Harvard Journal of Law & Technology
Volume 15, Number 2 Spring 2002

THE DEMEANING OF IDENTITY AND PERSONHOOD IN NATIONAL IDENTIFICATION SYSTEMS

Richard Sobel[*]

TABLE OF CONTENTS

---

* Richard Sobel is a Senior Research Associate in the Program in Psychiatry and the Law at Harvard Medical School and a former fellow at the Berkman Center for Internet and Society at Harvard Law 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 as 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, Aug. 7–10, 2000. He would like to thank Daniel Solove and Shaun Spencer for their comments, and Wendy Netter, Kathryn Gainey, Ryan Billings, Anjan Choudhury, Jason Crowley, and Michael Krasnovsky for research assistance, and Darcy Paul, Emily Pollack, and Allen Nunnerly for editorial assistance. He would also like to thank the Office of Public Interest Advising and the Howe Grant for Civil Rights and Civil Liberties at Harvard Law School for their support. A pre-September 11th version of this analysis appeared as *The Degradation of Political Identity under a National Identification System*, 8 B.U. J. SCI. & TECH. L. 37 (2002) from which portions, especially Sections IV to VI, are drawn here with permission.

I. INTRODUCTION

Even before the attacks on New York City and Washington, D.C. on September 11, 2001, America was moving toward a system of national identification numbers, databanks, and identity cards that conflicts with basic American principles and freedoms. That movement and its recent acceleration contradict the constitutional and philosophical bases of democratic government and undermine the fundamental foundations of political and personal identity. While the problems a national identification system ("NIDS") is intended to solve occur in relatively authoritarian societies, the troubles created by such a bureaucratic scheme plague free societies as well by foreclosing vital options and opportunities. A NIDS demeans political and personal identity by transforming personhood from an intrinsic quality inhering in individuals into a quantity designated by numbers, represented by physical cards, and recorded in computer databanks. Rather than constituting an inherent part of personhood and dignity, ersatz-identity becomes an attribute of bureaucratic and computerized systems. The growing impact of a NIDS on due process, freedom from unreasonable search, free expression, freedom of travel, the right to employment, separation of powers, and federalism makes this issue particularly appropriate for contemporary constitutional and policy analysis.

As privacy advocate Robert Ellis Smith has argued, the ongoing developments toward a national identification system fundamentally contradict the bases of the American system of governance.[1] In an open democratic society based on Lockean and Jeffersonian principles, the government derives its powers from the consent of the gov-

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

erned.[2] Similarly, the United States Constitution was developed to circumscribe state power through federalism and the designation of fundamental rights. As a consequence, activities such as work, travel, and medical care are to be readily available and respectful of privacy in free societies. In contrast, in authoritarian societies, the government bestows, or denies, identities and opportunities through identification numbers or documents and intrudes into individuals' lives. In addition, because the government has the power to coerce and to control, people confront force when they seek to disobey government directions, including requirements for identification.

Several pre-September 11th ("9/11") databank and identification laws and regulations provided the basis by the mid-1990s for developing a bureaucratic surveillance system through the combination of data collection and identification requirements. Even before its extension, such a national identification system implemented by the government contradicted and circumvented basic constitutional rights, such as privacy. Moreover, a NIDS demeans the political values of identity by substituting ersatz-identities for identities based on personhood.

The fundamental identity and personhood that identification systems challenge are bulwarks for individual development. "[T]he 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] Individuals have the right to remain free from intrusion because personhood and fundamental rights in an open society create a political space, or buffer, around the individual that permits free expression and unencumbered action.

In a free society under a constitution of enumerated and delegated powers, a regime develops based upon and generating basic, retained rights for individuals as persons. This system derives from the overarching principle of governance by consent. This dimension creates a buffer around individuals and against state action. Individuals inherently possess rights and political identities.

However, under a national identification system, rights are derived from credentials. People obtain ersatz-identities based on identification documents and numbers or places in databanks. The require-

2. *See* JOHN LOCKE, SECOND TREATISE OF GOVERNMENT (Hackett 1980) (1690); THE DECLARATION OF INDEPENDENCE (U.S. 1776).

3. Thornburgh v. Am. Coll. of Obstetricians & Gynecologists, 476 U.S. 747, 777 n.5 (1986) (Stevens, J., concurring) (quoting Charles Fried, *Correspondence*, 6 PHIL. & PUB. AFF. 288–89 (1977)).

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

ment to prove identity or appear in a national databank in order to obtain and exercise certain rights demeans the foundation on which free governance is based. The use of personal information for governmental action without consent or due process violates liberty and property rights.

The existence of databanks and identification schemes implies that society has a right to surveil its subjects and to define individual identities separate from the inherent nature of personhood. The difference appears in the contrast between a system with a constitutional right to be free from unreasonable search as a person and a system with police privileges to search anyone at will. Freedom from search by virtue of personhood contrasts with obtaining that right only after one has proved to be a citizen through identification and thus deserving of that right or privilege. When one may only exercise fundamental rights with proper documentation, the nature of political and personal identity is degraded.

Personhood is a fundamental element of both personal and political identity[5] that implies a "bundle of rights."[6] As Justice William O. Douglas noted about the importance of personhood in his concurrence to *Roe v. Wade* in *Doe v. Bolton*, "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.[7] In his dissent in *United States v. White*, Justice Douglas advised that:

> 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.[8]

---

5. *See* JANNA MALAMUD SMITH, PRIVATE MATTERS: IN DEFENSE OF THE PERSONAL LIFE 28–29 (1997); *see also* ROBERT ELLIS SMITH, A NATIONAL ID CARD: A LICENSE TO LIVE 3, 7 (2002) (discussing personhood as autonomy and citing J. Braxton Craven, Jr., *Personhood: The Right to be Let Alone*, 1976 DUKE L.J. 699 (1976), and Justice Sandra Day O'Connor's majority opinion in *Planned Parenthood of Southeastern Pennsylvania v. Casey*, 505 U.S. 833 (1992)).

6. *See* Christopher Pollmann, Capitalist Development, Personal Identity and Human Rights, Presentation to the Harvard Law School Human Rights Program (Feb. 14, 2002) (citing Catherine MacKinnon's gloss in TOWARD A FEMINIST THEORY OF THE STATE on Kant in FUNDAMENTAL PRINCIPLES OF THE METAPHYSICS OF ETHICS).

7. Doe v. Bolton, 410 U.S. 179, 211 (1973) (Douglas, J., concurring) (referring to *Roe v. Wade*).

8. United States v. White, 401 U.S. 745, 764 (1971) (quoting RAMSEY CLARK, CRIME IN AMERICA: OBSERVATIONS ON ITS NATURE, CAUSES, PREVENTION AND CONTROL 287 (1970)).

The creation of a NIDS undermines the basic principles of personhood, sovereignty, due process, and federalism in the U.S. Constitution while ultimately providing questionable utility. The increased reach and effects of a NIDS on these fundamental issues requires the exploration and contemplation of its constitutional and policy implications.

II. THE COMPONENTS OF A NIDS AND ITS INITIAL DEVELOPMENT

Even before the recent calls for a national ID card, a NIDS was developing from the combination of government databanks and ID requirements. The five basic parts of an incipient NIDS are the Immigration Reform and Control Act of 1986 ("IRCA"),[9] the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 ("IIRIRA"),[10] the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 ("Welfare Reform Act"),[11] the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"),[12] and the Federal Aviation Administration ID requirement and Computer Assisted Passenger Screening system ("CAPS").[13] Other governmental and private databank and ID requirements also contributed to a NIDS both before and after 9/11. These five databanks constitute an informal NIDS, of which a national ID (or national ID number) is only one component.

Each of the major elements of the NIDS has a government identification or government databank component. The responses to terrorism and subsequent calls for a national ID may accelerate and expand the integration of these and other existing databanks and government ID requirements. While all of these systems have law enforcement implications, this Article emphasizes civil and administrative databanks and ID schemes. Other databanks involve on law enforcement activities, such as the Federal Bureau of Investigation's ("FBI") National Crime Information Center 2000 ("NCIC"). This distinction may

---

9. Immigration Reform and Control Act of 1986, Pub. L. No. 99-603, 100 Stat. 3359 (1986) [hereinafter IRCA].

10. Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, 110 Stat. 3009-546 to 3009-724 (1996) [hereinafter IIRIRA].

11. Personal Responsibility and Work Opportunity Reconciliation Act of 1996, Pub. L. No. 104-193, 110 Stat. 2105 (1996) [hereinafter Welfare Reform Act].

12. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) [hereinafter HIPAA].

13. For a complementary analysis that includes educational databanks, see Charlotte Twight, *Watching You: Systematic Federal Surveillance of Ordinary Americans*, 4 INDEP. REV. 165 (1999) [hereinafter *Watching You*]; *see also* CHARLOTTE A. TWIGHT, DEPENDENT ON D.C.: THE RISE OF FEDERAL CONTROL OVER THE LIVES OF ORDINARY AMERICANS 235–76 (2002) [hereinafter DEPENDENT ON D.C.].

be eroding, however, in response to recent calls to integrate private with public databanks, and criminal justice databanks with credit card and travel histories, to create a "trusted traveler system" as discussed below.[14]

The Immigration Reform and Control Act of 1986 requires employers to have employees fill out and sign an I-9 verification form to prove that they are U.S. citizens or have governmental permission to work in the United States. To verify citizenship or government approval of employment, employers are also required to ask employees within three days of commencing employment to provide government identification, such as a passport or a driver's license plus a Social Security card. Employers may be fined up to $10,000 for each undocumented alien employed.[15]

In 1996, IIRIRA extended IRCA.[16] IIRIRA requires employees to provide identification to prove citizenship or government permission to work.[17] In addition, IIRIRA provides for a five- to seven-state "Pilot Program for Employment Eligibility Verification," which allows for databank checks for Social Security numbers.[18] It also provides funding for the "Machine-Readable-Document Pilot Program" in Iowa and the "Criminal Alien Identification System" Pilot Program.[19] IIRIRA calls for the standardization of birth certificates and driver's licenses in all states including Social Security numbers ("SSNs")[20] and for the development of prototype counterfeit-resistant Social Security cards.[21]

The Welfare Reform Act of 1996 mandates the creation of a federal databank to track all newly hired employees. The National Directory of New Hires ("New Hires Databank") 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 transmitted to a national databank at the Department of Health and Human

---

14. Tom Ramstack, *ID Card in Works for Air Passengers*, WASH. TIMES, Jan. 31, 2002, at A1.

15. 8 U.S.C. § 1324a(e)(5) (2001).

16. IIRIRA, Pub. L. No. 104-208, 110 Stat. 3009-546 to 3009-724 (1996).

17. 8 U.S.C. § 1324a(b) (as amended by Pub. L. No. 104-208, § 412(a), 110 Stat. 3009-667 (1996)); *see also* Pub. L. No. 104-208, 110 Stat. 3009-656 (1996) (discussing pilot program that allows attestation of U.S. citizenship without being required to present documents).

18. IIRIRA, Pub. L. No. 104-208, § 404, 110 Stat. 3009-664 to 3009-665 (1996). Interestingly, Section 404(h)(2) of IIRIRA states, "[n]othing 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.* at 3009-665.

19. IIRIRA, Pub. L. No. 104-208, §§ 326, 401–05, 110 Stat. 3009-630, 3009-655 to 3009-666 (1996).

20. IIRIRA, Pub. L. No. 104-208, § 656, 110 Stat. 3009-716 (1996). *But see infra* note 265 on its repeal.

21. Development of Prototype of Counterfeit-Resistant Social Security Card, Pub. L. No. 104-208, § 657, 110 Stat. 3009-719 (1996).

Services ("HHS"). The New Hires Databank's stated purpose is to assist federal and state officials in locating parents who owe child support by tracking them from job to job and state to state, but it affects all newly hired employees. Thus, over time it would include almost the entire labor force of 120 million people.[22] As noted below, its uses have now been expanded to tracking repayment of educational loans.

