4-5, 1999 and "The Degradation of the Moral Economy of Political Identity Under a Computerized National Identification System" at the Panel on "Informing Identities" Conference on "Moral and Political Economy of Computer Culture," Franke Institute, University of Chicago, August 7-10, 2000. The author would like to thank Daniel Solove at Seton Hall Law School and Shaun Spencer at Harvard Law School for their comments and Michael Krasnovsky and Wendy J. Netter for able research assistance. He would also like to thank the Howe Grant for Civil Rights and Civil Liberties directed by John Mansfield and the Office of Public Interest Advising directed by Lisa Dealy at Harvard Law School for their support. Finally, he appreciates the efforts of Boston University Journal of Science & Technology Law's managing editor Allen C. Nunnally in making possible the timely publication of this article.

I. ABSTRACT

Over recent years, even prior to September 11, 2001, federal laws and regulations have substantially pushed the U.S. toward a National Identification System. Statutes and regulations promulgated by federal authorities have increased the government's power to monitor citizens' lawful activities through the use of national identification numbers, databanks, and identification cards that undermine political and personal identity. The Immigration Reform and Control Act of 1986, the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (Welfare Reform Act of 1996), the Health Insurance Portability and Accountability Act of 1996, and the FAA/Airline ID requirement along with the Computer-Assisted Passenger Screening system propose national identification and databanks as solutions for problems with illegal immigration, child support, health costs, and airline security. Because the centralization and monitoring of personal information increases the likelihood of abuses, the power gained by the government to misuse this information typically outweighs their supposed benefits and degrades political and personal identity.

The creation of a National Identification System ("NIDS") contradicts the fundamental principles of personal liberty, the government's burden of proof, and federalism set forth in the Constitution and is of questionable utility. 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. Under such a system, identity no longer inheres in personhood, the natural characteristic that provides for individual rights by presumption and extension as well as for the creation of a political buffer around individuals. Rather, under a NIDS, identity is attained through numbers and cards. Such pseudo identities become commodities in a political economy of surveillance that profoundly undermines the nature of personhood, identity, and privacy in a free society. Additional ID checks or databank matches without probable cause, during which a person may be denied basic rights absent "proper" documentation, positive identification, or an ID number, degrade by accretion political and personal identity based in personhood and human dignity. Hence, a NIDS stands fundamentally opposed to the nature of constitutional governance in a free society and must be halted.

II. INTRODUCTION

America is moving toward a system of national identification numbers, databanks, and identity cards that contradicts the constitutional and philosophical bases of democratic government and undermines the moral economy of political and personal identity. Because the kinds of problems that a national identification system (“NIDS”) is supposed to solve tend to occur in relatively closed societies, the troubles a NIDS creates as a bureaucratic scheme may soon foreclose options and opportunities central to a free society. NIDS degrades the moral economy of political and personal identity by modifying personhood from an intrinsic quality inhering in individuals into a quantity measured by numbers, represented by physical cards, and recorded in computer databanks. Rather than being an inherent part of personhood and dignity, pseudo-identity becomes a characteristic attribute of bureaucratic and computerized systems. The growing impact of NIDS on due process, burden of proof, freedom from search, free expression, freedom of travel, the right to employment, and federalism makes this issue particularly appropriate for contemporary ethical and policy analysis.

These characteristics were aggregating even prior to the tragic events of September 11, 2001, whose aftermath has accelerated their development. It is important to explore the natures of personhood and identity, as they existed prior to its potential modification in the anti-terror aftermath, as a standard by which to judge the changes proposed and undertaken. (A subsequent article will examine these more closely, especially in light of governmental responses to the September attacks.¹) This pre-crisis articulation of that standard also identifies a target toward which to return in a post-terror-stricken society.

The ongoing developments toward a NIDS, as privacy advocate Robert Ellis Smith notes, fundamentally contradict what it means to be an American.² In an open democratic society, the government derives its powers from the consent of the governed, constitutions are developed to circumscribe state power, and activities such as work, travel, and medical care are readily available and treated in ways respectful of privacy. In contrast, the government in authoritarian societies bestows, or denies, identities and opportunities through identification numbers or documents, intruding into individuals’ lives. In addition, especially because the government has the power to coerce individuals and to control their lives, people confront force when they must follow, or if they disobey, the government’s directions.

At this moment, our democratic society and way of life are confronted by an authoritarian shift. Several recent laws and administrative regulations provide

¹ Richard Sobel, *The Demeaning of Identity and Personhood In National Identification Systems*, 15 HARV. J.L. & TECH. (forthcoming 2002).

² See Robert Ellis Smith, *A National ID Card Violates American Traditions*, PRIVACY JOURNAL, Mar. 1991, at 4.

the bases for developing a bureaucratic surveillance system through a combination of databanks and identification requirements. A NIDS implemented by the government contradicts and circumvents basic constitutional rights, such as privacy. Moreover, it degrades the moral values of identity by substituting impersonal pseudo-identities for identities based on personhood.

Though people are social animals, “the concept of privacy embodies the ‘moral fact’ that a person belongs to himself and not [to] others nor to society as a whole.”³ The “condition of privacy is a moral value for persons who also prize freedom and individuality; part of its defense against unwarranted invasion should include advocacy of a moral right to privacy.”⁴ Hence, individuals in a free political system enjoy a right against intrusion because personhood and fundamental rights in a free political system create a political space, or buffer, around the individual that permits free expression and unencumbered action.

In a free society and under a constitution of delegated powers, there develops a moral economy that is based upon and further generates basic rights for individuals as persons. This economy derives from the overarching criterion of governance by consent that underlies justice and human dignity. This moral dimension, tied to the burden of proof falling on the state, creates a buffer around individuals and against state action. Individuals inherently possess and exercise rights and political identities buttressed by the buffer created by the moral economy of a constitutional regime.

However, under a NIDS, rights and privileges develop from credentials, and people obtain pseudo-identities based on ID documents and numbers or places in databanks. The requirement to prove identity or appear in a national databank in order to obtain and exercise certain rights degrades the moral economy on which free governance is based. The use of personal information without consent violates property rights and due process protections.

Databanks and other identification schemes imply that society and government have the legitimate power to define and derive individual identities separate from the inherent nature of personhood. The difference appears in the contrast between a right to be free of unreasonable search as a person under the Constitution and a system in which the police may search anyone at will. Freedom from unreasonable search by virtue of personhood contrasts with obtaining that right only after one has proved to be a citizen through identification and thus is “deserving” of that “right.” When one can only exercise fundamental rights because one has proper documentation, the nature of political and personal identity and dignity are degraded.

³ *Thornburgh v. Am. Coll. of Obstetricians & Gynecologists*, 476 U.S. 747, 777 (1986).

⁴ JUDITH WAGNER DECEW, *IN PURSUIT OF PRIVACY: LAW, ETHICS AND THE RISE OF TECHNOLOGY* 28 (Cornell University Press 1997).

Since privacy and liberty, as well as autonomy in personhood, protect the “inviolate personality,”⁵ the degradation of personhood and self-identity is an affront to human dignity.⁶ As Justice Douglas noted about the importance of personhood in his concurrence in *Roe v. Wade*,⁷ “the autonomous control over the development and expression of one’s intellect, interests, tastes, and personality” is a constitutionally protected right and fundamental to privacy.⁸ In his dissent in *United States v. White*, Justice Douglas admonished:

Invasions of privacy demean the individual. Can a society be better than the people composing it? When a government degrades its citizens, or permits them to degrade each other, however beneficent the specific purpose, it limits opportunities for individual fulfillment and national accomplishment.⁹

The creation of a NIDS contradicts the fundamental principles of personal liberty, sovereignty, due process, and federalism set forth in the Constitution and is of questionable utility. The increasing impact of NIDS on fundamental freedoms and values makes this issue essential to explore in its various ethical, constitutional, and policy dimensions.

III. WHAT CONSTITUTES A NIDS AND HOW IS IT DEVELOPING?

A national identification system is developing from the aggregation of numerous databanks and ID requirements. The five basic parts of a NIDS include the Immigration Reform and Control Act of 1986,¹⁰ the Illegal Immigration Reform and Immigrant Responsibility Act of 1996,¹¹ the Personal Responsibility and Work Opportunity Reconciliation Act of 1996,¹² the Health Insurance Portability and Accountability Act of 1996,¹³ and the FAA ID requirement¹⁴ and Computer Assisted Passenger Screening system.¹⁵ Other public and private databank and ID requirements also contribute to a NIDS.

⁵ Samuel D. Warren & Louis D. Brandeis, *The Right To Privacy*, 4 HARV. L. REV. 193 (1890).

⁶ See DECEW, *supra* note 4, at 28.

⁷ 410 U.S. 179 (1973).

⁸ *Id.* at 211.

⁹ *United States v. White*, 401 U.S. 745, 764 (1971) (Douglas, J. dissenting) (quoting RAMSEY CLARK, *CRIME IN AMERICA: OBSERVATIONS ON ITS NATURE, CAUSES, PREVENTION AND CONTROL* 287 (Simon and Schuster 1970)).

¹⁰ Pub. L. No. 99-603, 100 Stat. 3359 (1985) (codified as amended in scattered sections of 8 U.S.C.).

¹¹ Pub. L. No. 104-208, 110 Stat. 3009-546 (1996) (codified as amended in scattered sections of 8 U.S.C.) [hereinafter IIRIRA].

¹² Pub. L. No. 104-193, 110 Stat. 2105 (1996) (codified in scattered sections of 42 U.S.C.).

¹³ Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified at scattered sections of 26, 29, and 42 U.S.C.) [hereinafter Welfare Reform Act].

¹⁴ See Charlotte Twight, *Watching You: Systematic Federal Surveillance of Ordinary*

B.U. J. SCI. & TECH. L.

The Immigration Reform and Control Act of 1986 (“IRCA”) requires employers to have employees prove that they are U.S. citizens or have governmental permission to work. Employees must fill out and sign an I-9 verification form and provide government identification, such as a passport, in order to work. Employers may be fined up to \$10,000 per violation for employing undocumented aliens¹⁶ and are subject to a six-month maximum prison sentence if they demonstrate a persistent pattern of hiring unauthorized aliens.¹⁷

The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (“IIRIRA”) has stringent penalties for “fraudulent use of government-issued documents.”¹⁸ Individuals may be imprisoned for up to twenty-five years for violating these stricter provisions under the statute.¹⁹ In addition, the IIRIRA provides for a five-state “Pilot Program for Employment Eligibility Verification,” which allows for databank checks for Social Security numbers,²⁰ as well as funding for the “Machine-Readable-Document Pilot Program” in Iowa and the “Criminal Alien Identification System” pilot program.²¹ The IIRIRA calls for the standardization of birth certificates and driver’s licenses in all states²² and for the development of prototype counterfeit-resistant social security cards as well.²³ Under the IIRIRA, an employer may no longer verify that its employee is authorized to work by examining a certificate of U.S. citizenship, certificate of naturalization, or unexpired foreign passport. Rather, it requires a United States passport, resident alien card, or alien registration card in order to work in the United States.²⁴

Americans, INDEPENDENT REV., Fall 1999, at 165 (providing a complementary analysis to this article).

¹⁵ *See id.*

¹⁶ 8 U.S.C. § 1324a(e)(4) (2000).

¹⁷ JACK L. RUNYAN, A SUMMARY OF FED. LAWS AND REGULATIONS AFFECTING AGRIC. EMPLOYERS: IMMIGRATION REFORM AND CONTROL ACT OF 1986, U.S. DEP’T OF AGRIC., ECON. RESEARCH SERV., AGRIC. INFO. BULLETIN NO. 652 (Aug. 1992).

¹⁸ 18 U.S.C. § 1028(b) (2000).

¹⁹ *Id.*

²⁰ IIRIRA, Pub. L. No. 104-208, § 404, 110 Stat. 3009-664 to 3009-665 (1996) (codified as amended at 8 U.S.C. § 1324a note (2000)). Interestingly, § 404(h)(2) of IIRIRA states “Nothing in this subtitle shall be construed to authorize directly or indirectly, the issuance or use of national identification cards or the establishment of a national identification card.” *Id.* § 404(h)(2), 110 Stat. at 3009-665.

²¹ IIRIRA, Pub. L. No. 104-208, §§ 326, 401-405, 110 Stat. 3009-630, 3009-655 to 3009-666 (1996) (codified as amended at 8 U.S.C. § 1252 note (2000)).

²² IIRIRA, Pub. L. No. 104-208, § 656, 110 Stat. 3009-716 (1996) (codified as amended at 5 U.S.C. § 301 note (2000)).

²³ IIRIRA, Pub. L. No. 104-208, § 657, 110 Stat. 3009-719 (1996) (codified as amended at 42 U.S.C. § 405 note (2000)).