The Health Insurance Portability and Accountability Act of 1996 was passed in an effort to make health insurance transferable when people change employers.[23] HIPAA mandated the development of both a unique health identifier ("UHID") and a national electronic collection system for personal health care data. The goal of a unique national health identifier was to facilitate the tracking of patients, health care providers, health plans, and health care events paid for by public or private funds. It was meant to assist in monitoring patients' health conditions, recording changes in providers, obtaining patients' old records, streamlining billing, and creating a national database to analyze costs or perform research studies. All information from patients' medical records would be included in this electronic system.[24]

Since October 1995, the Federal Aviation Administration ("FAA") has required airlines to ask passengers to identify themselves with government-issued photo identification.[25] For this purpose, pas-

---

22. *See* Robert Pear, *Vast Worker Database to Track Deadbeat Parents*, N.Y. TIMES, Sept. 22, 1997, at A1.

23. *See* Sheryl Gay Stolberg, *Health Identifier for All Americans Runs Into Hurdles*, N.Y. TIMES, July 20, 1998, at A1; *see also* Richard Sobel, *No Privacy for All? Serious Failings in the HHS Medical Records Regulations*, 5 J. BIOLAW & BUS. (forthcoming 2002).

24. Besides the provisions for a unique health identifier ("UHID"), perhaps based on the Social Security number, or a biometric feature, the unsuccessful Health Security Act of 1993 that preceded HIPAA would have implemented a "health security card." President Clinton displayed a model of the card in his speech to Congress proposing the Health Security Plan. *See* Adam Clymer, *Clinton Asks Backing for Sweeping Change in the Health System: Address to Nation*, N.Y. TIMES, Sept. 23, 1993, at A1.

25. *See* E-mail from Ned Preston, Historian, Federal Aviation Administration ("FAA"), to Wendy J. Netter, Student, Harvard Law School (Jan. 25, 2002) (on file with author); Chris Woodyard, *Losing Photo ID Can Make Boarding Plane Next to Impossible*, USA TODAY, Jan. 3, 2000, at 2B; *see also* FAA, *Civil Aviation Security Passenger Information*, *at* http://cas.faa.gov/faq.html (last visited Feb. 23, 2002). The FAA has refused to release the information contained in Security Directive 96-05, which is believed to be the basis for this requirement. *See* NetAction, *Airport Security and Passenger Privacy* (Sept. 23, 1996), *at* http://www.netaction.org/notes/notes4.html (last visited Feb. 26, 2002) (discussing FAA's refusal to release the exact wording of the directive). Under Exemption 3 of the Freedom of Information Act ("FOIA"), 5 U.S.C. § 522 (2001), information is exempted from this requirement when matters are:

> (3) 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

sengers typically need to provide a driver's license with a photo, a passport, or a governmental agency ID card.[26] Though ID is not strictly required by the FAA, it is the standard procedure for air travel.[27] CAPS requires that all passengers be profiled at check-in.[28] Those who fit a certain profile, such as passengers paying for tickets in cash or traveling one-way, are subjected to increased scrutiny, including a more intrusive search of their carry-on and checked luggage.[29]

Two of these acts, the Welfare Reform Act and IIRIRA, also call for upgrading identification documents. Both include provisions that require the Social Security Administration ("SSA") to upgrade the actual Social Security card.[30] As noted above, IIRIRA establishes Iowa's Machine-Readable-Document Pilot Program, in addition to the Criminal Alien Identification System Pilot Program that is tied to employment scrutiny.[31] The act provides that federal agencies "may not accept for any official purpose a certificate of birth" or driver's li-

---

criteria for withholding or refers to particular types of matters to be withheld.

5 U.S.C. § 522(b)(3). This requirement began as part of non-binding guidelines issued by the FAA as "having a photo I.D. available." *See* U.S. Department of Transportation, *Statement of Secretary of Transportation Federico Pena on Additional Increases in Security* (Oct. 1, 1995), *at* http://ww.dot.gov/affairs/1995/sec.htm.

26. Though originally a security measure, the airlines enforced the ID requirement in part to enhance revenue. *See* Robert Ellis Smith, *Airlines Demanding ID, But Not for Security*, PRIVACY J., Nov. 1995, at 1.

27. *See* Letter from Adm. Cathal L. Flynn, Associate Administrator for Civil Aviation Security, Federal Aviation Administration, to Robert Ellis Smith, Publisher, PRIVACY J. (Jan. 14, 1996) (on file with author) ("[T]he actual presentation of identification by the passenger is not absolutely required, and there is currently no prohibition against allowing someone on an aircraft without such identification . . . [with] the use of alternative measures that provide the same level of security protection."); *see also* Civil Aviation Security, *Passenger Information*, *at* http://cas.faa.gov/faq.html (last visited Feb. 25, 2002) ("The FAA does not prohibit the airline from transporting any passenger who does not present a photo ID. Airlines have available to them alternative procedures that allow them to transport passengers without ID."); Preston, *supra* note 25.

28. *See Status of Aviation Security Efforts With a Focus on the National Safe Skies Alliance and Passenger Profiling Criteria: Hearing Before the House Comm. on Transp. and Infrastructure*, 105th Cong. 26 (1998) [hereinafter *Hearing*] (statement of Adm. Cathal L. Flynn, Associate Administrator for Civil Aviation Security, Federal Aviation Administration).

29. *See id.*; Dorothy Rabinowitz, *Critic at Large: Hijacking History*, WALL ST. J., Dec. 7, 2001, at A18; *see also* Exec. Order No. 12949, *reprinted as amended in* 50 U.S.C. § 1822 (2001) (permitting the legal "physical search for foreign intelligence" without a court order or a warrant).

30. IIRIRA, Pub. L. No. 104-208, § 657, 110 Stat. 3009-719 (1996); Welfare Reform Act, Pub. L. No. 104-193, § 111, 110 Stat. 2105 (1996).

31. IIRIRA, Pub. L. No. 104-208, §§ 326, 401–05, 110 Stat. 3009-630, 3009-655 to 3009-666 (1996).

cense that fails to comply with federal regulations.[32] The act also includes a federal funding provision to link birth and death records.[33]

Other databank and ID requirements also contribute to a NIDS. Department of Transportation ("DOT") and SSA requirements mandate upgrading 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, IIRIRA required that, by October 1, 2000, all state driver's licenses must display a SSN on or in driver's licenses.[34] A federalized driver's license would include the licensee's name, address, phone number, date of birth, physical descriptors, a photo, a social security number, and perhaps a biometric identifier. 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.[35] In response in April 1996, the Georgia Legislature passed a bill that mandates fingerprints for Georgia driver's licenses.[36] California, Florida, and Hawaii require fingerprints to apply for driver's licenses.[37] IIRIRA provisions for a federalized driver's license (or birth certificate) would deny federal benefits unless these ID documents incorporated social security numbers.[38] As a consequence, someone with an old driver's license (or birth certificate) would not be eligible to receive federal benefits. This requirement would force states, like Vermont, that do not require a photo on a driver's license to include one.[39]

Currently, the Problem Drivers Pointer System ("PDPS") and Commercial Driver's License System ("CDLIS") facilitate the inter-

---

32. *Id.* at § 656, 110 Stat. 3009-716.

33. *Id.*

34. *See* IIRIRA, *supra* note 20; Robert Ellis Smith, *Congress is Out of Step on Social Security Numbers*, PRIVACY J., Oct. 1996, at 1.

35. *See* Frank James, *ID-Number Proposals Raise Issue of Privacy*, CHI. TRIB., Aug. 31, 1998, at N6.

36. *See* GA. CODE ANN. tit. 40, § 40-5-28 (1996); 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 (last visited Feb. 23, 2002).

37. *See* J. Radick, *What's Required on a Driver's License*, PRIVACY J., July 2001, at 3; CAL. VEH. CODE § 12800 (West 1995) (neither Florida nor Hawaii have passed enabling legislation, although Hawaii's fingerprinting requirement is set forth in an Agency Statement issued by its Department of Transportation). However, legislatures in twenty-four states have passed laws allowing drivers to remove their SSNs from driver's licenses.

38. *See* Twight, *Watching You*, *supra* note 13, at 173.

39. At least five states, including Vermont and New Jersey, do not require photos on driver's licenses. *See* Ross Kerber, *All 50 States Agree to Upgrade Driver's Licenses Seeking to Improve Security Features*, BOSTON GLOBE, Jan. 13, 2002, at C1; Iver Peterson, *Hold That Pose: Driver's License Plan Slowed*, N.Y. TIMES, Apr. 3, 2002, B5; *Couple Sues Over N.J. Photo Licenses*, THE TRENTONIAN, May 3, 1985, A10.

state sharing of information on problem drivers.[40] In the aftermath of 9/11, the American Association of Motor Vehicle Administrators ("AAMVA") announced proposals to cooperate with upgrading the driver's license with security features, such as a fingerprint or digital photograph, which would turn it into a de facto national identity card.[41] These licenses would also include barcodes or magnetic strips so they could be electronically scanned. The plan would involve linking the driver's license databases with law enforcement agencies.[42]

Citizens currently cannot obtain or renew a passport without providing a taxpayer identification number, usually a SSN, under penalty of a $500 fine levied by the Internal Revenue Service ("IRS").[43] The intent of the provision is to allow the IRS to check on tax compliance by foreigners or citizens living abroad, yet the system is administered by the State Department, which issues passports to citizens living in the United States.[44] This provision is not subject to the Code of Fair Information Practices, which would prevent information about a person from being obtained "for one purpose from being used or made available for other purposes without his consent."[45] Thus, this requirement infringes the right to travel because individuals cannot get their passports renewed unless they provide a SSN.[46]

The Health Care Financing Administration, created in 1977 to manage the Medicare and Medicaid federal health programs, has set up a database to monitor the quality of health care among senior citizens. The database tracks the billing records and the performance of

---

40. Electronic Privacy Information Center, *Your Papers, Please: From the State Drivers License to a National Identification System* (Feb. 2002) at 7, *available at* http://www.epic.org/privacy/id_cards/yourpapersplease.pdf [hereinafter EPIC Report]. IIRIRA imposed it only for commercial driver's licenses. *See* Quaring v. Peterson, 728 F.2d 1121 (8th Cir. 1984), *aff'd by* Jensen v. Quaring, 472 U.S. 478 (1985); *see also* Bureau of Motor Vehicles v. Pentecostal House of Prayer, Inc., 380 N.E.2d 1225 (Ind. 1978) (prohibiting denial of a driver's license without a photo).

41. *See* EPIC Report, *supra* note 40, at 12; *see also* Kerber, *supra* note 39, at C1.

42. The old AAMVA standard advocated the use of barcodes and magnetic strips. *See* AAMVA National Standard for the Driver License/Identification Card (June 30, 2000) *at* http://www.aamva.org/Documents/stdAAMVADLIDStandrd000630.pdf (last visited Feb. 26, 2002).

43. 26 U.S.C. § 6039E (1994). This provision permits the Secretary of Treasury to exempt any class (e.g., resident citizens) as long as the exemption would not inhibit the section's purpose. The passport application provides that "all questions on this matter should be referred to the nearest IRS office." Inquiries by Ryan Billings, Student, Harvard Law School, to the Live Telephone Tax Assistance Office of the IRS on March 13–15, 2002 found no one familiar with the requirements or the exemption.

44. *See* Stephen Krüger, *Passports, Social-Security Numbers and 26 USC § 6039E*, 20 W. ST. U. L. REV. 1 (1992) (arguing that § 6039E is unconstitutional as a bill of attainder and a violation of the privilege against self-incrimination).

45. SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973) [hereinafter HEW REPORT].

46. *Id.*

over 9,000 Medicare-certified health care providers. Patients are asked, among other questions, personal information about "socially inappropriate behavior," "a sense of failure," and depression.[47] The database system has been scaled back, but not abandoned, because of public protest.[48] In late December 2001, HHS also proposed a Medicare databank to centralize all Medicare patient records under the routine use exemption to the Privacy Act of 1974.[49]

There are also several educational databanks that collect records on students as soon as they enter school, and contribute to a "nationwide data-exchange network."[50] The Goals 2000, Improving America's Schools, and School to Work Opportunity Acts created "vast and potentially ill-protected computerized records about children and families throughout America."[51] The National Center for Education Statistics tracks children's educational records and creates a "spider web of data exchange."[52] Data collection also includes socioeconomic status, learning disabilities, medical, behavioral, and family problems.[53] There are provisions for restricting the use and disclosure of individually identifiable data for statistical purposes, but they include exceptions for releasing individual data to the U.S. Comptroller General and the Secretary of Education.[54] Moreover, there are exceptions for disclosures without consent for routine uses and for civil or criminal law enforcement activity.[55] The "laws don't block the government's collection of individually identifiable information, only its use."[56]

The Bank Secrecy Act of 1970 created permanent records of all individuals' checks, deposits, and other banking activities. The statute also required similar recordkeeping for credit-card companies.[57] The act provided for informal access to records by law enforcement personnel. In *California Bankers Ass'n v. Shultz*, the Supreme Court held

---

47. Robert O'Harrow, Jr., *U.S. to Start Gathering Patient Data; Care Survey Draws Privacy Objections*, WASH. POST, Mar. 11, 1999, at A1.

48. *See* Stolberg, *supra* note 23.

49. For a discussion of how linking under routine use exemptions, and computer matching and integration of databanks violates Fair Information Practice consent principle, see Twight, *Watching You*, *supra* note 13, and Todd Robert Coles, Comment, *Does the Privacy Act of 1974 Protect Your Right to Privacy? An Examination of the Routine Use Exemption*, 40 AM. U. L. REV. 957, 975 (1991).

50. Twight, *Watching You*, *supra* note 13, at 186.

51. *Id.*

52. *Id.* at 187.

53. *Id.* at 167, 185–90.

54. *Id.* at 189.

55. *Id.*

56. *Id.*

57. Bank Secrecy Act, Pub L. No. 91-508, 84 Stat. 1114 (1970); Twight, *Watching You*, *supra* note 13, at 191.

that the act does not implicate Fourth Amendment protection.[58] While not developing a databank per se, the act creates the records and the potential mechanism for keeping track of all financial transactions in a central databank.[59] A December 1998 Federal Deposit Insurance Corporation ("FDIC") proposal for banks to scrutinize customer transactions — "in effect would have mandated warrantless searches of private financial records" — was put in abeyance.[60] Similar provisions, however, were resurrected after 9/11.[61]

Besides these databanks, there are numerous other government databanks that include records on over 280 million Americans. The Privacy Act requires a yearly census of databanks, but one has not been conducted recently.[62] The second annual report of the Privacy Act in June, 1977 showed a total of 6,753 "systems of records," as defined under the act, with data on 3.8 billion individual personal records. Among the largest are the SSA databank, tied to the Social Security card and now used regularly to verify SSNs for private employees. The IRS also has tax records on over 250 million Americans, but it has strong privacy protections.[63]

Moreover, the integration of public databanks with private data collections on purchasing patterns represents an extension of the NIDS. In seeking protection for the American people against terrorist attacks, former President Bill Clinton, calling himself a "fanatic civil libertarian,"[64] suggested that the federal government acquire the same

58. Cal. Bankers Ass'n. v. Shultz, 416 U.S. 21 (1971); United States v. Miller, 425 U.S. 435 (1976). The Right to Financial Privacy Act, Pub. L. No. 95-630 (1978) (codified as amended at 12 U.S.C. § 3402) was meant to restore some protection of financial records by requiring subpoena, search warrant, or government certification.

59. *See generally* Steven A. Bercu, *Toward Universal Surveillance in an Information Age Economy: Can We Handle Treasury's New Police Technology?*, 34 JURIMETRICS J. 383 (1994).

60. Twight, *Watching You*, *supra* note 13, at 190; *see also* TWIGHT, DEPENDENT ON D.C., *supra* note 13, at 267–68.

61. Robert Ellis Smith, *What's in the New Anti-Terrorism Law?*, PRIVACY J., Nov. 2001, at 7–8; *see also* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, §§ 311, 358 (2001).

62. *See generally* Office of Mgmt. & Budget, Second Annual Report on the Privacy Act of 1974 (1977); E-mail from Robert Ellis Smith, Publisher, PRIVACY J., to author (Feb. 11, 2002) (on file with author).

63. The IRS requires "a privacy impact assessment" mechanism for new computer systems and has a privacy advocate office. *See generally* Office of Privacy Advocate, Internal Revenue Serv., Privacy Impact Assessment Version 1.3 (1996); Gen. Accounting Office, Confidentiality of Tax Data: IRS' Implementation of the Taxpayer Browsing Protection Act (1999).

64. Former President William Jefferson Clinton, Question and Answer Session at the Institute of Politics Forum for the John F. Kennedy School of Government at Harvard University (Nov. 19, 2001).

information about residents that is in the possession of private firms.[65] "Under present law," Clinton claimed, "the biggest problem we've got is that the government doesn't have the capacity . . . private companies do to track the whereabouts and the activities of people like the two suspects that the CIA did identify when they came into the country on visas."[66] Private companies conducting mass mailings "have a far better capacity to track potential terrorists and other suspects who come into this country," without intruding upon privacy, and using "simple information that has been available for years" about all of us.[67] The private database holders' "capacity far exceeds anything the government has."[68] Clinton added that "we must improve our woefully inadequate computer tracking capacity, [and] integrate the information systems of the intelligence and law enforcement agencies."[69]

While companies that sell lists or conduct mass mailings have obtained the vast preponderance of American citizens' names, addresses, credit card balances, and utilities information, the American government, Clinton notes, does not have nearly as complete information.[70] Clinton argued that accessing this data is necessary to track potential terrorists and to trace the money that keeps terrorist networks active.[71] If "guys like Mohammed Atta [a leader of the 9/11 hijackers] have to stay for a long time, they will use their real names because they may get checked" to get utility bills and credit cards.[72] It is "most urgent" for increasing safety in the short run, Clinton argued, that the government develop the capacity, or contract to use the information and techniques that are now legal for use in the private sector.[73]

---

65. *See* Former President William Jefferson Clinton, Address at the Institute of Politics Forum for the John F. Kennedy School of Government at Harvard University (Nov. 19, 2001).

66. Clinton, *supra* note 64.

67. Clinton, *supra* note 65.

68. *Id.*

69. *Id.*

70. Clinton, *supra* note 64.

71. *Id.*

72. *Id.*

73. *Id. But see* William Matthews, *Commercial database use flagged*, FED. COMPUTER WK., Jan. 16, 2002, *available at* http://www.com/fcw/articles/2002/0114/web-epic-01-16-02.asp (describing a suit by the Electronic Privacy Information Center ("EPIC") under the Privacy Act that would require the Justice and Treasury Departments to disclose their purchase of information about individuals from commercial databanks).

III. INTEGRATING THE DATABANKS

Separately and jointly, the five main databases and other identification schemes set the foundation for a NIDS. Though currently limited in interconnections, there are overlaps among IRCA and IIRIRA information, and the New Hires Databank now extends to student loan compliance. The routine use exemptions applied to the educational acts, possible computer matching among government databanks, and the proposed linking of CAPS with other private and law enforcement databanks implicate the potential for integration into a full national identification system.

Following 9/11, there have been calls for the integration of government databanks and watch-lists at airports to create passenger profiles to identify "safe travelers" and to spot potential terrorists.[74] Such an integration would constitute a conflation of administrative, criminal justice, and national security databanks and procedures.

The monitoring of the NIDS and informing citizens of its constitutional and political implications have gained paramount importance because the parts of the NIDS are coalescing in a largely unrecognized manner.[75] While such a system might begin informally and partly voluntarily, the momentum will shift toward a precisely structured, mandatory system, requiring a card to be in one's possession at all times. Once in place, such a NIDS would be almost impossible to dislodge.

IV. POST-9/11 DEBATE OVER A NATIONAL IDENTIFICATION CARD

The call for a national ID emerged as a response to the 9/11 attacks partly because supporters of a national ID system claim that existing forms of ID are inadequate.[76] This conclusion "has been fueled by an explosion in the number of financial crimes in which fraud artists adopt the identity of their victims" and accelerated by feelings that a national ID would help fight terrorism.[77] A NIDS would include assigning a unique identifier to every American to facilitate the merging of numerous existing databases of information. This unified data-

---

74. Robert O'Harrow, Jr., *Intricate Screening of Fliers in Works: Database Raises Privacy Concerns*, WASH. POST, Feb. 1, 2002, at A1.

75. *See* Twight, *Watching You*, *supra* note 13; *see also* Richard Sobel, *The Degradation of Political Identity under a National Identification System*, 8 B.U. J. SCI. & TECH. L. 37 (2002).

76. *See* Robert O'Harrow, Jr., & Jonathan Krim, *National ID Card Gaining Support*, WASH. POST, Dec. 17, 2001, at A1 (noting that a "centralized ID database system would dramatically speed verification and make life more convenient for travelers, airlines and others").

77. *Id.*

base would permit governmental agencies to assist one another both to avoid national crises and to work together after a crisis has occurred.[78] Because the American government already retains significant information about its residents and citizens in disparate databases,[79] according to proponents, a NIDS would simply be a more effective compilation of existing information. A NIDS would also better ensure that no wrongdoer gets lost in the cracks of bureaucracy or remains anonymous while traveling.[80]

Notwithstanding concerns about government access to compiled information, NIDS proponents argue that sometimes privacy should be sacrificed in favor of necessity or convenience.[81] For example, people choose to obtain toll passes that allow them to move quickly through highway tollbooths. The passes also provide information to the toll authority about a person's movement, but those who obtain the passes may see the trade-off as a fair one without recognizing the long term surveillance consequences.[82] A NIDS poses a similar trade-off in that people may have "a little less anonymity for a lot more security."[83] To most, less privacy for more security seems reasonable.[84] According to a Pew poll immediately after the 9/11 attacks, 70% of Americans favored a national ID card to curb terrorism, though the percentages were lower in prior and subsequent polling.[85]

Acculturation is a common explanation for Americans' seeming lack of concern. Americans are used to producing photo identification for a multitude of activities, such as "flying, driving, drinking and

---

78. *See* Larry Ellison, *Digital IDs Can Help Prevent Terrorism*, WALL ST. J., Oct. 8, 2001, at A26, *available at* http://www.oracle.com/corporate/index.html?digitalid.html.

79. *See id.* ("Federal, state and local agencies issue Social Security cards, driver's licenses, pilot's licenses, passports and visas. They maintain thousands of databases to keep track of everyone from taxpayers and voters to suspected terrorists.").

80. *See* Alan M. Dershowitz, *Why Fear National ID Cards?*, N.Y. TIMES, Oct. 13, 2001, at A23 (arguing that no right to anonymity "is hinted at in the Constitution" and that America cannot afford to recognize such a right in the post-9/11 climate). *But see* George H. Carr, Note, *Application of U.S. Supreme Court Doctrine to Anonymity in the Networld*, 44 CLEV. ST. L. REV. 521 (1996) (discussing several Supreme Court cases that suggest otherwise).

81. *See* Dershowitz, *supra* note 80; *see also* O'Harrow, Jr., & Krim, *supra* note 76 (noting that a centralized ID database would dramatically speed verification and make life more convenient for travelers, airlines, and others).

82. *See* Dershowitz, *supra* note 80.

83. *Id.*

84. *See* Robert O'Harrow, Jr., *States Seek National ID Funds: Motor Vehicle Group Backs High-Tech Driver's Licenses*, WASH. POST, Jan. 14, 2001, at A4.

85. *See* O'Harrow, Jr., & Krim, *supra* note 76; Donna Leinwand, *National ID in Development: But Enthusiasm for the System Appears to be Fading, Poll Says*, USA TODAY, Jan. 22, 2002, at A2. For alternative levels of support, see *infra* note 332 and Robert Ellis Smith, *The Politics of the ID-card Debate*, PRIVACY J., December 2001, at 1.

check-cashing."[86] Military personnel already are given ID cards with embedded computer chips.[87] The AAMVA plan for a national security system would incorporate unique identifiers.[88]

Suggestions about the type of national ID system necessary to solve this problem vary. For instance, Harvard Law School professor Alan Dershowitz proposes a system using fingerprints in which the identification card itself would only contain minimal personal information, such as "name, address, photo and print."[89] The ID card aspect of the system could be optional, but would be meant to expedite security-check processes.[90]

Larry Ellison, CEO of the Oracle Corporation, has proposed a more complex system, in which "a national database combined with biometrics, thumb prints, hand prints, iris scans, or other new technology [would] detect false identities."[91] The database would contain information such as "names, addresses, places of work, amounts and sources of income, assets, purchases, travel destinations, and more[,]" information that already exists in databases maintained by private companies such as American Express and Visa.[92] Ellison argues that this comprehensive system would be one of the best ways to prevent terrorists from operating under assumed names and to generally protect secured locations, such as airports.[93]

Specifically, to gain entry to airports, Ellison's system "would require people to present a photo ID, put their thumb on a fingerprint scanner and tell the guard their Social Security number."[94] The person's records could be brought up from the database once their identity is confirmed. If there were risk factors, the appropriate measures could be taken to ensure safety.[95] While this system may seem complex and potentially cost prohibitive for the government, Ellison's company, Oracle, has "already offered to provide the necessary software for free, and [] other companies would pitch in with hardware and support."[96] "The database [c]ould be maintained and run by the government alone" to avoid the appearance of corporate benefit.[97]

If American citizens remain entitled to value their privacy, they are the ones who have to decide how much of that privacy they might

86. Dershowitz, *supra* note 80.
87. *See* O'Harrow & Krim, *supra* note 76.
88. *See id.*
89. Dershowitz, *supra* note 80.
90. *See id.*
91. Ellison, *supra* note 78.
92. *Id.*
93. *See id.*
94. *Id.*
95. *Id.*
96. Ellison, *supra* note 78.
97. *Id.*

exchange for more security. Dershowitz argues that the amount of privacy that would be relinquished is minimal, given that "[t]he existence of a national card need not change the rules about when ID can properly be demanded."[98] However, consideration must be given to the potentially increased likelihood that ID will be demanded by police.[99] Dershowitz maintains that a system that minimally inconveniences all members of the population may be superior to the current system of racial profiling where certain members of the population experience increased suspicion based solely on race or ethnicity.[100] For instance, if men of Arab descent have proper identification that checks out when compared to the database, they could pass through security at the same rate as other people.

Finally, Robert Scheer maintains that a national ID card may even prove to be a privacy benefit.[101] The Defense Department card "enables users to electronically sign and encrypt online documents."[102] An ID card could even contain the capacity to scramble cell phone calls for users.[103] In terms of protecting against fraud or misuse of cards, a national ID system has the potential to provide protection superior to current options.

The DOT is considering a "trusted-traveler" card for airline passengers, featuring a biometric description of the owner and probably awarded after an FBI background check. The card would aid those who want to travel without waiting in long lines.[104] In addition, the FAA is proposing an "air security screening system" to bring together air passengers' travel history, living arrangements, travel companions, and other personal data.[105]

Prior to 9/11, there were few calls for such a national ID and many voices questioning it. The political forces pressing for and against a NIDS are varied. Proponents include an association of gov-

---

98. Dershowitz, *supra* note 80.

99. *Id.* (claiming, in addition, how the Constitution does not create a right to anonymity).

100. *Id.*

101. Robert Scheer, *Yep, I Support a National ID Card*, YAHOO! INTERNET LIFE, Jan. 2002, at 54.

102. O'Harrow, Jr., & Krim, *supra* note 76.

103. *Id.*

104. *See* Tom Ramstack, *ID card in works for air passengers*, WASH. TIMES, Jan. 31, 2002, at A1. Not everyone advocates the idea. Associate director of the American Civil Liberties Union, Barry Steinhardt, said "[t]his so-called trusted-passenger card will become essentially mandatory for everyone to use not only on airlines but also buses, trains and perhaps drives over bridges and tunnels. The consequences of not having a trusted-passenger card is that you will be immediately suspect."

105. Robert O'Harrow, Jr., *Intricate Screening of Fliers in Works*, WASH. POST, Feb. 1, 2002, at A1 ("Critics say it would be one of the largest monitoring systems ever created by the government and a huge intrusion on privacy."). It would also involve rolling back privacy protections in the Fair Credit Reporting Act and the Drivers Privacy Protection Act. *Id.*

ernment officials as well as business leaders. Even before 2001, the National Governor's Association ("NGA")[106] had asserted the "great[] need for some type of personal identification mechanism "to combat fraud, crime, illegal immigration, and mismanagement of funds."[107] In 1996, the NGA called for the federal government to implement such a system to track citizens from birth to death.

Another private association raised the issue of a national ID without using that specific name. The AAMVA has called for creating a national license by linking driver's license records with the SSA, Immigration and Naturalization Service ("INS"), and law enforcement agencies.[108] These proposals to coordinate state driver's license databanks call for congressional mandates and funding of $100 million. While clearly advantageous for elected and appointed government employees with informational needs, its benefits to private citizens are less clear.[109] Both the NGA and AAMVA are private interest organizations of government officials, not government entities per se.[110]

---

106. The National Governor's Association ("NGA") is a private organization of government officials. *See* National Governor's Association, *Frequently Asked Questions*, *at* http://www.nga.org/nga/1,1169,C_FAQ,00.html (last visited Feb. 26, 2002). *Fortune* named it "one of Washington's most powerful lobbying organizations" due to its ability to lead the debate on issues that impact states from welfare reform to education, while maintaining "our Federalist system of government." *See id. at* http://www.nga.org/nga/1,1169,C_FAQ^D_302,00.html (last visited Feb. 26, 2002). The Frequently Asked Questions section asks, "[w]hy can't the public attend NGA meetings?" and responds:

> NGA's meetings are the business meetings of the organization — not meetings for the general public. The meetings are for NGA's members, which are governors. No outside groups or individuals participate in the meetings, unless they are invited speakers or panelists . . . No attendees, including the media, are allowed to observe 'Governors-only' sessions. Security is a major aspect of NGA meetings. It is important to provide a safe, secure and controlled environment for all meetings of the NGA.

Id. at http://www.nga.org/nga/1,1169,C_FAQ^D_297,00.html (last visited Feb. 26, 2002).

107. *See* David M. Bresnahan, *Governors Push National ID Plan*, WORLD NETDAILY, Nov. 13, 1998; *see also* David M. Bresnahan, *How Governors View States' Rights: Only Some Care About Executive Order 13083, National ID*, WORLD NETDAILY, Nov. 26, 1998. The NGA complained that Executive Order 13083 weakens federalism because it would have allowed federal agencies to set what is permissible for state and local governments to legislate.

108. Jennifer 8. Lee, *A Nation Challenged: Record Keeping; Upgraded Driver's Licenses Are Urged as National ID's*, N.Y. TIMES, Jan. 8, 2002, at A13.

109. Charlotte Twight, *Government Manipulation of Constitutional-Level Transaction Cost*, 56 PUB. CHOICE 131 (1988).

110. The AAMVA is a tax-exempt, nonprofit organization founded during the Depression to develop model programs in motor vehicle administration, police traffic services, and highway safety. It serves as an information clearinghouse for U.S. and Canadian enforcement officials and "encourage[s] uniformity and reciprocity." For its February, 2002 summit on federalizing the driver's license, AAMVA paid travel, hotel, and registration costs for a chief motor vehicle administrator, a law enforcement

In critiquing the AAMVA plan, the Electronic Privacy Information Center ("EPIC") argues that the proposed nationalized driver's license "does not accomplish its stated aims of increased safety and security, but merely shifts the potential for fraud and identity theft to a higher plane, where the intrinsic privacy invasion is greater, and the means of remedying inevitable flaws is more complex and difficult."[111] Centralizing authority over personal identity both increases the risk of ID theft as well as the scope of harm when it occurs. Privacy and security are best protected by "documents serving limited purposes and by relying on multiple and decentralized systems of identification in cases where there is a genuine need to establish identity."[112]

The AAMVA residency and identification proposals actually would increase the number of unlicensed drivers by making it harder for individuals to get licenses. According to EPIC, the AAMVA is not the right body to determine the "balance between identification and privacy" because it is a trade association representing public administrators that are not directly accountable to the public.[113] Its goal of "one card, one person, one record"[114] contradicts American diversity. EPIC maintains, "[t]he combination of technical concerns and prevalent American constitutional values protecting freedom of movement, privacy and anonymity," and "strongly suggests that any national identification scheme must be rejected."[115] "A national ID would create a false sense of security because it would enable individuals with an ID — who may in fact be terrorists — to avoid heightened security measures."[116]

Interestingly, the Bush administration, including the cyber security chief, Richard Clarke, has downplayed the idea of a national ID card.[117] Supreme Court Justice Antonin Scalia indicates that he would probably vote against such an idea if Americans held a referendum on the idea.[118] Conservative *New York Times* columnist William Safire

---

official, a driver's licensing representative, and an information technology representative, but not for public representatives. *See* EPIC Report, *supra* note 40. The Associate Members & Industry Advisory Board includes Experian, Polaroid, R.L. Polk & Co., IBM Corporation, American Express Company, and Hertz. *See* AAMVA, Associate Members & Industry Advisor Board, *at* http://www.aamva.org/links/mnu_lnkAssociateMembers.asp (last visited Feb. 26, 2002).

111. EPIC Report, *supra* note 40, at 2.

112. *Id.* at 4.

113. *Id.* at 5.

114. *Id.* at 6.

115. *Id.* at 16. The Driver's Privacy Protection Act is supposed to limit the sharing of DMV information, but has a number of exemptions. *See id.* at 9–10.

116. *Id.* at 14.

117. *See* O'Harrow, Jr., and Krim, *supra* note 76.

118. *See* Associated Press, *Supreme Court Justice Antonin Scalia is No Fan of National ID Card Proposal* (Nov. 15, 2001), *available at*

has warned that the "fear of terrorism has placed Americans in danger of trading our 'right to be let alone' for the false sense of security of a national identification card."[119] Internet advocacy groups like the Electronic Frontier Foundation ("EFF"), EPIC, and the American Civil Liberties Union ("ACLU"), as well as some conservative and libertarian groups, such as the Cato Institute, oppose a national ID plan. A coalition of forty groups opposes the AAMVA plan for a national identification system.[120]

Some advocates of a NIDS propose a limited document. Yet bureaucratic and technological imperatives and Americans' concern for security suggest that a more, rather than less, complex and intrusive system would be created. The following section provides a possible scenario for such a complete system.

V. THE FEATURES OF A FORMAL NIDS

Independent of the calls following 9/11 for a stand-alone NIDS, such a system has been developing through different databanks that track large numbers of people. The NIDS emerging out of the five major laws and regulations mentioned in the previous sections is likely to expand to fill other purposes. Given the post-9/11 call for a national ID, what might such a system look like beyond the aggregation of the existing databanks and ID schemes?[121]

A formal NIDS would require a national ID number, national databank, and national ID card, though less centralized systems are theoretically possible but unlikely in practice.[122] Administratively, a formal NIDS would include identification of a supposed constitutional provision permitting it, enabling legislation outlining its proposed provisions, and complex administrative regulations to implement it. Congress would need to pass specific enabling legislation since this is fundamentally a national issue, if constitutional.

The computer databanks of a NIDS would be organized by ID numbers and tied administratively, or perhaps electronically, to a physical card. The national ID numbers would be used for multiple purposes, and computer databanks that collect disparate pieces of information would be integrated. An individual would have to be located in the databank in order to have a legal identity and receive bu-

---

http://www.abcnews.go.com/wire/US/ap20011115_597.html (last visited Feb. 26, 2002).

119. William Safire, *Threat of National ID*, N.Y. TIMES, Dec. 24, 2001, at A15; *see also* William Safire, *The Computer Tattoo*, N.Y. TIMES, Sept. 9, 1982, at A27.

120. Brian Krebs, NEWSBYTES, *Nix State-Led National ID Plan, Coalition Urges Bush* (Feb. 12, 2002) *available at* http://www.newsbytes.com/news/02/174423.html.

121. See Bruce Schneier, *National ID Cards*, CRYPTO-GRAM NEWSLETTER (Counterpane Internet Security), Dec. 15, 2001, at 1 for a comparable analysis.