²⁴ 8 U.S.C. § 1324a(b) (2000). An individual may also present any other document designated by the Attorney General, if the document contains a photograph of the individual

The Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (“Welfare Reform Act”) mandates the creation of a federal databank to track newly hired employees. It records names, addresses, Social Security numbers, and wages for everyone hired after October 1, 1997. The information is collected at the state level and is then transmitted to a national database at the Department of Health and Human Services (HHS). Its stated purpose is to assist federal and state officials in locating parents who owe child support by tracking them from job to job and from state to state, but it affects all newly hired employees, and thus, over time, will include almost the entire labor force.²⁵ The Welfare Reform Act also calls on the Social Security Administration (“SSA”) to “harden” the social security card.²⁶

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) mandated the development of a “unique health identifier” and the creation of a national electronic data collection system for personal health care data, as part of a law whose purpose was to make health insurance transferable for people who change jobs. The goal of the national health identifier is to facilitate the tracking of patients, health care providers, health plans, and health care events paid for by public and private funds. It would assist monitoring patients’ health as they changed providers, assist patients in obtaining their old records, streamline billing, and create a national database to help in cost analysis and research studies. Information from patients’ medical records, even if paid for privately, would be included in this electronic system.²⁷

The Federal Aviation Administration (“FAA”) requires airlines to ask passengers on domestic flights to identify themselves with government issued photo identification.²⁸ For this purpose, passengers must typically provide a

and “such other personal identifying information relating to the individual as the Attorney General finds . . . sufficient for purposes of this subsection,” or a combination of social security account number card, “other documentation evidencing authorization of employment in the United States” and a driver’s license or similar document issued for the purpose of identification by a State, “if it contains a photograph of the individual or such other personal identifying information relating to the individual.” *Id.* The IIRIRA no longer allows an individual to demonstrate employment authorization by presenting certificate of birth in the U.S. or establishing U.S. nationality at birth. *See* 8 U.S.C. § 1324a(b)(1)(B), (C) (2000).

²⁵ *See* Robert Pear, *Vast Worker Database to Track Deadbeat Parents*, N.Y. TIMES, Apr. 30, 2000, at A1.

²⁶ *See* Welfare Reform Act, Pub. L. 104-193, § 111, 110 Stat. 2105 (1996) (codified as amended at 42 U.S.C. § 405 note (2000)).

²⁷ *See* Sheryl Gaye Stolberg, *Health Identifier for all Americans Runs Into Hurdles*, N.Y. TIMES, July 20, 1998, at A1.

²⁸ *See* Chris Woodyard, *Losing Photo ID Can Make Boarding Plane Next to Impossible*, USA TODAY, Jan. 3, 2000, at 2B; *see also* Federal Aviation Administration, *Civil Aviation Security, Passenger Information*, at <http://cas.faa.gov/faq.html> (last visited Jan. 2, 2002). To satisfy the identification requirement passengers must typically provide a passport or a driver’s license with a photo. *See U.S. General Services Administration, Additional Airport Security Measures*, at http://www.gsa.gov/Portal/content/offerings_content.jsp?content

passport or a driver's license with a photo. The FAA Computer Assisted Passenger Screening system ("CAPS") requires that all passengers be profiled at check-in and those who fit a certain "profile" be singled out for intensive searches of both carry-on and checked luggage for the purpose of preventing terrorism. Based on the profiling result, the checked luggage of "selectees" must be subject to a more intrusive x-ray search.²⁹

Other databank and ID requirements also contribute to a NIDS. Department of Transportation ("DOT") and SSA requirements mandate the upgrading of driver's licenses and Social Security cards as identification documents and require the DOT to impose standards to federalize the driver's license. In 1996, the DOT mandated that all states use Social Security numbers on or in driver's licenses by October 1, 2000, in order to gain acceptance for identification purposes by federal agencies.³⁰ A federalized driver's license would include the licensee's name, address, phone number, date of birth, physical descriptors, photo, possibly a biometric identifier, and a Social Security number.³¹ Proponents of the federalized driver's license maintain that it will reduce the number of forged identity documents used by illegal immigrants to gain federal benefits.³² In response, the Georgia Legislature passed a bill mandating fingerprints for Georgia driver's licenses in April 1996³³ while California, Colorado, Florida, and Hawaii already require fingerprints on driver's licenses.³⁴

OID=119458&contentType=1004 (last visited Jan. 7, 2002) (reflecting security procedures put in place after Sept. 11, 2001). The FAA has refused to release information contained in Security Directive 96-05, which is believed to be the basis for this identification requirement. See *How to Fly Without ID*, at <http://permanenttourist.com/4paths/fly-without-id.html> (last visited Jan. 7, 2002) (quoting ID requirements under Security Directive 96-05 from before Sept. 11, 2001 and discussing the ambiguity surrounding the disclosure of federal regulations on airline security). Under the Freedom of Information Act (FOIA), 5 U.S.C. § 552 (2000), information is exempted from release concerning matters which are "specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld." 5 U.S.C. § 552(b)(3).

²⁹ See Exec. Order No. 12949, 3 C.F.R. 321-322 (1995), *reprinted in* 50 U.S.C. § 1822 (2000) (allowing for the legal "physical search for foreign intelligence" without a court order or a warrant). See also *How to Fly Without ID*, *supra* note 28.

³⁰ See Robert Ellis Smith, *Congress is Out of Step on Social Security Numbers*, PRIVACY JOURNAL, Oct. 1996, at 1.

³¹ See Jennifer Lee, *Upgraded Driver's Licenses Are Urged as National ID's*, NEW YORK TIMES, Jan. 8, 2002, at A13.

³² See *id.*; see also Frank James, *ID-Number Proposals Raise Issue of Privacy*, CHICAGO TRIBUNE, Aug. 31, 1998, at N6.

³³ See Cyndee Parker, *National ID Card is now Federal Law and Georgia Wants to Help Lead the Way*, at <http://www.mcwebs.com/repeal/newgeorg.htm> (July 18, 1997).

³⁴ See J. Radick, *What's Required on a Driver's License*, PRIVACY JOURNAL, July 2001, at 3. However, legislatures in 24 states have passed laws allowing drivers to remove their

Citizens cannot obtain or renew a passport without providing a taxpayer identification number, usually a Social Security number, subject to a \$500 penalty levied by the IRS.³⁵ This law's stated intent is for the IRS to check on tax compliance by foreigners or citizens living abroad, but it is administered by the State Department, which issues passports required of citizens living in the U.S. desiring to travel abroad. Thus, the law violates the "fair information" principle³⁶ that information gathered for one purpose is not to be used for another purpose and also threatens the right to travel for individuals unable to get their passports renewed.

In addition, the Centers for Medicare and Medicaid Services (formerly the Health Care Financing Administration, which was created in 1997 to manage the Medicare and Medicaid federal health programs) utilizes a databank to monitor the quality of health care among senior citizens.³⁷ The information entered into the databank tracks billing records and the performance of over 9,000 Medicare-certified health care providers.³⁸ Patients are asked, among other questions, personal information about "socially inappropriate behavior," "a sense of failure," and depression.³⁹ The system has been scaled back, but not abandoned, because of protests.⁴⁰

Separately and jointly, these and other databanks and identification requirements are setting the foundation for a NIDS. The emphasis here is on civil and administrative databanks and ID schemes, rather than crime and law enforcement, such as the FBI's National Crime Information Center (NCIC) 2000. Because the parts of a NIDS have been coming together in a largely unrecognized manner, it is important to monitor them and to inform citizens of their constitutional and political implications.⁴¹

IV. WHAT WOULD A FORMAL NIDS LOOK LIKE?

What if these developments led to the creation of a completed NIDS? A formal NIDS would require an identity number, databank, and ID card. The system would begin by assigning each American resident a unique national

Social Security Numbers from driver's licenses. *Id.*; see also *Winners and Losers . . . State by State Analysis of Current Driver's License Laws and Requirements*, available at <http://www.networkusa.org/fingerprint/page4/fp-04-page4-winners-losers.html> (last modified May 1, 2001) (detailing a compilation of state driver's license requirements and noting that a variety of states do not require photographs on driver's licenses).

³⁵ 26 U.S.C. § 6039E (2000).

³⁶ See DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS, REPORT OF THE SEC'Y'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYS. (DHEW Pub. No. (OS) 73-94) 41, July 1973.

³⁷ See Robert O'Harrow Jr., *U.S. Set to Gather At-Home Patient Data*, WASHINGTON POST, March 11, 1999, at A1.

³⁸ See *id.*

³⁹ See *id.*

⁴⁰ See Stolberg, *supra* note 27, at A1.

⁴¹ See Twight, *supra* note 14, at 168-69.

identity number. Each citizen and identifiable immigrant would be uniquely identified by a numeral. Resident enumeration and data collection would begin at birth, defining each newborn as a data point to be tracked from cradle to grave through a government-issued number. Such a process has already begun with the relatively recent practice of issuing Social Security numbers at birth and requiring them to obtain marriage licenses⁴² and tax deductions for one's children of any age.⁴³ Those entering the country after birth would also be assigned an ID number.

For the existence and implementation of a NIDS, particularly a national identity card, there must also be a national computer databank organized by ID numbers. An individual would have to be entered into the databank to exist in a legal sense or to have a bureaucratic existence. Receiving an ID card would require meeting the criteria for being registered in the databank. ID numbers would be used for multiple purposes, and computer databanks would collect disparate pieces of information. For reasons of proposed efficiency, such a computer system would centralize and interconnect with educational, employment, social security, tax, and medical information. These data would paint a detailed portrait of each individual's habits and preference even though such collections would not be fully accurate or secure. One would not, moreover, have a political identity or be able to exercise political rights without proper ID. Inclusion in the databank would create a paper, plastic, or electronic person.

The possible scenario for a NIDS is straightforward. At birth, every U.S. citizen would be issued a national identification number and entered into a databank.⁴⁴ Over a lifetime, that number would track home addresses, information on the parents, health records, school records, job records and pension information. When the child became old enough to go to school or

⁴² E.g., *Requirements for Obtaining a Marriage License*, at <http://web.co.wake.nc.us/reeds/marriage/marriage.htm> (last modified Dec. 30, 2001) (indicating that social security numbers are required for obtaining a marriage license in North Carolina); *Texas Marriage License Information*, at http://www.sanantonioweddings.com/wedding_resources/marriage_license.htm (last modified Jan. 11, 2002) (indicating that social security numbers are required for obtaining a marriage license in Texas); *Marriage License Information*, at <http://utahreach.usu.edu/sanpete/govt/docs/marrfaq.htm> (last modified Apr. 10, 2000) (indicating that social security numbers are required for obtaining a marriage license in Utah).

⁴³ See 26 U.S.C. § 32(c)(3)(D)(i) (2000).

⁴⁴ See Annie I. Anton, *National Identification Cards*, at http://www.cc.gatech.edu/computing/SW_Eng/people/Phd/id.html (Dec. 17, 1996). Argentina requires all citizens to obtain a national identity document when they are 8 years old. See *id.* at Part II.A. If the document has not been registered for by the age of 9 years and 8 days, a fine 10 times that of the normal tariff is levied. See *id.* Citizens must re-register for a national identity document at the age of 16. See *id.* In addition, nine European Union countries have state-run identity card systems, with Britain, Ireland and Denmark being the exceptions. See *id.* at Part II.B.

work, he or she would be issued a national ID card to be carried outside the home.⁴⁵ The number would then track the citizen's schooling, health care, and places of employment. The databank could include the information on the citizen's driving records and the use of health care and government services. This system would also operate, with modifications, for legal immigrants. It might also include as many illegal immigrants and temporary visitors as identifiable. Citizens or residents might be required to carry their national ID at all times or produce it when entering school, applying for a job or government benefits, and traveling away from home.

In 1965 the Johnson administration proposed a National Data Center (NDC) to centralize and link all government data collection.⁴⁶ The NDC was to store records from four federal agencies: "population and housing data from the Bureau of the Census; employment information from the Bureau of Labor Statistics; tax information from the Internal Revenue Service; and benefit information from the Social Security Administration."⁴⁷ The concept of the NDC "slowly evolved into that of a massive databank containing cradle-to-grave electronic records for every U.S. citizen. The databank would contain every person's electronic birth certificate, proof of citizenship, school records, draft registration and military service, tax records, Social Security benefits, and ultimately, their death records and estate information."⁴⁸ The NDC would have led to a NIDS, but it was not implemented because of concerns about privacy and the high potential for abuse of the information centralized therein.

Although there has not yet been a serious call for a stand-alone NIDS, such a de facto system is developing as a result of the creation of different databanks that track large numbers of people. While a NIDS is taking shape out of the laws and regulations mentioned previously, it will likely expand to fill other purposes. Moreover, the National Governors Association ("NGA") asserted the "great" need for some type of personal identification mechanism "to combat fraud, crime, illegal immigration, and mismanagement of funds."⁴⁹ The NGA called for the federal government to implement such a system to track citizens from birth to death.