122. *Id.* at 1–2.

reaucratic recognition. To receive an ID card, an individual would have to meet registration requirements such as official proof of birth in the U.S. or legal residency. A proper ID would be required to receive government benefits or to exercise political rights. For instance, a national ID would be required for any official encounters, including with the police, or to vote.

Creating a NIDS would begin with the assignment of a unique national ID number.[123] This number would probably be a variant on the SSN and includes a security feature such as a "check" digit.[124] This data collection about American citizens would begin at birth. It would create for each newborn the prospect of being tracked from cradle to grave by way of a government-issued number. Such a process has already begun with the relatively recent (1990) practice of issuing SSNs at birth, and recording the SSN on the birth certificate.

In order to centralize the information indexed by a national ID number, there would need to be a national databank or a series of interconnected state or regional databanks. A potential basis for this system might be the integration of databanks from each of the five components of the preexisting NIDS. An alternative basis would be Social Security records, IRS data, or census enumerations if confidentiality restrictions were removed. This would involve amending the restrictions on use of governmental records and SSNs in the Privacy Act of 1974[125] and avoiding the Fair Information Practice principles[126] that information collected for one purpose should not be used for another without consent of the person identified. Because the AAMVA proposal involves a national lobbying organization seeking congressional legislation and funding, this is not really a form of federalism as it would be developed directly from state initiatives.[127]

For efficiency, such a computer system would centralize and interconnect with educational, employment, Social Security, tax, pension, medical information, and perhaps criminal records. This data would paint a detailed portrait of each individual's habits and preferences, even though such collections would not be fully accurate or secure.

---

123. Uruguay Round Agreements Act, Pub. L. No. 103-465, § 742, 108 Stat. 4809, 5010 (1994).

124. Twight, *Watching You*, *supra* note 13, at 182.

125. Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. § 552a (1994)).

126. *See* HEW REPORT, *supra* note 45, at 41, on the establishment of a Code of Fair Information Practices. The Code of Fair Information Practices holds that "[t]here must be a way for a person to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent." *Id.* at 41. The HEW Report also recommended against using the SSN as a national identifier for privacy reasons. *Id.* at xxi–xxii, xxxii–xxxv.

127. Lee, *supra* note 108.

A less extensive model for a NIDS lay in the Johnson Administration's 1965 proposal for a National Data Center ("NDC") to centralize and link government data collections.[128] The NDC would have stored 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."[129] The NDC databank would have contained "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."[130] The concept of the NDC "slowly evolved into that of a massive databank containing cradle-to-grave electronic records for every U.S. citizen."[131] The rejected NDC would have encompassed only part of the current informal NIDS.

A more complete national data system than an informal NIDS would include the health or travel records generated by HIPAA or CAPS. Like the proposed NDC, a formal NIDS databank would contain birth certificate, citizenship, school, draft, military service, tax Social Security, death records, and additional types of data.

Once established, procedures would have to be developed for entering, checking, and verifying inclusion in the database. There would need to be specific registration procedures at various points in life, periodic updating, and replacement of lost or stolen cards.

Most likely, people would receive a first national ID when entering school at about six years old, and perhaps an updated version upon taking a first job. Children and adults would have to renew their ID every five to ten years, and at life changes ranging from marriage to change of address. This process is similar to obtaining or renewing green cards for immigrants.[132] While superficially like renewing a driver's license, it would be much more serious and Kafkaesque[133] because of the importance of reestablishing eligibility for a national ID, and the consequences of being denied a card or its renewal. It would also encompass the procedures and bureaucratic requirements of registering for potentially deniable benefits or trying to renew a driver's license when one has a questionable driving record or be-

---

128. *See* SIMPSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY 13 (2000).

129. *Id.*

130. *Id.* at 13–14.

131. *Id.* at 13.

132. *See* Immigration and Naturalization Service, *You Don't Have to be an Immigrant to be Affected by the New Immigration Law* (advertisement), NEWSWEEK, Sept. 28, 1987, at 39.

133. *See* Daniel J. Solove, *Privacy and Power: Computer Databanks and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001).

comes elderly. Expired national IDs would not be valid or usable as identification.

A possible scenario for constituting a formal NIDS over the life cycle might include the following: at birth, every U.S. citizen would be enumerated and issued a national identification number that would be entered onto a paper or electronic birth certificate and into a hospital (or community) system connected to a national databank.[134] Permanent residents and naturalized citizens would be assigned national ID numbers during the process of naturalization or when registering for government benefits. This system would also try to include as many illegal immigrants and temporary visitors as possible.

When a child reached school age, he or she would apply for and, if meeting the criteria, be issued a national ID. Citizens would need to re-register for a NID at the age of sixteen.[135]

Over a lifetime, the national ID number would be used to track mandatory updating of home addresses, parental information, health records, school records, employment, and pension records. The NIDS databank, perhaps located at the HHS or the Commerce Department, could include the information on the citizen's receipt of government services such as health care or welfare benefits, and perhaps driving record. The national ID might also serve as a smart card for governmental and private purposes. It might be integrated with, or updated by, referencing certain private databanks.[136]

The national ID would also likely include more technologically sophisticated features, such as digital photos, to assist facial recognition technology, perhaps tied to airport or neighborhood video surveillance.[137] A biometric would be used to confirm identity electronically. The biometric features most likely would be fingerprint or iris scans, though in theory they could also include DNA representations. The physical card itself might include a barcoded magnetic strip or computer chip to include basic identification information and perhaps medical, eligibility, or criminal records. National IDs would also include anti-counterfeiting measures such as a hologram.[138]

---

134. *See* Annie I. Anton, *National Identification Cards* (Dec. 17, 1996), *available at* http://www.cc.gatech.edu/computing/SW_Eng/people/Phd/id.html.

135. *Id.*

136. *See* Joe Sharkey, *Get Smart? He'd Rather Not*, N.Y. TIMES, Feb. 22, 1998, at 14NJ1 (regarding New Jersey's abandoned plan to turn the driver's license into a smart card).

137. *See* Spencer S. Hsu, *D.C. Police Cameras Raise Privacy Issues; Morella Questions Surveillance Plan*, WASH. POST, Feb. 15, 2002, at B8; *see also* William Safire, *The Great Unwatched; The Cherished American Principle of Personal Freedom will be Sacrificed for Security*, PITT. POST-GAZETTE, Feb. 19, 2002, at A9.

138. Tom Ramstack, *Pay It Safe; 'Smart' Cards to Aid Transport Industry, But At What Cost?*, WASH. TIMES, Feb. 14, 2002, at B3. As with proposed "smart cards" for airport access, this would permit easier location of wanted persons and identification of people entering restricted areas. The inclusion of a transponder microchip tied

Some calls for a national ID suggest its use as voluntary or only for limited purposes such as getting a job, collecting welfare benefits, or air travel.[139] It is unlikely, however, to remain voluntary if indeed it were needed for specific governmental purposes. Voluntary might quickly transform into required to be possessed but not required to be carried at all times. A national ID might be required only when transacting official or quasi-official business. Earlier proponents of a worker ID card, for example, said it would be used at first only for two purposes and later modified to three.[140] Not having in one's possession a national ID when one is asked to produce it, however, might create embarrassment, suspicion, or even serve as cause for incarceration.[141] Alternatively, everyone could be required to carry the national ID at all times outside of one's home.[142] Even with this requirement, not everyone would carry one and not all ID would be valid.[143]

The basis for such centralized data collection would go beyond the five components of an informal NIDS mentioned above in order to integrate the constituent databanks. Controversy over the intrusive nature of similar data collection scuttled the NDC. Whether in the current post-9/11 atmosphere citizens would now accept such centralization, identification, and documentation is open to question because of the ways the expansion of national IDs conflicts with fundamental principles. Whether such a card would have a positive impact or create more problems than it would solve still needs to be addressed.

---

to the Global Positioning System in a mandatorily carried national ID would permit the monitoring of the location of individuals in the United States. While Orwellian and Kafkaesque in its implications, this is within the speed and data storage capacities of computers existing today or under development.

139. *See* Robert Scheer, *Privacy Watch: Yep, I Support a National ID Card*, YAHOO! INTERNET LIFE, Jan. 2002, at 54 (suggesting that a voluntary ID card should be introduced to facilitate secure online transactions).

140. Richard Sobel, *Immigration and Identification: Interview with Alan Simpson*, 29 MIGRATION WORLD 30, 33 (Sum. 2001).

141. *But see* Kolender v. Lawson, 461 U.S. 352 (1983) (holding that a California penal statute requiring individuals to supply "credible and reliable" identification upon the request of police officers was unconstitutionally vague on its face in violation of the due process clause of the Fourteenth Amendment).

142. 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. *See* United States v. O'Brien, 391 U.S. 367 (1968). O'Brien protested the Vietnam War by burning his draft card, in violation of Selective Service registration requirements prohibiting the destruction of draft cards. Thus, this case does not affirm the constitutionality of the regulation requiring males to carry the card per se (only dealing with O'Brien's violation of the statute forbidding the destruction of his card), yet it might be cited as a basis for requiring citizens to carry identification documents in the future.

143. Those most likely to carry out terrorist acts, however, are unlikely to be flagged by a NIDS. Potential terrorists might not be in the system, particularly if they are traveling on foreign passports or with fraudulent documents.

VI. HISTORICAL ABUSES THROUGH IDENTIFICATION SYSTEMS AND DOCUMENTS

Identity systems and documents have a long history of being used for social control and discrimination. Through the Civil War, slaves were required to carry passes in order to travel away from plantations. The pass laws ended formally with the Thirteenth Amendment's abolition of slavery and involuntary servitude in 1865 and with freedmen becoming citizens by virtue of their birth in the United States under the Fourteenth Amendment in 1868. Along with the granting of voting rights under the Fifteenth Amendment in 1870, these amendments were designed to enforce civil rights protections.[144]

Other forms of identification have been used for population control. Fingerprints have been used to track and control increasingly mobile, diverse populations.[145] Fingerprint identification offered a way to individualize ethnic minorities, particularly African and Asian Americans, as "White America" feared that they would all look the same.[146] Furthermore:

> [F]ingerprint identification allowed law enforcement officials to ignore the reality of human variation: that the "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 in the exigencies of policing in the United States.[147]

The development of passports as an identity document has followed a similar course in the United States. Under the Passport Act of 1926,[148] the Secretary of State has wide discretion to grant or withhold passports.[149] The act states that "[n]o passport shall be granted or issued to or verified for any other persons than those owing alle-

144. *See* H.M. HENRY, THE POLICE CONTROL OF THE SLAVE IN SOUTH CAROLINA (1914). *But see* ROBERT M. GOLDMAN, RECONSTRUCTION AND BLACK SUFFRAGE: LOSING THE VOTE IN REESE AND CRUIKSHANK (2001).

145. *See* SIMON A. COLE, SUSPECT IDENTITIES: A HISTORY OF FINGERPRINTING AND CRIMINAL IDENTIFICATION (2001).

146. *Id.* at 163.

147. *Id.* at 164.

148. 22 U.S.C. § 211a (2001).

149. *See id.*

giance, whether citizens or not, to the United States."[150] This discretion has led to discriminatory laws and practices, such as formerly barring members of communist organizations from applying for or renewing their passports, and from using or attempting to use their passports.[151] The Secretary of State used this statute to deny passports to individuals deemed to be Communists, a practice subsequently found unconstitutional by the Supreme Court.[152] The Court has held, however, that the State Department may prevent individuals from traveling to certain countries with which the United States has broken diplomatic ties.[153] The Secretary's discretion in the denying and granting of passports has led to discriminatory restrictions on the rights of individuals to travel. The use of passports as a method of suppressing dissent and controlling citizens' travel should be seen as abridging the due process clause of the Fifth Amendment.[154]

A system of identification cards was also used to isolate and gather Jews in Germany and other Nazi occupied territories prior to and during World War II. All German Jews had to apply for such cards by December 31, 1938.[155] Moreover, the Nazis conducted two separate censuses to identify Jews. The first in Germany in 1933 identified practicing Jews[156] and the second in the Greater Reich, including Germany, Austria, the Sudetendland, and the Saar in 1939, identi-

---

150. 22 U.S.C. § 212 (2001).