⁴⁵ See Twight, *supra* note 14, at 185-90 (analyzing educational databanks).

⁴⁶ See SIMSON GARFINKEL, *DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY* 13 (O'Reilly & Associates 2000).

⁴⁷ *Id.*

⁴⁸ *Id.*

⁴⁹ David M. Bresnahan, *Governors Push National ID Plan*, WORLDNETDAILY.COM, Nov. 13, 1998 (quoting the NGA), at http://www.Worldnetdaily.com/news/article.asp?ARTICLE_ID=16798. Some in the NGA complained, however, that Executive Order 13083, which would have allowed federal agencies to establish what is and is not permissible for state and local governments to legislate, violated principles of federalism. See David M. Bresnahan, *How Governors View States' Rights: Only Some Care About Executive Order 13083, National ID*, WORLDNETDAILY.COM, at http://www.Worldnetdaily.com/news/article.asp?ARTICLE_ID=16823 (Nov. 26, 1998).

V. HISTORY OF ABUSES WITH IDENTITY SYSTEMS AND DOCUMENTS

Identity systems and documents have a long history of uses and abuses for social control and discrimination. Through the Civil War, slaves were required to carry passes in order to travel outside of plantations. The pass laws only ended formally with the abolition of slavery by the Thirteenth Amendment in 1865 and with the freed slaves becoming citizens by virtue of their birth in the U.S. under the Fourteenth Amendment in 1868.⁵⁰

In addition, criminal identification through the use of fingerprints was often used to track and control increasingly mobile, diverse populations whose race or ethnicity made them suspect in the eyes of authorities.⁵¹ Fingerprint identification offered a way to individualize ethnic minorities, particularly African and Asian Americans, as many white Americans feared that they would all look the same.⁵² One commentator states:

Fingerprint identification allowed law enforcement officials to ignore the reality of human variation: that “races” were arbitrary categories that masked both the enormous breadth of intraracial variation and the existence of individuals who blurred racial boundaries. Instead, the widespread adoption of the fingerprint system allowed the mythical tripartite categorization of all people into ‘black,’ ‘white,’ and ‘yellow’ to persist. This crude categorization has, of course, had profound consequences for [policing] in the United States.⁵³

State bureaucracies also implemented passports in order to control citizens, particularly their right to travel.⁵⁴ The passport was first used in post-Revolutionary France, in order to “stymie the assembly of anti-government forces, prevent infiltration by foreign agents, and suppress vagrancy and crime.”⁵⁵ Other European states soon followed France’s lead and began using the passport as a method of “suppressing dissent and controlling crime The passport became a humble marker of ordinary citizenship, the earliest expression of the idea that all citizens should have some sort of identity document.”⁵⁶

⁵⁰ See Gary L. Hewitt, *The Southern Slave Patrol* (Jan. 21, 1991) (unpublished manuscript, on file with author at Princeton University, Department of History). Along with the granting of voting rights under the Fifteenth Amendment in 1870, these were established to undergird and enforce protections of the freedmen’s civil rights. See *id.* But see ROBERT M. GOLDMAN, *RECONSTRUCTION AND BLACK SUFFRAGE: LOSING THE VOTE IN REESE AND CRUIKSHANK* 124-26, 139-142 (University Press of Kansas 2001) (discussing the undermining of the Fourteenth and Fifteenth Amendment’s protections).

⁵¹ See SIMON COLE, *SUSPECT IDENTITIES: A HISTORY OF FINGERPRINTING AND CRIMINAL IDENTIFICATION* 163-64 (Harvard University Press 2001).

⁵² See *id.* at 163.

⁵³ *Id.* at 164.

⁵⁴ See *id.* at 10.

⁵⁵ *Id.*

⁵⁶ *Id.*

The development of passports as identity documents has followed a similar course in the U.S. Under the Passport Act of 1926,⁵⁷ the Secretary of State is given wide discretion to “either grant or withhold a passport as the public interests may require.”⁵⁸ The Act further states that “[n]o passport shall be granted or issued to or verified for any other persons than those owing allegiance, whether citizens or not, to the United States.”⁵⁹ This wide discretion has led to discriminatory laws and practices, such as a former statute barring members of communist organizations from applying for passports, renewing their passports, and from using or attempting to use their passports.⁶⁰ Although this statute was repealed soon after it was passed, it did not stop the Secretary of State from denying passports to individuals deemed to be communists, a practice subsequently found unconstitutional by the Supreme Court.⁶¹ The Court has held, however, that the Department of State may bar individuals from traveling to certain countries with which the U.S. had broken diplomatic ties.⁶² The wide discretion accorded to the Secretary of State in the denial and granting of passports has led to discriminatory restrictions on the rights of individuals to travel. The continued use of passports as a method of suppressing dissent and controlling the citizen abridges the due process clause of the Fifth Amendment.⁶³

A system of identification cards was used to isolate and round up Jews in Germany and other Nazi-occupied territories prior to World War II and in the occupied countries once the war began. All German Jews were required to apply for such cards by December 31, 1938.⁶⁴ Furthermore, the Nazis

⁵⁷ 22 U.S.C. § 211a (2000).

⁵⁸ *Id.*; see also 23 OP. ATT’Y. GEN. 509 (1901).

⁵⁹ 22 U.S.C. § 212 (2000).

⁶⁰ Subversive Activities Control Act of 1950, 50 U.S.C. § 785 (2000) (repealed 1954).

⁶¹ See *Kent v. Dulles*, 357 U.S. 116 (1958) (holding that the Fifth Amendment prohibits the Secretary of State from denying passports to individuals because of their alleged Communistic beliefs and associations and their refusal to file affidavits concerning present or past membership in the Communist Party); see also *Aptheker et al. v. Secretary of State*, 378 U.S. 500, 505 (1964) (holding section 6 of the Subversive Activities Control Act of 1950, 50 U.S.C. § 785, unconstitutional on its face because it “too broadly and indiscriminately restricts the right to travel and thereby abridges the liberty guaranteed by the Fifth Amendment”)

⁶² See *Zemel v. Rusk*, 381 U.S. 1, 13 (1965) (holding that the Passport Act of 1926 allows the Secretary of State to deny an individual a passport for travel to Cuba “not because of any characteristic peculiar to appellant, but rather because of foreign policy considerations affecting all citizens”).

⁶³ See COMM. ON FOREIGN AFFAIRS, SUBCOMM. ON STATE DEPT. ORG. AND FOREIGN OPERATIONS, *PASSPORTS AND THE RIGHT TO TRAVEL: A STUDY OF CONTROL OF THE CITIZEN* (1966) (on file with the Harvard Law School Library) (providing a complementary analysis).

⁶⁴ See RAUL HILBERG, *DESTRUCTION OF THE EUROPEAN JEWS* 118 (Holmes & Meier Publishing, Inc. 1985).

conducted two separate censuses, the first in Germany in 1933 to identify practicing Jews⁶⁵ and the second in the Greater Reich, including Germany, Austria, the Sudetenland, and the Saar in 1939 to identify “racial Jews.”⁶⁶ In the interest of “‘simplification’ of the administrative structure,” German Jews were removed from the civil service in 1935.⁶⁷ Jews were also required to carry IDs, and their passports and ration card were stamped with a red “J.”⁶⁸

When the outside media reported on Jewish persecution, they focused on registrations and censuses as the initial step of Nazidom. Nazi methodology, technology and ties to IBM generally remained outside the public consciousness⁶⁹ before specifics began to appear in print. A *New York Times* article from March 2, 1940, called *Jews in Cracow Move to Ghettos*, detailed how 80,000 Jews had been forced to move into a crowded urban area.⁷⁰ The story reported that “[a] common sight is the white armband with the blue Star of David, which all Jews must wear by government decree . . . [signifying] their registration in the government card file.”⁷¹ The atrocities that besieged the Jews and others during the Holocaust began with simple censuses, with the process of identification. As Black notes, “On October 28, 1939, for the Jewish people of Warsaw, everything stopped. That day they were counted.”⁷²

⁶⁵ EDWIN BLACK, *IBM AND THE HOLOCAUST: THE STRATEGIC ALLIANCE BETWEEN NAZI GERMANY AND AMERICA’S MOST POWERFUL CORPORATION* 54-56, 109 (Crown Publishers 2001).

⁶⁶ *Id.* at 169 (“There was little question to the world that the May 1939 national census was racial in nature.”). Reportage in the *New York Times* of the census project made clear that it would “provide detailed information on the ancestry, religious faith, and material possessions of all residents.” *Id.* (quoting *Reich to Take Census of Her 80 Millions*, N.Y. TIMES, May 17, 1939). By May 1939, almost “every ‘practicing Jew’ had been registered, surveyed, numbered, and sorted numerous times in a series of overlapping, often disjointed campaigns.” *Id.*

⁶⁷ HILBERG, *supra* note 64, at 86 (referring to proposals of Pfundtner in the spring of 1932).

⁶⁸ *Id.* at 175.

⁶⁹ See BLACK, *supra* note 65, at 201.

⁷⁰ See *id.*

⁷¹ *Id.* (quoting *Jews in Cracow Move to Ghettos*, N.Y. TIMES, March 16, 1940).

⁷² See *id.* at 189-190. A teacher, poet, and journalist in Warsaw, Chaim Kaplan, remarked of the effects of a forthcoming census,

“Today, notices informed the Jewish population of Warsaw that next Saturday there will be a census of the Jewish inhabitants Our hearts tell us of evil — some catastrophe for the Jews of Warsaw lies in this census The order for a census stated that it is being held to gather data for administrative purposes. That’s a neat phrase, but it contains catastrophe We are certain that this census is being taken for the purpose of expelling ‘nonproductive elements.’ And there are a great many of us now We are all caught in a net, doomed to destruction.” *Id.* at (quoting THE WARSAW DIARY OF CHAIM A. KAPLAN 57, 59 (Abraham Katsh, ed. and transl., Collier Books 1965)).

The collection of information facilitated by Dehomag, IBM's Germany subsidiary, helped "propel a burgeoning new binary of pseudo-science and official race hatred. Racial hygiene, race politics, and a constellation of anti-Semitic disciplines were [mere] talk in the absence of genuine statistics."⁷³ A rash of anti-Jewish laws and decrees prohibiting Jews from participating in most every facet of professional, governmental, academic, and commercial life were made possible by the power to identify all Jewish individuals by name.⁷⁴ The identification system was a potent weapon at police disposal, allowing them to arrest Jews at will.⁷⁵ The system "had a paralyzing effect on its victims . . . [and] induced the Jews to be even more docile."⁷⁶

The identification system was abetted by the use of punch card technology developed by IBM.⁷⁷ The juggernaut of the institution was inescapable.

Jews could not hide from millions of punch cards thudding through Hollerith machines, comparing names across generations, address changes across regions, family trees and personal data across unending registries Even as Hitler's fanatic followers thunder-marched through Nuremberg, Hollerith machines in Berlin were dispassionately clicking and rattling through stacks of punch cards slapping into hoppers to identify the enemy for the next drastic measures.⁷⁸

The Nazi identification system was uncanny. A population of that size had never been identified with such precision and such speed, nor with such far-

⁷³ *Id.* at 59.

⁷⁴ *See id.*

⁷⁵ HILBERG, *supra* note 64, at 179.

⁷⁶ *Id.*

⁷⁷ *See* BLACK, *supra* note 65, at 11. Black wrote:

What made me demand answers to the unmasked question about IBM and the Holocaust? I confronted the reality of IBM's involvement one day in 1993 in Washington at the United States Holocaust Museum. There, in the very first exhibit, an IBM Hollerith D-11 card sorting machine . . . was prominently displayed. Clearly affixed to the machine's front panel glistened an IBM nameplate . . . The exhibit explained little more than that IBM was responsible for organizing the census of 1933 that first identified the Jews. IBM had been tight-lipped about its involvement with Nazi Germany. So although 15 million people, including most major Holocaust experts, have seen the display, and in spite of the best efforts of leading Museum historians, little more was understood about this provocative display other than the brief curator's description at the exhibit and a few pages of supportive research. *Id.*

But see IBM Statement on Nazi-era Book and Lawsuit, at <http://ibm.com/Press/prnews.nsf/jan/E761868F46444B06852569F20064F555> (last visited Jan. 4, 2002) ("It has been known for decades that the Nazis used Hollerith equipment and that IBM's German subsidiary during the 1930s — Deutsche Hollerith Maschinen GmbH (Dehomag) — supplied Hollerith equipment These well-known facts appear to be the primary underpinning for these recent allegations.").

⁷⁸ *See* BLACK, *supra* note 65, at 107.

reaching ramifications and cruel intentions.⁷⁹ “The dawn of the Information Age began at the sunset of human decency.”⁸⁰ By 1942, the Nazis “no longer kill[ed] just Jewish people. [They] killed Jewish *populations*. This was the data-driven denouement of Hitler’s war against the Jews.”⁸¹

When the German Army invaded Denmark, Norway, the Netherlands, Belgium, Luxembourg, and France in 1940, officers examined birth records, voting records, and business records to identify Jews and members of other “undesirable” groups to be rounded up by the Gestapo and sent to the concentration camps.⁸² The Dutch Census Bureau expressed its gratitude to the German mandate to register all Jews, because its use created “an untold administrative simplification and a saving of tens of thousand [of guilders] for the country.”⁸³ The registration and documentation of Dutch Jews developed with little suspicion of the genocide that was to follow.

In the 1930s, the U.S.S.R. began requiring its citizens to carry internal passports.⁸⁴ One of the duties of the Soviet police, or *militia*, was the maintenance of the passport system.⁸⁵ The passport system was established not only for security purposes, but also to control movement within the U.S.S.R., which served to maintain a class system.⁸⁶ Namely, peasants were not allowed passports and were largely confined to live only where they were born.⁸⁷ Workers with passports could be authorized to live in certain areas by the *militia*, who thereby controlled travel within the country.⁸⁸

In 1939, Britain established a national identification system for the purpose of administering commodity rationing.⁸⁹ The police continually demanded to see this identification from citizens for enforcement purposes. Once a national ID was put into use, the temptation for police to demand it rose substantially. In part as a result of protests over these frequently occurring ID checks, the national ID was discarded after 1952.⁹⁰

For over 30 years from 1958 for men, and from 1963 for women, the South African government required Blacks to carry passes that prohibited them from

⁷⁹ See *id.* at 104.

⁸⁰ *Id.*

⁸¹ *Id.* at 365.

⁸² See WAYNE MADSEN, HANDBOOK OF PERSONAL DATA PROTECTION 22-23 (Macmillan Publishers Ltd. 1992).

⁸³ J. PRESSER, THE DESTRUCTION OF THE DUTCH JEWS 37 (E.P. Dutton & Co., Inc. 1969).

⁸⁴ See AMY W. KNIGHT, THE KGB, POLICE AND POLITICS IN THE SOVIET UNION 25 (Unwin Hyman 1990).

⁸⁵ See *id.*

⁸⁶ See RANDOLPH L. BRAHAM ET AL., THE USSR AFTER 50 YEARS: PROMISE AND REALITY 80 (Samuel Hendel & Randolph L. Braham eds., 1967).

⁸⁷ See *id.*

⁸⁸ See *id.*

⁸⁹ See Anton, *supra* note 40.

⁹⁰ See Donna Seaman, *Identity Cards, Trumped Again*, THE ECONOMIST, Feb. 5, 1994, at 61.

moving about the country freely. The small green reference books that all black citizens carried regulated where they had the right to travel and settle in the country. The official purpose of the pass was to provide proof that a Black South African had the right to be present in a specific area.⁹¹ In 1985, to spread the burden of requiring identification equally to all races, a new law decreed that all South Africans were to carry ID cards. Yet, over a ten-year period, blacks were arrested 637,584 times under the law, while there were no instances of whites arrested under the same law.⁹²

In Rwanda, a system of identity cards that distinguished Hutus from Tutsis contributed to the killings. In his poignant remarks on March 25, 1998 about the genocide in that country,⁹³ President Clinton criticized the West for moving too slowly in responding to massacres whose scope and procedures echoed earlier holocausts.⁹⁴ In the President's words describing the genocide, "when they were found, the old and the sick, the women and children alike, they were killed — killed because their identity card said they were Tutsi"⁹⁵

The low likelihood of similar abuses with identification documents in the U.S. does not foreclose the possibility of bureaucratic and discriminatory misuses of identity badges and numbers. In fact, enumeration without observance of strict privacy protection has also lead to dangers here in the United States. The U.S. Census, required by the Constitution to be conducted

⁹¹ See ROGER OMOND, *THE APARTHEID HANDBOOK: A GUIDE TO SOUTH AFRICA'S EVERYDAY RACIAL POLICIES* 122-23 (Penguin Books 1986) (noting that under the first pass laws in South Africa enacted in 1760, all slaves "in the cape" were forced to carry passes).

⁹² In Colorado, American Indians are required to carry a Certificate of Degree of Indian Blood, which distinguishes them from other minorities. See Deborah Frazier, *Indian's ID Card Reminds of Humiliation*, ROCKY MOUNTAIN NEWS, Mar. 22, 1998, at 11R. American Indians were not originally citizens under the Constitution, and were only granted citizenship in 1924. See Act of June 2, 1924, 43 Stat. 253 (codified as amended at 8 U.S.C. § 1401(b) (2000)). In *Bowen v. Roy* an American Indian challenged the constitutionality of using social security numbers in the federal food stamp and AFDC programs on religious grounds. See *Bowen v. Roy*, 476 U.S. 693 (1986). The Court, in an opinion by Chief Justice Warren Burger, held that the statutory requirement that a state agency use a social security number in administering subject programs does not violate the free exercise clause, notwithstanding the plaintiff's belief that use of the number would impair the child's spirit. See *id.* at 712.

⁹³ At the same time that these atrocities were occurring, partially because of the Hutus' ability to identify the Tutsis, the U.S. was implementing IRCA (1986), a law that the 1990 GAO report had found to be discriminating, and the FAA CAPS profiling system that disproportionately selected people from certain ethnic groups (1996). See Michael X. Marinelli, *INS Enforcement of the Immigration Reform and Control ACT of 1986: Employer Sanctions During the Citation Period*, 37 CATHOLIC U. L. REV. 829, 836 (1988); see also, Heather E. Reser, *Airline Terrorism: The Effect of Tightened Security of The Right to Travel*, 63, J. AIR L. AND COM., 820, 840 (1998).

⁹⁴ See Presidents' Remarks to Genocide Survivors in Kigali, Rwanda, 1998 PUB. PAPERS, March 25, 1998.

⁹⁵ *Id.*

B.U. J. SCI. & TECH. L.

every 10 years,⁹⁶ is currently the only complete enumeration of the population. While less sensitive than health care data, census information is kept secret by law for 72 years⁹⁷ with felony penalties for violations.⁹⁸ Furthermore, information contained in the census may only be used for its statistical purposes and may not be published in any manner by which a person could be identified individually.⁹⁹ This protection rests in part on the recognition that the social system as a whole may benefit from the Census, but individuals are at risk from providing such information.¹⁰⁰

Even before the Japanese attack on Pearl Harbor, however, President Franklin Delano Roosevelt ignored these protections and ordered the Census Bureau to collect all information on “foreign-born and American-born Japanese” from the Census data lists.¹⁰¹ Within days, information from the 1930 and 1940 censuses on all Japanese Americans was gathered and distributed to the Federal Bureau of Investigation, the governors, and the top military officials in western states.¹⁰² Its use facilitated the internment of Japanese Americans on the West Coast.¹⁰³

Toyosaburo Korematsu, a Japanese-American, sued claiming deprivation of liberty and property without due process. The Supreme Court found for the government, holding that the internments were constitutional under the war powers of Congress and the Executive, and were justified by military

⁹⁶ U.S. CONST. art. I, § 2, cl. 3.

⁹⁷ See 44 U.S.C. § 2108(b) (2000). Interestingly, this section makes no mention of a 72 year period, but rather states, “With regard to the census and survey records of the Bureau of the Census containing data identifying individuals enumerated in population censuses, any release pursuant to this section of such identifying information contained in such records shall be made by the Archivist pursuant to the specifications and agreements set forth in the exchange of correspondence on or about the date of October 10, 1952, between the Director of the Bureau of the Census and the Archivist of the United States.” See *id.* The 72 year period derives from the a National Archives and Records Administration regulation. See National Archives and Records Administration Access to Records Containing Personal Information, 36 C.F.R. § 1256.4(a)(3) (2001) (“NARA will not grant access to restricted census and survey records of the Bureau of the Census less than 72 years old containing data identifying individuals enumerated in population censuses in accordance with 44 U.S.C. § 2108(b).”)

⁹⁸ See 13 U.S.C. § 214 (2000).

⁹⁹ See *id.*

¹⁰⁰ See JOHN TOLAND, *INFAMY: PEARL HARBOR AND ITS AFTERMATH* 270 (Anchor Books: 1992).

¹⁰¹ *Id.*; see also William Seltzer and Margo Anderson, *After Pearl Harbor: The Proper Role of Population Data Systems in Time of War* (2000) (unpublished manuscript on file with the authors at Fordham University and University of Wisconsin-Milwaukee, respectively).

¹⁰² See *id.* at 285. While it did not identify individuals, the report provided information of where clusters of Japanese-Americans lived. See *id.*

¹⁰³ See BLACK, *supra* note 65, at 346.

necessity.¹⁰⁴ As Justice Francis Murphy's dissenting opinion illuminated, the exclusion of Japanese based on their ethnicity goes beyond what was considered military necessity and "falls into the ugly abyss of racism."¹⁰⁵

The gathering of information based on Japanese ancestry shows the ease with which even the most tightly drawn statutory and constitutional rights can be violated during periods of crisis and fear.¹⁰⁶ A computerized system makes the efforts to identify and locate citizens much easier as was demonstrated by the use of Hollerith systems by both American and Dutch census bureaus in 1943 to create racial "dot maps" to coordinate transfers respectively, to internment camps here and to concentration camps in Nazi Germany.¹⁰⁷

Even following what might have been considered a period of national crisis during World War II after the surprise attack on Pearl Harbor, the threat of closely tracking citizens remained very real. In 1968, the U.S. Supreme Court upheld the Selective Service System requirement that men of draft age carry their draft cards at all times.¹⁰⁸ This could set the basis for requiring citizens to carry identification documents in the future.

VI. CRITIQUE OF NIDS: PROBLEMS WITH ID AND DATABANK REQUIREMENTS

Examples of the expansion of less pervasive systems like Social Security numbering suggest the problems that a NIDS would produce in the U.S. In the

¹⁰⁴ *Korematsu v. U.S.*, 323 U.S. 214 (1944).

¹⁰⁵ *Id.* at 233.

¹⁰⁶ *See generally* GORDON SILVERSTEIN, *IMBALANCE OF POWERS: CONSTITUTIONAL INTERPRETATION AND THE MAKING OF AMERICAN FOREIGN POLICY* (Oxford University Press 1997) (analyzing how individual rights and due process have been violated for national security).

¹⁰⁷ BLACK, *supra* note 65, at 346.

¹⁰⁸ *U.S. v. O'Brien*, 391 U.S. 367 (1968). O'Brien protested the Vietnam War by burning his draft card. *See id.* at 675. This constituted a violation of the Selective Service registration requirements, *see id.* at 376, which state, "Every person required to present himself for and submit to registration must, after he is registered, have in his personal possession at all times his Registration Certificate (SSS Form No. 2) [draft card] prepared by his local board which has not been altered and on which no notation duly and validly inscribed thereon has been changed in any manner after its preparation by the local board. The failure of any person to have his Registration Certificate (SSS Form No. 2) in his possession shall be prima facie evidence of his failure to register." *See* 32 C.F.R. § 1617.1 (1962); *see also* 32 C.F.R. § 1623.5 (1962) ("Every person who has been classified by a local board must have in his personal possession at all times, in addition to his Registration Certificate (SSS Form No. 2), a valid Notice of Classification (SSS Form No. 110) issued to him showing his current classification."). O'Brien was convicted, even though he contended the burning of his draft card to be protected under the First Amendment's right to free speech. *See id.* at 376. O'Brien did not consider the constitutionality of the regulations requiring the carrying of a draft card; it held only that punishing O'Brien for burning his draft card in protest did not violate his First Amendment right to free expression. *See id.*

1930s, President Roosevelt and members of Congress promised that the Social Security number would be kept confidential and the Social Security card would not be used for purposes of identification.¹⁰⁹ The Social Security account numbers were supposed to be used only for purposes of administering the Social Security pension system, and the Social Security cards used to read “not for identification.”¹¹⁰ Yet requirements for use of the Social Security number for identification have proliferated. At a time when Nazi Germany and Stalinist Russia were setting up registration and identification systems, the use of the Social Security number in the U.S. raised troubling questions.¹¹¹

Since the implementation of the Social Security number in 1936, under the provisions of the Social Security Act of 1935,¹¹² there have been almost 40 congressionally authorized uses for it as an identification number.¹¹³ In 1943, Executive Order 9397 allowed any federal agency “planning to establish a new system of permanent account numbers” to use the Social Security number.¹¹⁴ A major expansion occurred in 1962 when the IRS began using the Social Security number as the official individual tax ID number.¹¹⁵

Prior to 1973, individuals did not commonly obtain Social Security numbers until they were around eighteen years old and ready to work. This changed when the Social Security Amendments of 1972 authorized the SSA to enumerate children at the time that they first entered school, at approximately age five.¹¹⁶ The Tax Reform Act of 1986 required individuals filing a tax return after December 31, 1997 to include the taxpayer identification number — usually the Social Security number — for tax dependents age five and over.¹¹⁷ The Family Support Act of 1988 required individuals filing a tax return due after December 31, 1989, to include the taxpayer identification number of each dependent two-years-old or more.¹¹⁸ The Omnibus Budget Reconciliation Act of 1990 required that individuals filing a tax return due after December 31, 1991, include the taxpayer identification number of each dependent one-year-old or older.¹¹⁹ Finally, the Internal Revenue Service

¹⁰⁹ See Lisa Dean, *Endangered Liberties: Social Security Numbers: Then and Now* (Radio America radio broadcast, June 22, 1998).