151. Subversive Activities Control Act of 1950, 50 U.S.C. § 785 (2001) (repealed 1993).

152. *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 Communist beliefs and associations and their refusal to file affidavits concerning present or past membership in the Communist Party); *see also* Aptheker v. Secretary of State, 378 U.S. 500, 505 (1964) (holding Section 6 of the Subversive Activities Control Act of 1950 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"); Saenz v. Roe, 526 U.S. 489 (1999) (holding that California's residency requirement for receiving welfare benefits violated the right to travel under the Privileges and Immunities Clause).

153. *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").

154. *See* COMM. ON FOREIGN AFFAIRS, SUBCOMM. ON STATE DEP'T 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). *But see* Haig v. Agee, 453 U.S. 280 (1981) (upholding the denial of a passport when travel is a threat to national security).

155. *See* RAUL HILBERG, THE DESTRUCTION OF THE EUROPEAN JEWS 54 (Student ed., Holmes & Meier Publ'g, Inc. 1985) (1961). Even before the censuses, Germany had collected health records that were ultimately used to aid the process of targeting Jews. *See* TWIGHT, DEPENDENT ON D.C., *supra* note 13, at 233.

156. EDWIN BLACK, IBM AND THE HOLOCAUST: THE STRATEGIC ALLIANCE BETWEEN NAZI GERMANY AND AMERICA'S MOST POWERFUL CORPORATION 55–56 (2001).

fied "racial Jews."[157] German Jews were required to carry IDs, and their passports and ration cards were stamped with a red "J."[158] As Edwin Black noted in *IBM and the Holocaust*:

> [W]henever Jewish persecution was reported, the media invariably reported the incessant registrations and censuses as Nazidom's initial step....For example, a March 2 [sic], 1940, *New York Times* article, entitled "Jews in Cracow Move to Ghettos," described how 80,000 Jews had been herded into overcrowded flats in a squalid urban district devoid of resources. "A common sight," the report asserted, "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.[159]

The Holocaust that besieged the Jews began with simple censuses for the purpose of identification. As Black notes, "[o]n October 28, 1939, for the Jewish people of Warsaw, everything stopped. That day they were counted."[160]

Furthermore, the processing of this information by Dehomag, IBM's German subsidiary, helped to combine pseudo-science and official race hatred. "Racial hygiene, race politics, and a constellation of related anti-Semitic disciplines were just talk in the absence of genuine statistics. Now a lightning storm of anti-Jewish legislation and decrees restricting Jews from all phases of academic, professional, governmental, and commercial life would be empowered by the ability to target the Jews by individual name."[161] Germany depended on "IBM technology for its totalitarian vision of the future."[162]

---

157. *Id.* at 169.

158. HILBERG, *supra* note 155, at 119.

159. *See* BLACK, *supra* note 156, at 201 (quoting *Jews in Cracow Move to Ghettos*, N.Y. TIMES, Mar. 16, 1940, at 3); *see also* Richard Sobel, *supra* note 75, at n. 77, for the origins of Black's awareness of IBM technology's role in the Holocaust. *But see* CURT GENTRY, J. EDGAR HOOVER: THE MAN OF SECRETS 244–45 (1991), on how former FBI director, J. Edgar Hoover opposed the relocation of Japanese-Americans when he felt the "most likely spies had already been arrested" by the FBI soon after Pearl Harbor.

160. *Id.* at 190. Chaim Kaplan, a teacher, poet, and journalist in Warsaw, remarked of the effects of a forthcoming census, "[t]oday, 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." *Id.* at 189.

161. *Id.* at 59; *see also* Press Release, IBM, Statement on Nazi-era Book and Lawsuit (Feb. 14, 2001), *at* http://ibm.com/Press/prnews.nsf/jan/ E761868F46444 B06852569F20064F555 ("It has been known for decades that the Nazis used Hollerith equipment and that IBM's German subsidiary during the 1930s — Deutsche Hollerith

The identification system "was a powerful weapon in the hands of the police. . . . [I]t enabled police to pick up any Jew, anywhere, anytime. . . . [I]dentification had a paralyzing effect on its victims. The system induced the Jews to be even more docile . . . ."[163] The identification system was assisted by punch card technology.

> 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.[164]

It was a society where "[n]o one would escape. This was something new for mankind. Never before had so many people been identified so precisely, so silently, so quickly and with such far-reaching consequences. The dawn of the Information Age began at the sunset of human decency."[165] In the aggregate, "[b]y early 1942 . . . Nazi Germany no longer killed just Jewish people. It killed Jewish *populations*. This was the data-driven denouement of Hitler's war against the Jews."[166]

Similarly, when the German Army invaded Denmark, Norway, the Netherlands, Belgium, Luxembourg, and France in 1940, officers examined birth, voting, and business records to identify Jews and members of other "undesirable" groups to be rounded up by the Gestapo and sent to concentration camps.[167] The Dutch Census Bureau expressed gratitude for the German requirement to register all Jews, because it created "an untold administrative simplification and a sav-

---

Maschinen GmbH (Dehomag) — supplied Hollerith equipment. . . . These well-known facts appear to be the primary underpinning for these recent allegations.")

162. Robert Urekew, *Justice Delayed: IBM's Collaboration with Nazi Germany*, 23 HARV. INT'L REV. 84, 84–85 (2002) (reviewing EDWIN BLACK, IBM AND THE HOLOCAUST: THE STRATEGIC ALLIANCE BETWEEN NAZI GERMANY AND AMERICA'S MOST POWERFUL CORPORATION (2001)).

163. HILBERG, *supra* note 155, at 58.

164. *See* BLACK, *supra* note 156, at 107; *see also* COLE, *supra* note 145, at 250 ("In a sense, the use of punch cards to represent individuals brought identification full circle, since the problem of personal identification had stimulated the development of the punch card.").

165. *See* BLACK, *supra* note 156, at 104.

166. *Id.* at 365 (emphasis in original).

167. *See* WAYNE MADSEN, HANDBOOK OF PERSONAL DATA PROTECTION 22–23 (1992).

ing of tens of thousand [of guilders] for the country."[168] The registration and documentation of Dutch Jews developed with limited suspicion of the approaching genocide.

In the 1930s and 1940s, the Union of Soviet Socialist Republic ("U.S.S.R.") began requiring citizens to carry internal passports. The Soviet police, or *militsia,* maintained the passport system. Virtually everyone over the age of sixteen was required to have one. The extensive information on the passports included age, marital status, nationality, employer's name, employment beginning and end dates, and criminal record.[169]

In 1939, Britain established a national identification system for administering commodity rationing.[170] The police regularly demanded this identification for enforcement purposes.[171] Once a national ID was in use, the temptation for police to demand it rose substantially.[172] Partly because of protests over these frequently occurring ID checks, the national ID was discarded after 1952 when rationing ended.[173]

For over thirty years, beginning in 1958 for men and in 1963 for women, the South African government required blacks to carry passes that prohibited their moving freely about the country.[174] The green reference books that all black citizens carried regulated where they could travel in the country.[175] The official purpose of the pass was to prove that a South African black had the right to be present in a specific area.[176] In 1985, to spread the burden of requiring identification to all races, a new law decreed that all South Africans were to carry ID cards.[177] Yet, over a ten-year period, blacks were arrested 637,584 times under the new law, whereas there were no whites arrested under the same law.[178]

A system of identity cards that distinguished Hutus from Tutsis contributed to the killings in Rwanda. In remarks on March 25, 1998 about the genocide there,[179] President Clinton criticized the West for

---

168. JACOB PRESSER, THE DESTRUCTION OF THE DUTCH JEWS 37 (1969).

169. *See* RONALD HINGLEY, THE RUSSIAN SECRET POLICE: MUSCOVITE, IMPERIAL RUSSIAN, AND SOVIET POLITICAL SECURITY OPERATIONS (1971); *see also* AMY W. KNIGHT, THE KGB, POLICE AND POLITICS IN THE SOVIET UNION (1990).

170. *See* Anton, *supra* note 134.

171. *Id.*

172. *Id.*

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

174. ROGER OMOND, THE APARTHEID HANDBOOK: A GUIDE TO SOUTH AFRICA'S EVERYDAY RACIAL POLICIES 122 (1986).

175. *Id.*

176. *Id.* The first "pass laws" in South Africa, enacted in 1760, mandated that all slaves "in the cape" carry passes.

177. *Id.* at 123.

178. *Id.*

179. At the same time that these atrocities were occurring, partially because of the Hutus' ability to identify the Tutsis, the United States was implementing IIRIRA

moving too slowly in responding to the massacres whose scope and procedures echoed the earlier Holocaust. "And when they were found, the old and the sick, women and children alike, they were killed — killed because their identity card said they were Tutsi. . . ."[180] The limited likelihood of such abuses with identification documents in the United States does not remove the possibility of bureaucratic and discriminatory misuses of identity badges and numbers.

In fact, enumeration without observance of strict privacy protection has also led to dangers here. The U.S. Census, conducted every ten years under constitutional mandate, is currently the only complete enumeration of the population.[181] While less sensitive than medical data, census information is to be kept secret by law for seventy-two years,[182] with felony penalties for violations.[183] Even more than educational information, census information may only be used for its statistical purposes and may not be published in any way in which individuals could be identified.[184] This protection rests partly on recognizing that the social system as a whole may benefit from the Census, but individuals may be at risk by providing such information.[185]

Yet even before the Japanese attack on Pearl Harbor, President Franklin Delano Roosevelt ignored these protections and ordered the Census Bureau to collect information on "American-born and foreign-born Japanese" from the Census data lists.[186] Information from the

---

(1996) and the FAA was requiring CAPS (1995). *See* IIRIRA, *supra* note 10; Federal Aviation Reauthorization Act of 1996, Pub. L. No. 104-264, § 307, 110 Stat. 3213 (1996).

180. President William J. Clinton, Address to Genocide Survivors, Assistance Workers, and U.S. and Rwandan Government Officials at Kigali Airport, Rwanda (Mar. 25, 1998), *at* http://usinfo.state.gov/regional/af/prestrip/w980325a.htm.

181. U.S. CONST. art. I, § 2, cl. 3.

182. 44 U.S.C. § 2108(b) (1994). Interestingly, it makes no mention of a seventy-two-year period, but rather states:

> [w]ith 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 . . . .

Id.; *see also* 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).").

183. 13 U.S.C. § 214 (1994).

184. 13 U.S.C. § 9 (1994).

185. *See* JOHN TOLAND, INFAMY: PEARL HARBOR AND ITS AFTERMATH 269 (1992).

186. *Id.* at 269–70; s*ee also* William Seltzer and Margo Anderson, After Pearl Harbor: The Proper Role of Population Data Systems in Time of War (2000) (unpub-

1930 and 1940 censuses on all Japanese-Americans was quickly gathered and distributed to the FBI, the governors, and the top military officials in western states.[187] Its use led to the internment of almost 110,000 Japanese-Americans on the West Coast, two-thirds of whom were U.S. citizens.[188]

A Japanese-American affected by the internment, Toyosaburo Korematsu, sued claiming violation of due process and deprivation of liberty and property. The Supreme Court found for the government because the internments were constitutional under the war powers of Congress and the Executive, and were justified by military necessity.[189] As Justice Francis Murphy's dissenting opinion illuminated, the internment of Japanese based on their ethnicity goes beyond military necessity and "falls into the ugly abyss of racism."[190]

The gathering of information based on race and ancestry shows how easily even the most tightly drawn statutory and constitutional rights can be violated during periods of crisis and fear. Racial profiling, particularly tied to computerized identification systems and documents, raises these issues anew. With a computerized national identification system, the efforts to identify and locate "dangerous" citizens can be made much easier.

VII. PRAGMATIC CRITIQUE OF A NIDS: PROBLEMS WITH ID AND DATABANK REQUIREMENTS

There are numerous practical problems with a NIDS. This section critiques each of the components and the system overall. The next sections explore fundamental problems with the nature of a national ID or a NIDS.

The expansions of less pervasive systems like Social Security numbering and the New Hires Databank suggest the problems that a NIDS would produce in the United States. In the 1930s, President Roosevelt and members of Congress promised that the Social Security card would be kept confidential and would not be used for identifica-

---

lished manuscript, on file with authors at Fordham University and University of Wisconsin-Milwaukee, respectively).

187. *See* TOLAND, *supra* note 185, at 285.

188. *See* BLACK, *supra* note 156, at 346.

189. *See* Korematsu v. United States, 323 U.S. 214 (1944); *see also* Hirabayashi v. United States, 320 U.S. 81 (1943). *But see* ex parte Mitsuye Endo 323 U.S. 283 (1944), where a loyal citizen, not charged with any offense, was entitled to be released from confinement under a writ of habeas corpus. William Rehnquist called *Endo* "a minor victory for civil liberties." *See* WILLIAM H. REHNQUIST, ALL THE LAWS BUT ONE: CIVIL LIBERTIES IN WARTIME 221 (1998).

190. *Korematsu*, 323 U.S. at 233.

tion purposes.[191] The SSNs were supposed to be used only to administer the Social Security system. The Social Security card previously said "not for identification."[192] Yet required uses of the SSN for identification and government programs have proliferated. At the same time that Germany and Russia were setting up population registration systems during the prewar Depression, the Social Security Administration in the United States was establishing a pension registration system that raised troubling questions.[193]

Since the implementation of the Social Security account number in 1936, its use as an identification number has been congressionally mandated more than forty times.[194] In 1943, President Roosevelt authorized federal agencies to use SSNs "exclusively" for new permanent account numbers.[195] In 1961, the Civil Service Commission ordered the SSN to become the identifier for all federal employees. A major expansion occurred in 1962, when the IRS began using the SSN, as opposed to a separate tax ID, as an individual tax ID number. In 1965, Medicare began using SSNs as patient identifiers and in 1967 the Defense Department began using them for military personnel.[196]

After Watergate, Congress passed the Privacy Act of 1974 to restrict the collection and disclosure of private information by the government.[197] In particular, it restricted use of the SSN as a personal identifier. This followed a Department of Health, Education, and Welfare report ("HEW Report") that established the Fair Information Principles, including the provision that data about an individual gathered for one purpose should not be otherwise used without the consent of that individual.[198] The report also rejected as a serious threat to privacy and liberty the idea of the SSN as a national ID.[199] In fact, the Privacy Act prohibited government agencies from denying benefits for refusing to provide a SSN.[200]

---

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

192. Robert Pear, *Not for Identification Purposes (Just Kidding)*, N.Y. TIMES, July 26, 1998, at WK3.

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

194. Pub. L. No. 74-271, 74 Stat. 620 (1936); 145 CONG. REC. E 3 (daily ed. Jan. 6, 1999) (statement of Rep. Paul).

195. *See generally* Sandy Cerato, *Chronology of Social Security Number Policy Changes*, The Official Website of the Social Security Administration, History Page, Social Security Online, *at* http://www.ssa.gov/history/ssnchron.html (last modified Mar. 1, 2000) (providing a thorough chronological overview of amendments to the Social Security Act).

196. *See id.*

197. Privacy Act of 1974, Pub. L. No. 93-579, § 7, 88 Stat. 1896, 1909 (1974).

198. HEW REPORT, *supra* note 45.

199. *Id.*

200. Privacy Act of 1974, *supra* note 197.

However, subsequent federal legislation has frequently amended the Social Security Act and permitted additional uses of the SSN.[201] In particular, the Tax Reform Act of 1976 permitted the use of SSNs for tax, public assistance, driver's license, and motor vehicle registration purposes.[202] Grandfathering for existing uses and a routine use exception also limited the protections of the Privacy Act.[203]

Use of SSNs became widespread as the result of two patterns: the development of federal requirements for an SSN beyond the SSN's initial purpose and the extensive use of the SSN in the public sector. SSNs are required by law for draft registration,[204] Medicare,[205] Medicaid,[206] Aid to Families with Dependent Children,[207] Food Stamps,[208] interest-bearing bank accounts,[209] Housing and Community Development grants,[210] and state commercial driver's licensing programs.[211]

Prior to 1973, individuals did not usually obtain SSNs until they were roughly sixteen to eighteen years old and ready to work. The Social Security Amendments of 1972 authorized the SSA to enumerate children at the time that they first entered school at about age five.[212] Over the next decade, tax laws and revenue enhancements reduced the age at which Social Security numbering became required to birth. The Tax Reform Act of 1986 required individuals filing a tax return after December 31, 1987 to include the taxpayer identification number, typically the SSN, for tax dependents age five and older.[213] The Family Support Act of 1988 required individuals filing a tax re-

---

201. *See* Cerato, *supra* note 195.

202. Tax Reform Act of 1976, Pub. L. No. 94-455, 90 Stat. 1520 (1976).

203. Privacy Act of 1974, *supra* note 197, at 1896-97, 1909.

204. *See* Department of Defense Authorization Act, 1982, Pub. L. No. 97-86, § 916, 95 Stat. 1099, 1129 (1981).

205. *See* 42 U.S.C. § 1320a-3 (2001).

206. *See* 42 U.S.C. § 1320b-7 (2001).

207. *See* Social Security Amendments of 1974, Pub. L. No. 93-647, § 101, 88 Stat. 2337, 2359 (1975).

208. *See* Food Stamp Act of 1977, Amendments, Pub. L. No. 96-58, § 4, 98 Stat. 389, 391 (1979).

209. *See* Interest and Dividend Tax Compliance Act of 1983, Pub. L. No. 98-67, § 105, 97 Stat. 369, 380 (1983) (imposing penalties for withholding Taxpayer Identification Number, which is usually the SSN).

210. *See* Housing and Community Development Act of 1987, Pub. L. No. 100-242, § 165, 101 Stat. 1815, 1864 (1988).

211. *See* Commercial Motor Vehicle Safety Act of 1986, Pub. L. No. 99-570, § 12006, 100 Stat. 3207, 3207-175 (1986); U.S. GEN. ACCOUNTING. OFFICE, REPORT TO THE CONGRESS, GAO/HEHS-99-28, GOVERNMENT AND COMMERCIAL USE OF THE SOCIAL SECURITY NUMBER IS WIDESPREAD (1990), *available at* http://www.gao.gov/archive/1999/he99028.pdf. SSNs are required on marriage, driver's, and professional licenses. *Id.* at 8.

212. Social Security Amendments of 1972, Pub. L. No. 92-603, § 137, 86 Stat. 1329, 1364 (1972).

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

turn due after December 31, 1989 to include the taxpayer identification number for each dependent claimed age two or older.[214] 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 age one or older.[215] Finally, in 1994 the General Agreement on Tariffs and Trade, a stipulation in the 1994 Uruguay Round Agreements Act, required taxpayer identification numbers at birth, effective on 1996 returns.[216] This provision was to make up for lost revenues from lower tariffs by requiring a SSN to verify claims of dependents on tax returns. Consequently, government tracking now typically begins when a child receives a SSN at birth.[217]

The routine use exemption to the Privacy Act also seriously weakened the law's protections of personal data. The exemption was included in the House bill to permit routine transfers of information, compatible with the purposes of the original collection by federal agencies.[218] Although the Senate version would have protected individual privacy more rigorously, integral elements of the Senate bill were eliminated in the final compromise of the Privacy Act. For example, the final version omitted the establishment of a Privacy Protection Commission with investigatory and enforcement powers.[219] The legislative compromise to create the Privacy Act "revealed a preference for the government's right to gather and to use personal information over the individual's right to privacy."[220] The Privacy Act included several loopholes for federal agencies to avoid the provisions

---

214. Family Support Act of 1988, Pub. L. No. 100-485, § 704(a), 102 Stat. 2343, 2427–28 (1988).

215. Omnibus Budget Reconciliation Act of 1990, Pub. L. No. 101-508, § 11112, 104 Stat. 1388, 1388–411 (1990).

216. Uruguay Round Agreements Act, Pub. L. No. 103-465, § 742, 108 Stat. 4809, 5010 (1994).

217. Since 1990, the SSA's "Enumeration at Birth Program" has provided SSNs to about 75% of newborns. *See* SOCIAL SECURITY ADMINISTRATION, A-08-00-10047, AUDIT OF ENUMERATION AT BIRTH PROGRAM (2001), *available at* http://www.ssa.gov/oig/adobepdf/A-08-00-10047.pdf; *see also* Flavio L. Komuves, *We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers*, 16 J. MARSHALL J. COMPUTER & INFO. L. 529, 541 (1998).

218. *See* 120 CONG. REC. 36,967 (1974) (statement of Rep. Moorhead) (stating that routine use exemption recognized the impracticality of listing all appropriate uses).

219. The legislative history of the act indicates that the Senate bill, S. 3418, proposed to prohibit the denial of services by private businesses for refusal to provide a SSN. *See* S. REP. NO. 93-1183, at 6943 (1974).

220. Todd Robert Coles, Comment, *Does the Privacy Act of 1974 Protect Your Right to Privacy? An Examination of the Routine Use Exemption*, 40 AM. U. L. REV. 957, 975 (1991).

and increased legislative, judicial, and executive branch supervision are needed to ensure adequate enforcement of the Privacy Act.[221]

Potential privacy protecting provisions of the Privacy Act pertained to the routine use exemption and computer matching. The routine use exemption requires notice of the nature and scope of every routine use by federal agencies to be published in the Federal Register.[222] The requirement to provide notice of routine uses was intended to distinguish between those uses that were "routine transfers of information" in conformance with the Privacy Act and those that were intended to circumvent the act.[223] Without strict congressional or judicial oversight, federal agencies have used the routine use notice requirement to escape the Privacy Act requirements by using broad terms in their routine use notices.[224] Although the act identifies the Office of Management and Budget as the office with the responsibility for formulating guidelines and oversight of federal agencies under the act, this office has failed to adequately supervise federal agency invocations of the routine use exemption.[225]

The most significant amendment to the Privacy Act pertained to computer matching. Computer matching was the most prominent example of misuse of the routine use exemption. It conflicted with the act's purpose of keeping government-held data confidential.[226] In response, the Computer Matching and Privacy Protection Act of 1988 excluded computer matching from the definition of a routine use.[227]

The unintended consequences of IRCA have similarly affected basic rights. Even with its ID requirement, IRCA has become ineffective and discriminatory. Though ID checks for IRCA were meant to end "illegal immigration," its brief and minimal effect on the rate of illegal arrivals has essentially disappeared.[228] In 1989, there were perhaps two to three million illegal immigrants in the United States.[229] By 1996, there may have been twice as many.[230] While the INS indi-

---

221. *See id.* at 986–89 (describing how Congress cannot effectively supervise the routine use exemption under the Privacy Act through agency reports).

222. *See id.* at 975–76.

223. *See id.*

224. *See id.* at 980.

225. *See id.* at 983–86.

226. *See id.* at 981.

227. *See id.* at 982.

228. *See* U.S. GEN. ACCOUNTING. OFFICE, REPORT TO THE CONGRESS, GAO/GGD-90-62, IMMIGRATION REFORM: EMPLOYER SANCTIONS AND THE QUESTION OF DISCRIMINATION 138 (1990), *available at* http://archive.gao.gov/d24t8/140974.pdf.

229. *See* ELIZABETH S. ROLPH, IMMIGRATION POLICIES: LEGACY FROM THE 1980S AND ISSUES FOR THE 1990S 39–40 (1992).