¹¹⁰ Robert Pear, *The Nation; Not for Identification Purposes (Just Kidding)*, N.Y. TIMES, July 26, 1998, at D3.

¹¹¹ See *Hamilton Predicts Tags for Workers*, N.Y. TIMES, Nov. 1, 1936, Sec. 2, at 5.

¹¹² Pub. L. No. 74-271, 74 Stat. 620 (1936) (codified as amended at 42 U.S.C. § 301 et seq. (2000)).

¹¹³ See 145 CONG. REC. E3 (daily ed. Jan. 6, 1999) (statement of Hon. Ron Paul).

¹¹⁴ Exec. Order No. 93973 (Nov. 22, 1943), C.F.R. § 282 (1943-1948 Compilation).

¹¹⁵ See *Social Security Online, Social Security Number Chronology*, at <http://www.ssa.gov/history/ssnchron.html> (last modified Dec. 3, 2000).

¹¹⁶ Social Security Amendments of 1972, Pub. L. No. 92-603, § 137, 86 Stat. 1329, 1365 (codified as amended at 42 U.S.C. § 405 (2000)).

¹¹⁷ Tax Reform Act of 1986, Pub. L. No. 99-514, § 1524(a), 100 Stat. 2085, 2749.

¹¹⁸ Family Support Act of 1988, Pub. L. No. 100-485, § 704(a), 102 Stat. 2343, 2427.

¹¹⁹ Omnibus Budget Reconciliation Act of 1990, Pub. L. No. 101-508, § 11,111, 104

Restructuring and Reform Act of 1998 required taxpayer identification numbers for dependent children from birth.¹²⁰ This provision was included to compensate for lost revenues from lower tariffs and required a Social Security number for dependents to be claimed on tax returns. Consequently, government tracking has started at an ever earlier point for individuals who now receive a Social Security number at birth.

The numerous other items of personal information required to maintain such a database of 285 million people¹²¹ and the expanding number of agencies able to access its data have significantly expanded its scope. Like the promise that Social Security numbers would only be used for keeping track of pension accounts, any promise of privacy about a national identity databank would soon be compromised.

ID requirements are equally expansive and discriminatory. Though the use of ID checks for IRCA was meant to end “illegal immigration,” its brief and minimal effect on the rate of illegal arrivals has essentially disappeared, while it has instead produced negative consequences.¹²² In 1989, there were an estimated two to three million illegal immigrants in the United States.¹²³ More recent figures suggest perhaps twice as many.¹²⁴ The Immigration and Naturalization Service (“INS”) indicates that the number of illegal immigrants has risen significantly since IRCA was passed.¹²⁵ This still means that more than 280 million people in America who are not illegal are subject to the IRCA and INS jurisdiction. A full-page advertisement in 1986 by the INS to introduce the country to IRCA showed Uncle Sam point out that “You don’t have to be an immigrant to be affected by the New Immigration Law.”¹²⁶

A 1990 General Accounting Office report to Congress found that rather than ending illegal immigration IRCA had created “widespread discrimination”

Stat. 1388-1, 1388-411.

¹²⁰ Internal Revenue Service Restructuring Act of 1998, Pub. L. No. 105-206, § 6021(c), 112 Stat. 685, 824 (1994) (codified as amended at 26 U.S.C. § 32(c)(3)(D)(i) (2000)).

¹²¹ The U.S. Census Bureau estimated the population of the United States to be 285,832,252 as of January 1, 2002. See *United States Census Bureau, Population Clocks*, at <http://www.census.gov> (last visited January 1, 2002).

¹²² See U.S. GEN. ACCOUNTING OFFICE, IMMIGRATION REFORM: EMPLOYER SANCTIONS AND THE QUESTIONS OF DISCRIMINATION 3-7 (Statement of Charles A. Bowsher, U.S. Comptroller, before the Senate Judiciary Committee Mar. 30, 1990)

¹²³ See ELIZABETH S. ROLPH, IMMIGRATION POLICIES: LEGACY FROM THE 1980S AND ISSUES FOR THE 1990S 40 (Rand 1992).

¹²⁴ See IMMIGRATION AND NATURALIZATION SERV., ILLEGAL ALIEN RESIDENT POPULATION (ESTIMATES OF THE UNDOCUMENTED IMMIGRANT POPULATION IN THE UNITED STATES), Oct. 1996, available at <http://www.ins.usdoj.gov/graphics/aboutins/statistics/illegalien/index.htm> (last modified Nov. 14, 2001) [hereinafter INS RESIDENT ALIEN REPORT].

¹²⁵ See *id.*

¹²⁶ *Immigration and Naturalization Serv., You Don’t Have to Be an Immigrant to Be Affected by the New Immigration Law*, NEWSWEEK, Sept. 28, 1987, at 38.

against Hispanics and Asians.¹²⁷ The report found that 19% of employers would not hire people because of their citizenship status, ethnicity, or accent.¹²⁸ The IRCA thus encourages discrimination against foreign-looking applicants, particularly Hispanic and Asian citizens and residents, because of the employer's desire to avoid legal problems associated with the hiring of illegal immigrants. In short, the law itself causes de facto and de jure discrimination.

Though it has done little to reduce the influx of so-called illegal aliens, the law has forced citizens to provide ID to work. However, some American citizens may not have "proper" ID and many "official" cards may be inaccurate due to bureaucratic errors. Consequently, the right to employment is no longer inherent in personhood or citizenship but is only granted for properly credentialed labor force members. Some employers claim that it violates their religious freedom to treat "neighbors" as "strangers."¹²⁹

The IRCA does not work as proposed, in part, because some employers do not check the cards for reasons of convenience, preference to hire illegal aliens, or repugnance at the law. Furthermore, it fails because many of the law's targets, particularly illegal immigrants, are able to obtain fraudulent cards.¹³⁰ No matter how stringent the requirements to check IDs become, some employers will risk fines in order to pay a captive workforce less than they pay others, often for below minimum wage. Employers can make large profits because illegal aliens are easily exploited, in part, because they don't have valid IDs and because the IRCA reduces other job options. The risk of fines under the IRCA becomes a cost of doing business. In short, having such

¹²⁷ See U.S. GEN. ACCOUNTING OFFICE, *supra* note 122, at 6.

¹²⁸ See *id.* at 1, 7. Such a finding of "widespread discrimination" was supposed to trigger expedited procedures for repeal of the Employer Sanctions provision of IRCA but the Congress ignored the requirement. See U.S. GEN. ACCOUNTING OFFICE, REPORT TO THE CONG., IMMIGRATION REFORM: EMPLOYER SANCTIONS AND THE QUESTIONS OF DISCRIMINATION 138, (GAO/GGD-90-62), March 1990; see also Immigration Reform and Control Act of 1986, Pub L. No. 99-603, 100 Stat. 3359 (1986).

¹²⁹ See *American Friends Serv. Comm. Corp. v. Thornburgh*, 961 F.2d 1405, 1406 (9th Cir. 1991). In *American Friends*, a Quaker charitable and relief organization challenged the IRCA's "employer sanction" provision, claiming that it violated the free exercise clause of the First Amendment, but the claim was rejected by the 9th Circuit Court of Appeals. See *id.* The AFSC's beliefs required it and its members to "'welcome — that they help and not show hostility to — the sojourner, the stranger, the poor, and the dispossessed in their midst.' Thus, [they] . . . can neither discharge brothers and sisters whose religious beliefs preclude their producing proof of secular work authorization, nor refuse human beings work — thus depriving them of the means to feed and clothe themselves and their children — simply because they may be strangers in our land." *Id.* (quoting Appellant's Opening Brief (citation omitted)).

¹³⁰ See Ed Koch, *Technology a Boon for Forged ID Industry*, LAS VEGAS SUN, at <http://archive.nandotimes.com/nation/story/0,1038,500308837-500496033-503478886-0,00.html> (Feb. 11, 2001).

a system of IDs in place may actually make it easier for employers who want to hire and exploit illegal immigrants to do so.

Moreover, the IRCA does not work, at least in part, because almost half of illegal immigrants arrive legally and overstay their visas.¹³¹ In addition, many people come for non-work reasons such as to be reunited with family members. The law threatens anyone in the U.S. who hires someone to provide a good or service, such as babysitting, landscaping, and tax accounting. Placing the burden of verifying identity documents on the employer essentially deputizes employers as INS agents and creates the need to be familiar with the different IDs.

The National Directory of New Hires created under the Welfare Reform Act has also expanded a NIDS. Though it is only supposed to prevent child non-support by monitoring the work, income, and addresses of parents who owe child support, the directory keeps track of all new hires, estimated at 60 million annually.¹³² Cumulatively, it will include all persons employed after its 1997 inception. Yet states already keep registries of those seven million people owed child support,¹³³ which could be checked without keeping records on approximately 100 million others.¹³⁴ Additionally, most people are not on welfare, and most people who have jobs support their children. This databank jeopardizes the privacy of the whole working population because of the potential misdeeds of a small minority. Though currently restricted, the government is likely to increase access to this databank for other agencies that want to know the location of employees, just as it has increased access to the SSA databank for verification of Social Security numbers.¹³⁵

¹³¹ See INS RESIDENT ALIEN REPORT, *supra* note 124.

¹³² See Donna Bonar and Linda Deimeke, National Directory of New Hires, Address at the John F. Kennedy School of Government, Strategic Computing & Telecommunications in the Public Sector Conference (Jan. 28, 1999).

¹³³ U.S. BUREAU OF THE CENSUS, APR. CURRENT POPULATION SURVEY: CHILD SUPPORT FOR CUSTODIAL MOTHERS AND FATHERS, Oct. 2000, *available at* <http://www.census.gov/hhes/www/childsupport/cs97.html>. The most recent statistics show that approximately 7,876,000 custodial parents were due child support, approximately 4,720,000 received some child support, and approximately 2,863,000 received the full amount of child support; *see also* David Byrd, *Making Dad Matter*, NATIONAL JOURNAL, Apr. 15, 2000 at 1196, 1197, *available at* <http://www.facstaff.bucknell.edu/pagana/mg312/dad.htm>. There may be 2.7 million non-custodial fathers who owe child support.

¹³⁴ DEP'T OF HEALTH AND HUMAN SERV., HHS FACT SHEET — CHILD SUPPORT ENFORCEMENT: A CLINTON ADMINISTRATION PRIORITY, *at* <http://www.acf.dhhs.gov/programs/cse/fct/csf1.htm> (Nov. 14, 1996). The Child Support Enforcement (CSE) program, established in 1975 under Title IV-D of the Social Security Act, involves 54 separate state systems, each with their own laws and procedures. *See id.* In addition, HHS operates the Federal Parent Locator System, a computer matching system that locates non-custodial parents who owe child support. *See id.*

¹³⁵ *See* Pear, *supra* note 25, at A1; *see also* Tanya N. Ballard, *Reports Says Agencies Must Protect Privacy When Sharing Data*, *at* <http://www.govexec.com/news/index.cfm?mode=report&articleid=19986> (Apr. 20, 2001).

B.U. J. SCI. & TECH. L.

HIPAA's "administrative simplification" requirement for a "unique health identifier" and "national electronic data collection and data system for personal health care data" expand a NIDS framework. The unique health identifier compromises health care privacy and confidentiality by making health information more easily available to employers, insurance companies, and law enforcement agencies that have access to the computer system. Since most people's health information is currently scattered among several doctors and insurance companies, centralizing this information, as the HHS's 2000 rules on electronic medical records would assist in doing, will make it much easier for others to delve into private health records.¹³⁶ An on-line universal health information system would pose the likelihood that people's most closely held medical secrets would be available to those with access to the system. This would make it extremely difficult to obtain confidential health care. Information given to a physician in confidence could ultimately be used against the individual by law enforcement, as law enforcement and national security agencies would have access to private health information.¹³⁷

A unique health identifier (HID) or a national ID number used to obtain medical care and perhaps other federal services would make it easier for the federal government to monitor people without safeguards.¹³⁸ This kind of enumeration for "administrative simplification" is fraught with danger, yet there are inadequate protections to keep personal information private. The HHS comprehensive medical records regulations will permit law enforcement and national security disclosure that compromise confidentiality.¹³⁹ As currently structured, the lapses in the HHS plan for law enforcement, in combination with the unique HID, would lead to the phenomenon known as "docs to cops," where patients' information could contribute to criminal investigations.¹⁴⁰

Possible privacy abuses could be numerous in a NIDS. Linking health records would allow people to be identified in reverse. By searching based on diseases, instead of names, it would be possible to create lists of people with certain medical conditions. Employers with access to a health identifier and information could deny jobs based on the possible financial cost of a pre-existing medical condition under the company's health insurance plan.

¹³⁶ See Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. § 160, 164 (2001).

¹³⁷ See *id.* § 164.512; see also Richard Sobel, The HHS Medical Records Privacy Regulations: The Layout and the Lapses, Presentation at the Harvard Medical School Program in Psychiatry and the Law (June 20, 2001).

¹³⁸ See Warren E. Leary, *Panel Cites Lack of Security on Medical Records*, N.Y. TIMES, Mar. 16, 1997, at A1. In 1997, a National Research Council Panel suggested that health organizations should impose controls to limit access to patient information by using passwords, electronic blocks, tracking people with access to the record, and limiting access on a need-to-know basis because of the potential for abuse and misuse. See *id.*

¹³⁹ See 45 C.F.R. § 164.512(f).

¹⁴⁰ See Sobel, *supra* note 137.

Employers could make promotion decisions based on health rather than performance.¹⁴¹ Furthermore, genetic information could be included as part of a NIDS and used for these discriminatory purposes.¹⁴²

Unlike a Social Security number, which is attached to a system of public benefits, a unique health identifier would not provide direct benefits to the assignees. Rather, it would benefit commercial interests such as those of health care insurers and information technology vendors who would profit from setting up and managing the information systems themselves.¹⁴³ Concern about the HID plan was so widespread that the Clinton Administration held off on implementing the plan until Congress or HHS comes up with privacy safeguards.¹⁴⁴ However, now that the HHS medical records regulations have been approved, the idea of a unique health identifier is likely to resurface.

The FAA photo identification requirement does not in itself additionally improve air travel safety beyond the level ensured by x-ray or magnetometer screening. Anyone clever enough to create a destructive device has the capacity to create or obtain false identity documents to travel under an assumed name. Moreover, first time malefactors, even those prepared to sacrifice their own and other people's lives, would neither need fake identification nor be recognizable by photo or facial identification. Similarly, computer-assisted profiling is unlikely to locate or deter potential terrorists beyond what security agents can accomplish by questioning people flying one way on a cash ticket, and such questioning requires neither high technology nor ID checks.

Requirements for photo IDs to travel and the creation of databanks for profiling of passengers' personal travel habits unnecessarily invade the privacy

¹⁴¹ The HHS regulations prohibit the unauthorized disclosure of personalized health information, such as to an employer who might wish to consider such information for hiring purposes. See 45 C.F.R. § 164.510. See also *Standards for Privacy of Individually Identifiable Health Information*, DEPARTMENT OF HEALTH AND HUMAN SERVICES, OFFICE FOR CIVIL RIGHTS at <http://www.hhs.gov/ocr/hipaa/finalmaster.html> (last visited Jan. 13, 2002) (noting that authorization from the patient is required before a covered entity can disclose information to an employer for employment decisions).

¹⁴² See Robin Cheryl Miller, *Validity, Construction, and Operation of State DNA Database Statutes*, 76 A.L.R. 5th 239, 239 (2000) ("Every state has enacted a statute creating a DNA (deoxyribonucleic acid) database for use in solving various classes of crimes."). The FBI's Combined DNA Index System (CODIS) "enables federal, state, and local crime labs to exchange and compare DNA profiles electronically, thereby linking crimes to each other and to convicted offenders." FED. BUREAU OF INVESTIGATIONS, CODIS MISSION STATEMENT, at <http://www.fbi.gov/hq/lab/codis/program.htm> (last modified June 20, 2001).

¹⁴³ See Beverly Woodward, *Intrusion in the Name of "Simplification,"* WASHINGTON POST, Aug. 15, 1996, at A19.

¹⁴⁴ See Robert Ellis Smith, *Health Identifier Stalled*, PRIVACY JOURNAL, Oct. 1997, at 3. A unique health identifier was a key feature of the defeated Clinton health care plan, as was a Health Security card, a model of which President Clinton displayed in his speech to Congress proposing the plan. See *id.*

of millions of passengers and threaten their right to travel without materially affecting the safety of the flying public. These measures diminish freedom to travel by creating restrictions on airplane passengers that limit air travel only to those with government identification. Both x-raying checked baggage and matching it to passengers would be a more effective strategy for increasing air safety that would not pose as many privacy concerns. Prohibiting even small potential weapons, securing cockpit door, assigning air marshals strategically, and updating crew training are more effective and less intrusive responses to wider dangers.¹⁴⁵

The DOT's mandate for a federalized driver's license changes the purpose of a driver's license from that of a document that demonstrates ability to drive to that of a de facto national identity card. The move toward a federalized driver's license to meet the requirements of IIRIRA compromises individual privacy rights. Citizens in states that do not put Social Security numbers on their driver's licenses could find it difficult or impossible to get a job, board a plane, vote, cash a check, obtain a student loan, purchase firearms, open a bank account, purchase insurance, receive Medicare or Medicaid benefits, or receive other federal benefits. Furthermore, the presence of so much personal information in one place would encourage and facilitate identity theft. Fortunately the DOT and IIRIRA Social Security Number requirements were held in abeyance in 1999 due to complaints about their impact on privacy.¹⁴⁶

VII. PRACTICAL CONSIDERATIONS

A NIDS would be expensive to establish and maintain, and would be subject to numerous errors. It would contribute to misuses, and the administration of such a computerized identification system would create a self-perpetuating bureaucracy. At one hundred to two hundred dollars per person for administrative experts for interviews and validations of documents, costs could be \$25-30 billion dollars. It would cost between \$3 and \$6 billion a year to run, or \$30 to \$60 billion per decade.¹⁴⁷

Error rates common in government databanks would deny many Americans at least temporary access to the workplace or health care based upon whether or not someone's Social Security number were found in a database search. Error rates at 1-3% for a labor force of over 100 million people would deny one to three million people the opportunity to work. In 1992 the INS tried a similar pilot system, planning to compile a databank containing the names of

¹⁴⁵ See Robert Ellis Smith, *False ID a Key Part of the Conspiracy*, PRIVACY JOURNAL, Oct. 2001, at 5.

¹⁴⁶ See Robert Ellis Smith, *SSNs Nixed From Licenses*, PRIVACY JOURNAL, Oct. 1999, at 1.

¹⁴⁷ See John J. Miller & Stephen Moore, *A National ID System: Big Brother's Solution to Illegal Immigration*, Cato Policy Analysis No. 237, Sept. 7, 1995, available at <http://www.cato.org/pubs/pas/pa237.html>.

all eligible workers.¹⁴⁸ In 28% of the cases, the INS could not immediately retrieve information electronically on people, and it took up to two weeks to find that information by hand.¹⁴⁹ Furthermore, two-thirds of those missing workers were found to be eligible after the two-week search and only 9% were found to be ineligible.¹⁵⁰ The error rate would certainly be higher for a national identification system.

The existence of a government databank, in itself, increases the likelihood of privacy infringements. For instance, in 1995, over 500 Internal Revenue Service (IRS) agents were caught checking into the financial data of their friends, relatives, and celebrities.¹⁵¹ The IRS subsequently promised that such misuse of confidential data would be treated with a “zero tolerance” policy.¹⁵² However, over 1,000 similar incidents occurred in 1997 with only twenty-three employees losing their jobs.¹⁵³

The major databanks that would potentially make up a NIDS could be accessible to a wide variety of users and perhaps via the Internet. Such a framework would make personal information available not only to those with Internet access and authority to enter the databanks but also to those with the ability to hack into the databanks on-line. The posting of Social Security numbers on-line by P-TRAK, a part of Lexis-Nexis, and the Social Security PEBES system that allows access to wage and benefits data created so much controversy concerning the information they conveyed and the privacy of that information that the systems had to be abandoned.¹⁵⁴

The existence of government databanks and identification schemes linked to an identification number also increases the likelihood of private collection of additional data. Social Security numbers are often shown on driver’s licenses, and merchants can obtain purchasing profiles from credit card companies by

¹⁴⁸ *See id.*

¹⁴⁹ *See id.*

¹⁵⁰ *See* Glenn Garvin, *Bringing the Border War Home*, REASON, Oct. 1995, available at <http://reason.com/9510/GARVINfeat.shtml>.

¹⁵¹ *See* Robert D. Hershey, *Snooping by I.R.S. Employees Has Not Stopped, Report Finds*, N.Y. TIMES, Apr. 9, 1997 at A16. Unauthorized access (UNAX) provisions used to keep IRS and other government employees from looking through tax returns are in place to combat such invasions of privacy. *See* INTERNAL REVENUE SERV., TAX INFORMATION SECURITY GUIDELINES FOR FEDERAL, STATE, AND LOCAL AGENCIES, PUBLICATION 1075, June 2000, available at <http://ftp.fedworld.gov/pub/irs-pdf/p1075.pdf>.

¹⁵² *See id.* at A16.

¹⁵³ *See id.*

¹⁵⁴ *See* George Mannes, *Angry Callers Want Off Online File*, N.Y. DAILY NEWS, Sept. 19, 1996, at 22; *see also* John Schwartz, Barbara J. Saffir and Staff, *Privacy Concerns Short-Circuit Social Security’s Online Service; Agency Unplugs Web Feature as it Reconsiders Security*, WASHINGTON POST, Apr. 10, 1997, at A23; Zachary Tumin, *Social Security on the Web: The Case of the Online PEBES (1998)* (unpublished manuscript, on file with the John F. Kennedy School of Government, Harvard University), available at <http://www.ksg.harvard.edu/iip/cases/ssa.html>.

Social Security numbers.¹⁵⁵ Health information is also collected in private medical databases, such as the Medical Information Bureau.¹⁵⁶ Furthermore, the clearinghouse provision of the HHS medical regulations could create centralized health information depositories with relatively easy administrative access for law enforcement agencies. The tracking of personal information by state and federal governments and private corporations reinforces the possible collection of additional data in a NIDS.

Institution of a NIDS creates the risk that one's identity could be revoked accidentally or purposefully. Errors in the database could deny individuals their jobs or even their freedom. Incorrect information in a "secure" databank will be very difficult to correct. If a National ID were lost, obtaining a new one could be extremely difficult and time-consuming. Losing one's National ID gives rise to the risk of losing one's identity, livelihood, and liberty. If an individual did not show up in the database at a crucial time, such as at a job check, border crossing, or police traffic stop, or even if small errors were present in one's ID at such times, the potential consequences could be unemployment, detention, or arrest. Furthermore, instituting a NIDS could easily lead to a requirement that it be carried at all times.¹⁵⁷

The pressures to develop technical "fixes" to complex social problems are threatening to produce a NIDS, but such a "fix" is unlikely to actually "solve" the problems that the component parts from which it is developing are supposed to address. The laws and databanks of a NIDS, once in existence, are likely to remain permanent bureaucratic fixtures with detrimental consequences. As Amitai Etzioni notes in *The Limits of Privacy*, a NIDS provides the government with more information than the East German secret police, the Stasi, had at the height of its power before it was abandoned in 1989 at the collapse of the regime and the fall of the Berlin Wall.¹⁵⁸

VIII. FUNDAMENTAL CRITIQUE OF NIDS

A national identification system fundamentally contradicts basic American principles and freedoms. The Constitution and the Bill of Rights afford protections against arbitrary government power. This scheme of protection includes federalism as the means of dividing power among different levels of state and national governments (vertical separation of powers). Also included

¹⁵⁵ See Robert Kuttner, *Why Not a National ID Card?*, WASHINGTON POST, Sept. 6, 1993, at A23.

¹⁵⁶ See *id.*

¹⁵⁷ For a critique of the national ID card, see, e.g., William Safire, *Threat of National ID*, NEW YORK TIMES, Dec. 24, 2001, at A15.

¹⁵⁸ See AMITAI ETZIONI, *THE LIMITS OF PRIVACY* 10 (Basic Books 1999) ("Corporations now regularly amass detailed accounts about many aspects of the personal lives of millions of individuals, profiles of the kind that until just a few years ago could be compiled only by the likes of the East German Stasi or other major state agencies, with huge staffs and budgets.").

in this scheme is the separation of powers that divides authority and incorporates checks and balances among the competing and cooperating legislative, executive, and judicial branches of government (horizontal separation of powers). One of the essential purposes of both federalism and separation of powers is to resist the threats to democracy and liberty posed by centralized power. These structural provisions of American governance specifically place liberty ahead of efficiency in fundamental importance. As Justice Louis Brandeis explained in 1926,

The doctrine of the Separation of Powers was adopted by the convention of 1787, not to promote efficiency, but to preclude the exercise of arbitrary power. The purpose was, not to avoid friction, but, by means of the inevitable friction incident to the distribution of the governmental powers among three departments, to save the people from autocracy.¹⁵⁹

“The American political system was set up to be inefficient, to divide power What ID numbers do is centralize power, and in a time when knowledge is power, then centralized information is centralized power.”¹⁶⁰

Similarly, the presumption and existence of unimpeded individual action protected by the political buffer around personhood undergirds individual rights. These “privileges and immunities”¹⁶¹ are represented, for example, by the right of citizenship, presumption of innocence, the burden of proof on the state, the prohibition of unreasonable search (with reasonableness based on particularized suspicion), and the prohibition against self-incrimination. These rights exist due to the individual’s nature as a person protected from arbitrary and unrestricted state action by the Constitution. They inhere in personhood and are degraded when one can only exercise them by virtue of possession of an ID card, number or place in a databank. In short, these rights may not be subject to ID checks before they can be exercised because political identity and personhood exist inherently in a free society.

Native citizenship is founded in birthright, not in governmental permission or action.¹⁶² Since the American system is one where “the citizens themselves are sovereign, citizenship is not subject to the general powers of their government.”¹⁶³ As Justice Hugo Black noted in his majority opinion in *Afroyim v. Rusk*, “The Constitution, of course, grants Congress no express

¹⁵⁹ *Myers v. United States*, 272 U.S. 52, 293 (1926).

¹⁶⁰ See Stolberg, *supra* note 27, at A11 (quoting Richard Sobel of Harvard University).

¹⁶¹ U.S. CONST art. IV, § 2 (“The citizens of each state shall be entitled to all the privileges and immunities of citizens in the several states.”); see also U.S. CONST amend. XIV, § 2 (“No State shall make or enforce any law which shall abridge the privileges or immunities of the citizens of the United States.”).

¹⁶² See SILVERSTEIN, *supra* note 106, at 110 (“[Several] cases from the 1950s and 1960s . . . produced a clear ruling from the [Supreme] Court . . . the government — even with both branches acting together — had no constitutional authority to strip an American of his or her citizenship.”).

¹⁶³ *Perez v. Brownwell*, 356 U.S. 44, 65 (1958) (Warren, J., dissenting).

power to strip people of their citizenship, whether or not in the exercise of the implied power to regulate foreign affairs or in the exercise of any specifically granted power.”¹⁶⁴ Furthermore, “The very nature of our free government makes it completely incongruous to have a rule of law under which a group of citizens temporarily in office can deprive another group of citizens of their citizenship.”¹⁶⁵ A NIDS would signal a return to parliamentary or monarchical sovereignty, where people’s identities are granted and defined by the government or monarch.¹⁶⁶ This contrasts with the system of popular and constitutional sovereignty that has developed since the Declaration of Independence and the U.S. Constitution, in which the government derives its power from the consent of the governed.¹⁶⁷

A NIDS, on the other hand, creates bureaucratic hindrances for citizens and immigrants in a free society. A NIDS turns citizens into the charges of the government, effectively reversing the nature of citizenship by birth expressed in the Fourteenth Amendment. Because consent by the governed is an active part of citizenship and of personhood, the government’s ability to give or take away identities destroys the proper relationship of the government to the governed. Since the government would issue (or deny) national ID cards, the government would in effect own and have to consent to people’s identities.¹⁶⁸ The proper balance of citizen and state becomes distorted when government bestows and deprives identity through documents, numbers, or places in databanks.

Document requirements degrade political and personal identity by abetting the reversal of the proper relationship of citizen to government identified in the Declaration of Independence¹⁶⁹ and the Preamble to the U.S. Constitution.¹⁷⁰

¹⁶⁴ *Afroyim v. Rusk*, 387 U.S. 253, 257 (1967).

¹⁶⁵ *Id.* at 268.

¹⁶⁶ *See generally* GEOFFREY MARSHALL, *PARLIAMENTARY SOVEREIGNTY AND THE PARLIAMENT* (Clarendon Press 1957) (discussing the role and authority of the Parliament in Great Britain).

¹⁶⁷ *See generally* WILLIAM EDWARD NELSON, *MARBURY V. MADISON: THE ORIGINS OF JUDICIAL REVIEW* (University Press of Kansas 2000) (providing a complementary analysis).

¹⁶⁸ Harvard University’s identification system may be a microcosm of this idea. Harvard’s ID cards state: “This card is the property of Harvard University.” *See* Harvard University ID Card. This suggests that Harvard University owns the identities of its students and employees.

¹⁶⁹ THE DECLARATION OF INDEPENDENCE ¶ 2 (U.S. 1776) (“We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness. That to secure these rights, Governments are instituted among Men, deriving their just powers from the consent of the governed, That whenever any Form of Government becomes destructive of these ends, it is the Right of the People to alter or to abolish it, and to institute new Government, laying its foundation on such principles and organizing its powers in such form, as to them shall seem most likely to effect their Safety and Happiness.”).

¹⁷⁰ *See* U.S. CONST. pmb. (“We the People of the United States in Order to . . . establish

A NIDS reverses the appropriate relationship from a system based on fundamental rights to one based on bureaucratic requirements. The rights to life, liberty, and the pursuit of happiness in the Declaration of Independence and the right to travel preceding the Constitution in the Articles of Confederation are undermined by a NIDS. The Articles of Confederation state:

The better to secure and perpetuate mutual friendship and intercourse among the people of the different States in this Union, the free inhabitants of each of these States . . . shall be entitled to all privileges and immunities of free citizens in the several States; and the people of each State shall free ingress and regress to and from any other State.¹⁷¹

The Supreme Court has repeatedly upheld the right to travel as a fundamental aspect of a free society.¹⁷²

Because American democracy was created by acts of consent of the governed in the establishment of the United States — as opposed to European democracies, which devolved from autocratic monarchies — the arrogation of the powers of identity formation by the state in a NIDS is profoundly contrary to the fundamental principles of a free society. This state identity bestowal also undermines the constitutional promise of a republican form of government¹⁷³ and implicates the problems for individual rights that the Founding Fathers associated with parliamentary sovereignty.

Centralization of too much information makes abuse possible and likely because the government has the power to coerce through the courts, police, and the military. The FAA travel and IRCA work requirements for ID restrict the

justice . . . secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America.”).

¹⁷¹ THE ARTICLES OF CONFEDERATION art. IV (Nov. 15, 1777).

¹⁷² See *Kent v. Dulles*, 357 U.S. 116, 125 (1958) (“The right to travel is part of the ‘liberty’ of which the citizen cannot be deprived without due process of law under the Fifth Amendment.”); see also *Saenz v. Roe*, 526 U.S. 489, 504-11 (1999) (holding that where a California statute limited welfare benefits for new state residents that would otherwise have been received by the new residents in their states of prior residence, the statute is unconstitutional, violating the Fourteenth Amendment right to travel); *Aptheker et al. v. Secretary of State*, 378 U.S. 500, 505 (1964) (holding that § 6 of the Subversive Activities Control Act of 1950, 50 U.S.C. § 785, unconstitutional on its face because it “too broadly and indiscriminately restricts the right to travel and thereby abridges the liberty guaranteed by the Fifth Amendment”). But see *Zemel v. Rusk*, 381 U.S. 1, 13 (1965) (finding the Secretary of State’s refusal to validate a citizen’s passport for travel to Cuba did not deny citizen due process, particularly in view of the President’s statutory obligation to protect citizens abroad).

¹⁷³ U.S. CONST. art. IV, § 4 (“The United States shall guarantee to every State in this Union a Republican Form Government, and shall protect each of them against Invasion; and on Application of the Legislature, or of the Executive (when the Legislature cannot be convened) against domestic Violence.”).

rights and benefits inherent to citizens in a free society. Such document requirements essentially facilitate denying employment and abridging the right to travel by proceeding from the assumption that everyone is illegal or suspect until proven otherwise. Under a NIDS, rights due to an individual as a person under the law cease to exist without proper identification.

The Fourth, Fifth, Ninth and Fourteenth Amendments' provisions on liberty mandate leaving constitutionally protected citizens alone; a person should go unintruded upon unless evidence amounting to a proper standard for intrusion is reached. The Fourth Amendment protects individuals against unreasonable search and seizure unless there is probable cause and particularized suspicion that an individual has committed or may be committing a crime. The combination of the right to remain silent in the First and Fourth Amendments¹⁷⁴ and the prohibition against self-incrimination in the Fifth Amendment¹⁷⁵ protect against requirements to provide identification absent probable cause.

A NIDS instead provides a back door around the Fourth Amendment by making it too easy for the state to get information. Because of the ease of access, centralized databanks make ID checks simple and routine. Checks of a databank and demands for identification without probable cause facilitate further routine intrusions that destroy the protections in personal and political spaces against scrutiny over one's person and effects.¹⁷⁶ Requirements for photo identification in order to work or travel, or the full development of a national ID databank, destroy one of the most basic freedoms accorded to Americans by the Constitution — the right to be left alone in privacy and anonymity unless there is a particularly compelling reason for intrusion.¹⁷⁷ They also degrade the protection provided by the Fourth and Fifth Amendments against "invasion of the 'sanctities of a man's home and the privacies of life.'"¹⁷⁸ Furthermore, these requirements erode the fundamental right to travel, a cornerstone of the right against self-incrimination and liberty in free society.

Personal liberty, which is guaranteed to every citizen under our constitution and laws, consists of the right of locomotion, to go where one pleases, and when, and to do that which may lead to one's business or pleasure, only so far restrained as the rights of others may make it necessary for the welfare of all other citizens. One may travel along the public highways or in public places; and while conducting themselves in a decent and orderly manner, disturbing no other, and interfering with the rights of no other citizens, there they will be

¹⁷⁴ See *Miranda v. Arizona*, 384 U.S. 436, 444, 445 (1966).

¹⁷⁵ See *Malloy v. Hogan*, 378 U.S. 1, 3 (1964).

¹⁷⁶ See Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 79 DENV. U. L. R. (forthcoming 2002).

¹⁷⁷ See *Kolender v. Lawson*, 461 U.S. 352 (1983).

¹⁷⁸ *Olmstead v. United States*, 277 U.S. 438, 473 (1928) (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

protected under the law, not only in their persons, but in their safe conduct. The constitution and the laws are framed for the public good, and the protection of all citizens, from the highest to the lowest; and no one may be restrained of his liberty, unless he has transgressed some law. Any law which would place the keeping and safe conduct of another in the hands of even a conservator of the peace, unless for some breach of the peace committed in his presence, or upon suspicion of felony, would be most oppressive and unjust, and destroy all the rights which our constitution guarantees.¹⁷⁹

The Fifth and Fourteenth Amendments prohibit the denial of liberty or property without due process. In contrast, a NIDS abets the denial of benefits because someone does not appear in the databank or because one's identity is revoked accidentally or deliberately. A NIDS removes a person's identity and transfers it to cards, numbers, and databanks.¹⁸⁰ Consequently, identity exists in a document rather than in a person, as people become paper, plastic, or electronic subjects.¹⁸¹

The creation of a NIDS poses a further threat to the principle of federalism embodied in the Constitution and the Tenth Amendment, whereby powers not delegated to Congress are reserved to the states.¹⁸² Under their police power, states have the authority to set their own law enforcement and licensing requirements. However, under a NIDS, as in the federalization of the driver's license, a license becomes a national document, thereby circumventing the states' police power and discretion in establishing identification standards.

Previously totalitarian nations like the former Soviet Union and South Africa, which once required internal passports to travel, are now moving away from identity documents and travel restrictions. The FAA and IRCA requirements, however, move toward the internal passport requirements that still exist in authoritarian countries like Thailand and China.¹⁸³ In fact, airline requirements often encourage the traveling public in the U.S. to carry their passport in order to fly domestically. Many people only begin to understand the implications of this requirement when they realize that they have to carry

¹⁷⁹ See *Pinkerton v. Verberg*, 78 Mich. 573, 584 (1889).

¹⁸⁰ See HENRY LOUIS GATES, *THIRTEEN WAYS OF LOOKING AT A BLACK MAN* xx-xxi, 207-08 (Vintage Books 1998).

¹⁸¹ See *id.* The Third Amendment, regarding the quartering of British soldiers, is also relevant to the case against a NIDS. A reason the framers resisted quartering is that the British soldiers were spies in the colonists' homes. By including a transistor microchip in a national ID, the card itself could become a spy in the home of Americans. It would also allow the government to track the movements of individuals. Cellular phone tracing by GPS and face recognition technology facilitate a reduction in probable cause necessary for searches and impose significant restrictions on the right to travel. See Diane E. Lewis, *Devices Keep Close Watch on Workplace: Biological Data May Replace ID Cards*, BOSTON GLOBE, June 24, 2001, at H1 (describing the possible effects and uses of such technology).

¹⁸² See U.S. CONST. amend X.

¹⁸³ See Philip Elmer-Dewitt, *Peddling Big Brother*, TIME, June 24, 1991, at 62.

documents meant for foreign travel in order to fly in the U.S. or when they forget to bring proper ID to an airport and are denied boarding.

If a NIDS were fully realized and everyone were issued a national ID card, citizens would eventually be required to carry and produce it upon official request. The regularity of such procedures would, in effect, make a police demand for ID a routine and reasonable request, without expectation of privacy, further circumventing Fourth Amendment protections.¹⁸⁴ The phrase “Your papers, please” used to be a joke in the U.S. Its implications are no longer amusing.

Like the assurances that Social Security numbers would only be used for tracking pension accounts, promises of privacy about a national identity or health databank could easily be compromised. Numerous other items of personal information required to maintain the databank’s function among 285 million people and the expansion of the number of agencies with access to some of its data both pose threats to privacy.¹⁸⁵ This has already begun to happen, as the HHS health records regulations would allow law enforcement and national security personnel access to medical information,¹⁸⁶ and other agencies seek access to the one another’s personal information databases.¹⁸⁷

The spontaneity of human existence, Robert Ellis Smith argues, disappears in the need to constantly carry “papers” on one’s person.¹⁸⁸ Simply traveling on a plane or getting a new job becomes impossible unless one has government ID. Getting in and out of one’s office become occasions for surveillance by the use of electronic ID cards whose use is regularly recorded, while presenting ID when going in and out of academic and residential buildings at many universities prepares students for such practice in the outside world.¹⁸⁹ Traveling with “EZ Pass” on tollways records where a driver was at certain

¹⁸⁴ See Shaun B. Spencer, *supra* note 176.

¹⁸⁵ See Jeffrey Rosen, *The Eroded Self*, N.Y. TIMES, Apr. 30, 2000, at 6-46. It could also be possible for governments to identify people with certain partisan affiliations (describing how “bits and pieces of stray data” in cyberspace meant to be private may be used to reconstruct identities of persons without permission).

¹⁸⁶ See 45 C.F.R. § 164.512 (2001).

¹⁸⁷ See Tanya N. Ballard, Report Says Agencies Must Protect Privacy When Sharing Data, GOVEXEC.COM, at <http://www.govexec.com/news/index.cfm?Mode=report&articleleid=19986> (April 20, 2001).

¹⁸⁸ See Robert Ellis Smith, *The True Terror Is In the Card*, N.Y. TIMES MAGAZINE, Sept. 8, 1996, at 58.

¹⁸⁹ See Matthew W. Granade & Adam S. Hickey, *Don’t Look: Harvard is Watching*, FIFTEEN MINUTES: THE MAGAZINE OF THE HARVARD CRIMSON, Apr. 3, 1997, at 8; see also Peter Wayner, *Closed-Door Policy*, N.Y. TIMES, Nov. 12, 1998, at 1.

hours of day or night.¹⁹⁰ In some instances, even walking around without proper ID may be cause for arrest.¹⁹¹

By combining information previously available only from multiple sources, a full NIDS, as in aggregate private databanks, would allow the government to create information mosaics. This would infuse information that, standing alone, might have been inconclusive without meaning gleaned from other sources. These collections of details on individuals' lives contribute to serious invasions of privacy, ongoing surveillance of lawful activities, and chilling effects on political involvement and expressions.

Each of the provisions coming together to form an informal NIDS constitutes bureaucratic surveillance in the name of solving social problems that a NIDS does not fix or that could be addressed more efficiently and less intrusively in other ways. A NIDS constitutes a general invasion of privacy by collecting and integrating more information than necessary about citizens and other residents.

The history of discriminatory and oppressive uses of identity badges, identity numbers, and databanks against Jews in Germany, Blacks during slavery in the U.S. and under Apartheid in South Africa, and Japanese-Americans during World War II in the U.S. should create wariness of the problems caused by quick fixes like identity documents. Any national system of identification would ultimately be offensive and intrusive to fundamental rights. A NIDS is a peril to these rights rather than a useful social tool. In essence, because a NIDS is itself a burgeoning bureaucratic mechanism used to collect people's private and public information, it cannot be adequately safeguarded against privacy invasions and abuses.

IX. TOWARD A WORLD WITHOUT NIDS

Personal spontaneity, seclusion in privacy, the dignity of personhood, and the pursuit of happiness need to be revered and preserved. Most individuals move freely around their homes, offices, and places of study without even considering that their movement might be recorded. Getting a new job, flying to anywhere in the U.S., and having the ability to travel the world freely are aspects of a free society. Individuals should feel free to exercise their freedoms. Personhood is enhanced when ID checks are rare and when totalitarian regimes collapse or are diminished.

The decision of England to abandon wartime ID cards, the passage of the Privacy Act of 1974,¹⁹² the suspending of the unique health identifier, and the halting of federalization of the driver's license show that the tide against a

¹⁹⁰ Frank Hotchkiss, *Odds and Ends in the Automotive World*, at http://www.americaontheroad.com/column/odds_ends.html (last modified Apr. 20, 2001).

¹⁹¹ *Cf.* *Kolender v. Lawson*, 461 U.S. 352 (1983) (discussing a statute requiring those loitering or wandering the streets to provide "credible and reliable" identification on request by a peace officer).

¹⁹² 5 U.S.C. § 552a (2000).

NIDS can be stopped and reversed. When people are not required to carry and show ID, the likelihood that it will be requested inappropriately is greatly reduced. When the standards of probable cause are respected before ID can be requested, the buffer around individuals is protected and the demand for ID is thus necessarily decreased.

The U.S. Supreme Court upheld this principle in *Kolender v. Lawson*.¹⁹³ In a majority opinion by Justice Sandra Day O'Connor, the Court held a California statute requiring persons "who loiter or wander the streets to identify themselves and to account for their presence when requested by a peace officer" unconstitutional because it was "vague on its face within the meaning of the Due Process Clause of the Fourteenth Amendment by failing to clarify what is contemplated by the requirement that a suspect provide a 'credible and reliable' identification."¹⁹⁴ The statute involved an inappropriate demand for identification, as it circumvented the Fourth Amendment's requirement that an officer have probable cause or reasonable suspicion to search or seize a suspect.¹⁹⁵ With this decision the Supreme Court supported the right to go about one's business without the likelihood of being stopped by the police.

Credible and reliable identification should depend more on the individual's credibility, such as the ability to answer questions or provide one's name and address,¹⁹⁶ than on the nature or presence of a government-issued ID. Possession of a plastic card should not be the determinative factor of credibility, lest a person's identity be conflated with a mere document.

In addition, Congress wisely decided to abandon the plan for a National Data Center in the 1960's due to citizen uproar.¹⁹⁷ Similarly, in a 1981 cabinet

¹⁹³ 461 U.S. 352 (1983).

¹⁹⁴ *Id.* at 353-54.

¹⁹⁵ In *Brown v. Texas*, the Supreme Court, in an opinion by Chief Justice Warren Burger, held that the application of a Texas statute requiring Brown to identify himself violated the Fourth Amendment because the officers lacked the reasonable suspicion necessary to detain Brown. See *Brown v. Texas*, 443 U.S. 47, 52-53 (1979). The statute at issue, however, provided that an individual need only provide his name and address "to an officer 'who has lawfully stopped him and requested the information.'" *Id.* at 49 & n.1. Thus, though the arrest was unlawful, the statute provides a better framework and definition of "credible identification" than the statute at issue in *Kolender v. Lawson*, 461 U.S. 352.

¹⁹⁶ In *Brown v. Texas*, the Supreme Court, in an opinion by Chief Justice Warren Burger, held that the application of a Texas statute requiring Brown to identify himself violated the Fourth Amendment because the officers lacked the reasonable suspicion necessary to detain Brown. See *Brown v. Texas*, 443 U.S. 47, 52-53 (1979). The statute at issue, however, provided that an individual need only provide his name and address "to an officer 'who has lawfully stopped him and requested the information.'" *Id.* at 49 & n.1. Thus, though the arrest was unlawful, the statute provides a better framework and definition of "credible identification" than the statute at issue in *Kolender v. Lawson*, 461 U.S. 352.

¹⁹⁷ See GARFINKEL, *supra* note 46, at 14. A 1969 poll by the Harvard University Program on Technology and Society found that 56% of Americans opposed development of the National Data Center. See *id.*

meeting, adviser Martin Anderson convinced President Reagan not to require a national ID card by suggesting “another way that I think is a lot better. It’s a lot cheaper. It can’t be counterfeited. It’s very lightweight, and impossible to lose. It’s even waterproof. All we have to do is tattoo an identification number on the inside of everybody’s arm.”¹⁹⁸ Anderson’s statement about the perils of national ID cards and immigration laws prevented a major step in the direction of a NIDS. In 1998, Clinton adviser Ira Magaziner helped table the unique health identifier plan after protests in a public hearing and prominent media coverage.¹⁹⁹

These acts, the abandonment of the proposed National Data Center, freezing funding for implementing the DOT federalized driver’s license, and the tabling of the unique health identifier requirements provide time for thoughtful actions and remind us that encroachments on fundamental rights can be stopped and reversed.²⁰⁰ Today, U.S. citizens can once again assert their rights to privacy and liberty by restricting the collection and access of data by the government through ID requirements like those of the IRCA and the FAA.²⁰¹ Each of these steps against a NIDS can be repeated to keep our society free from unwarranted governmental intrusion.

X. CONCLUSION

The creation of a national identification system contradicts the constitutional principles of liberty, burden of proof on the government, and federalism. When personhood depends on governmental identification systems, people lose their fundamental right to political and personal identity and the buffer that protects them from state intrusion. The implementation of a NIDS diminishes liberty and personhood, and weakens constitutional protections against search and seizure. Databank and document requirements profoundly degrade the moral economy of identity, personhood, and human dignity that undergird a free society.

Federal laws and regulations that monitor citizens’ lawful activities via national ID numbers, databanks, and cards increase the government’s surveillance capacity and power. The IRCA, IIRIA, WRA, HIPAA, and FAA ID/CAPS propose national databanks or IDs as solutions for problems with

¹⁹⁸ MARTIN ANDERSON, *REVOLUTION 276* (Harcourt Brace Jovanovich 1988).

¹⁹⁹ See Ira Magaziner, Remarks at the Harvard University Third Biennial International Conference on Internet & Society (June 1, 2000); see also Remarks at The Harvard Information Infrastructure Project: Creating a Competitive Global Electronic Marketplace (Feb. 22, 1999). Concern about the HID plan was so widespread that Clinton tabled implementing the plan until Congress could safeguard privacy. See Vice President Al Gore, Remarks at New York University Commencement (May 14, 1998); Tipper Gore, Remarks at the National Alliance for the Mentally Ill: From Discovery to Recovery (July 16, 1998); see also James, *supra* note 32, at N6; Stolberg, *supra* note 27, at A1.

²⁰⁰ See Robert Ellis Smith, *SSNs Nixed From Licenses*, *PRIVACY JOURNAL*, Oct. 1999, at 1.

²⁰¹ See GARFINKEL, *supra* note 46, at 257-271.

B.U. J. SCI. & TECH. L.

illegal immigration, health costs, nonpayment of child support, and airline security. These databanks and ID requirements are typically ineffective and overreaching reactions that degrade privacy and liberty. Though terrorism is more threatening, it is but the most recent justification for extending such a system. These standards are articulated here as a reminder of what needs to be protected and a basis for reclaiming our free and democratic way of life in a post-terror society.

The power that the government gains through the centralization and monitoring of personal information vastly outweighs the supposed benefits. The proposed solutions through databanks and IDs are illusory and should be abandoned for fair and effective remedies targeted to specific problems and that respect people's rights. A culture of freedom depends upon upholding rights that flow from personhood. The moral economy of personhood and identity can only thrive if the extension of a NIDS and degradation of political and personal identity are reversed.

The prevention of a NIDS would preclude a society in which personhood is commodified and in which individuals are judged based not on their actions but on their numerical location in a databank. A NIDS hastens Orwell's *Nineteen Eighty-Four*, Huxley's *Brave New World*, and Black's *IBM and The Holocaust*. It degrades the very nature of personhood that underlies basic liberties in a free society. The imperatives of the tragic events of September last notwithstanding, a NIDS stands fundamentally opposed to the founding principles of this nation and must ultimately be abandoned.