230. *See* IMMIGRATION AND NATURALIZATION SERVICE, ILLEGAL ALIEN RESIDENT POPULATION (ESTIMATES OF THE UNDOCUMENTED IMMIGRANT POPULATION IN THE UNITED STATES: OCTOBER, 1996) (last updated Dec. 2001),

cates that illegal immigration has risen significantly since IRCA was passed,[231] this still means that 275 million Americans who are not illegal immigrants are subject to IRCA and INS jurisdiction. A full-page INS advertisement in 1986 to introduce the country to IRCA showed an Uncle Sam proclaiming without irony that "[y]ou don't have to be an immigrant to be affected by the New Immigration Law."[232]

A 1990 General Accounting Office ("GAO") report to Congress discovered that instead of ending illegal immigration, IRCA had created "widespread discrimination" against Hispanics and Asians.[233] The report found that 19% of employers would not hire people because of their citizenship status, ethnicity, or accent.[234] IRCA thus encourages discrimination against foreign-looking applicants, particularly Hispanic and Asian American citizens, because of the employers' desire to avoid legal problems associated with the hiring of illegal immigrants. In sum, the law itself causes both de facto and de jure discrimination. The GAO finding of widespread discrimination was intended to trigger an expedited repeal that never occurred.[235]

Though it has done little to reduce the influx of so-called illegal aliens, the law has forced citizens to provide ID to work and has established a pilot databank and procedures for requiring government permission to work. However, as Senator Spencer Abraham (R-MI) noted in original opposition to IRCA,[236] some American citizens may not have proper ID and many official cards and entries in the databank may be inaccurate because of bureaucratic errors. Consequently, the right to employment is no longer inherent in personhood or citizenship, but is granted by the government for properly credentialed labor force members. Some employers claim that it violates their religious freedom to treat "strangers" as neighbors.[237]

---

available at http://www.ins.usdoj.gov/graphics/aboutins/statistics/illegalalien/index.htm.

231. *See id.*

232. Advertisement, Immigration and Naturalization Serv., NEWSWEEK, Sept. 28, 1987, at 39.

233. *See* U.S. GEN. ACCOUNTING. OFFICE, *supra* note 228, at 38.

234. *See id.* at 7.

235. U.S. GEN. ACCOUNTING. OFFICE, *supra* note 228; *see also* Sobel, *supra* note 140, at 34.

236. 142 CONG. REC. S3328-04 (1996) (statement of Sen. Abraham).

237. *See* Am. Friends Serv. Comm. Corp. v. Thornburgh, 961 F.2d 1405, 1406 (9th Cir. 1991) (holding that IRCA did not violate the free exercise clause of the First Amendment). The Ninth Circuit heard at least three other unsuccessful challenges to the employment verification of the IRCA. *See* Mester Mfg. Co. v. INS, 879 F.2d 561, 569–71 (9th Cir. 1989) (rejecting employer's arguments that provisions of the IRCA violated procedural due process and substantive due process and also rejecting employer's prima facie challenge of the constitutionality of IRCA); Big Bear Super Market No. 3 v. INS, 913 F.2d 754, 757–58 (9th Cir. 1990) (holding that the pertinent provisions of IRCA describing employer's record-keeping requirements were not

IRCA does not work as proposed partly because some employers do not check for identification because they find it inconvenient to do so, prefer to hire illegal aliens, or find the law repugnant. Furthermore, it fails because many targeted illegal immigrants can obtain false IDs.[238] No matter how stringent the requirements to check IDs become, some employers prefer to risk fines in order to pay a captive workforce less than they pay others, often far below minimum wage. Employers can make large profits because illegal aliens are easily exploited partly because they don't have valid IDs, and IRCA reduces other job possibilities. The risk of fines becomes the cost of doing business. In short, a system of IDs may make it easier for employers who want to hire and exploit illegal immigrants to do so.

Moreover, IRCA does not work because perhaps half of illegal immigrants arrive legally and overstay their visas.[239] In addition, many people come for reasons unrelated to work, such as reuniting with family members. The law threatens anyone in the United States who hires others to provide goods or services, such as babysitting, landscaping, or tax accounting. Burdening employers with verifying identity documents essentially deputizes employers as agents of the INS and creates the need to become familiar with different ID documents.

The National Directory of New Hires under the Welfare Reform Act represents a significant expansion of NIDS. Though it is supposed to prevent child nonsupport by monitoring the work, income, and addresses only of parents who owe child support, it in fact keeps track of all newly hired employees, estimated at sixty million annually.[240] Yet states already keep registries of those 2.3 million people owing unpaid child support.[241] These state-run directories could be checked and cross-referenced without keeping records on roughly fifty-eight mil-

---

ambiguous as a greater degree of ambiguity was tolerated in statutes which imposed civil rather than criminal penalties); Intercommunity Ctr. for Justice & Peace v. INS, 910 F.2d 42, 44 (9th Cir. 1991) (holding that IRCA did not violate the free exercise clause of the First Amendment).

238. *See* Ed Koch, *Fake IDs can be tough to identify*, LAS VEGAS SUN (Feb. 3, 2001), *available at* http://www.lasvegassun.com/sunbin/stories/archives/2001/feb/03/511386804.html.

239. *See* Alexandra Marks, *A Harder Look at Visa Overstayers*, CHRISTIAN SCI. MONITOR, Feb. 5, 2002, at 1; *see also* Siobhan Gorman, *Shortchanging Prevention?*, 34 NAT'L J. 391 (2002); Siobhan Gorman, *Tracking the Foreigners Among Us*, 33 NAT'L J. 3362 (2001).

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

241. *See* U.S. BUREAU OF THE CENSUS, APRIL CURRENT POPULATION SURVEY: CHILD SUPPORT FOR CUSTODIAL MOTHERS AND FATHERS (2002), *available at* http://www.census.gov/prod/2000pubs/p60-212.pdf (last visited Feb. 26, 2002).

lion others who do not owe support.[242] This databank endangers the privacy of the entire working population because of the misdeeds of a small group. Other legislation is likely to increase access to this databank by additional agencies that want to know the location of employees, just as laws and regulations have increased access to SSA verification of SSNs.[243]

In 1999, access to the New Hires Databank expanded to cross-check information about people who received government student loans.[244] Since students must provide their SSN to be eligible for student loans, access to the New Hires Databank enables the government to collect on defaulted student loans by acquiring the address or employer from the New Hires Databank of anyone who has defaulted on a student loan.[245] The House Report on the legislation authorizing this noted that providing the Secretary of Education with access to the New Hires Databank is an "exceptionally constructive use of the New Hire information."[246] In addressing privacy concerns, the Committee Report reasoned that because the Secretary of Education only receives names of individuals who are "fraudulently in debt to the Federal government . . . privacy concerns will not be compromised," because "[i]nformation on all individuals who have not committed fraud will not leave the HHS data base."[247] As of September, the Education Department had collected about $130 million through "matching data" with the New Hires Databank.[248] By comparing more than two million records with the New Hires Databank, the Education Department found one million student loan defaulters (and intends to increase its

242. *See* DEP'T OF HEALTH AND HUMAN SERVICES, DHHS FACT SHEET — CHILD SUPPORT ENFORCEMENT: A CLINTON ADMINISTRATION PRIORITY (Nov. 14, 1996), *available at* http://www.acf.dhhs.gov/programs/cse/fct/csf1.htm (last visited Feb. 26, 2002). The Child Support Enforcement ("CSE") program, established in 1975 under Title IV-D of the Social Security Act, involves fifty-four separate state systems, each with their own laws and procedures. In addition, HHS operates the Federal Parent Locator System, a computer matching system that locates non-custodial parents who owe child support. *Id.*

243. *See* Pear, *supra* note 22, at A1.

244. *See* Consolidated Appropriations Act of 2000, Pub. L. No. 106-113, § 303, 113 Stat. 1501, 1501A304-06 (1999) (amending § 453(j) of the Social Security Act and permitting information to be used only for collection purposes). The Secretary of Education can disclose information about student loan-holders to an agency holding a loan, an agent of the Secretary of Education, and the Attorney General. *Id.*

245. *See* Higher Education Amendments of 1986, Pub. L. No. 99-498, § 484, 100 Stat. 1268, 1480 (codified at 20 U.S.C. § 1091 (2001)).

246. COMM. OF WAYS & MEANS, FATHERS COUNT ACT OF 1999, H.R. REP. NO. 106-424, pt. 1, at 45 (1999) (noting that the New Hires Databank information can be used "to locate individuals who are committing fraud against the United States government by refusing to pay various debts owed to U.S. taxpayers.").

247. *Id.* at 46.

248. *See* Greg Langlois, *Education Touts Loan Default Tool*, FED. COMPUTER WK. (Sept. 24, 2001), *available at* http://www.fcw.com/fcw/articles/2001/0924/news-edu-09-24-01.asp.

efforts).[249] However, providing access to individual SSNs and personal data through the New Hires Databank was not the purpose for which the Welfare Reform was passed.[250]

Several proposed bills would allow access to the New Hires Databank to state unemployment agencies.[251] Representative Ron Paul (R-TX) noted that expanding the use of the New Hires Database to prevent fraud in state unemployment compensation "brings us closer to the day when the database is a universal tracking system allowing government officials easy access to every individual's employment and credit history."[252]

HIPAA's "administrative simplification" requirement to create a UHID and "national electronic data collection and data system for personal health care data" would also expand a NIDS. Yet the UHIDs would reduce medical 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 medical records are currently scattered among several doctors and insurance companies, centralizing this information under the HHS's 2000 rules on electronic medical records will make it much easier for others to delve into private health records.[253] An online universal health information system would create the likelihood that people's most carefully guarded medical secrets would be available to those with access to or the ability to hack into the system. This would make it almost impossible to maintain confi-

---

249. *See id.*

250. *See* Personal Responsibility and Work Opportunity Reconciliation Act of 1996, Pub. L. No. 104-193, § 316, 110 Stat. 2105, 2214–18 (1996) (creating in the Federal Parent Locator Service an automated directory that included name, SSN, and birth date, and requiring federal employers to submit a quarterly report of each employee and wages paid during the previous quarter).

251. *See* Child Support Distribution Act of 2000, H.R. 4678, 106th Cong. § 603; *see also* CONSERVATIVE ACTION TEAM, POLICY BRIEF: H.R. 4678 — CHILD SUPPORT ENFORCEMENT ACT OF 2000, at 2 (2000), *at* http://www.house.gov/burton/RSC/DadsPB.PDF (last visited Feb. 25, 2002) (noting that some House members may not want to give state agencies access to the New Hires Databank because "expanding use of the Federal Database might lead to privacy violations and abuse of the system"). The Fathers Count Act of 1999, H.R. 3073, § 606 also proposed access to the New Hires Database by the State Employment Security agencies to "save millions of dollars each year in Unemployment Insurance overpayments that are avoided and recovered." COMM. OF WAYS & MEANS, *supra* note 246, pt. 1, at 50.

252. The Honorable Ron Paul, Statement on the Child Support Distribution Act of 2000 (Sept. 7, 2000), *available at* http://www.house.gov/paul/congrec/congrec2000/cr090700child.htm (last visited Feb. 25, 2002) (stating opposition to H.R. 4678 on constitutional and privacy grounds). Ironically, a recent and controversial counterexample of maintaining a firewall in data use is the Justice Department's rejection of the FBI's request to access the records of 9/11 hijackers for purchases of firearms because it violated the terms of the instant gun check legislation. *See* Neil A. Lewis, *A Nation Challenged: The Senate Hearing*, N.Y. TIMES, Dec. 7, 2001, at A1.

253. *See* Sobel, *supra* note 23.

dential health care. Information shared with a physician in confidence could ultimately be used against the individual by law enforcement or national security agencies that would have access to private health information.[254]

A UHID or a national ID number used to obtain medical care and perhaps other federal services would make it easier for the federal government to keep track of people without safeguards.[255] Such enumeration for administrative simplification is surrounded by danger because there are inadequate protections to keep it private. The HHS comprehensive medical records regulations permit law enforcement and national security disclosure that compromises confidentiality.[256] As currently structured, the lapses in the HHS plan for law enforcement, especially in combination with the UHID, could lead to the phenomenon known as "docs to cops," where patients' information could contribute to criminal investigations.[257]

There are several types of privacy abuses that could arise under this system. Centralizing medical records would allow people to be identified in reverse. By searching based on diseases rather than names, it would be possible to create lists of people with specific medical conditions. In addition, though the regulations prohibit it, employers with access to health identifiers and database information might inappropriately deny jobs based on the possible financial cost of a pre-existing medical condition on the company's health insurance plan. Employers might make promotion decisions based on medical conditions rather than performance.[258] Furthermore, genetic information included as part of a NIDS could be used for discriminatory purposes.[259]

Unlike the SSN, which is attached to a system of public benefits, a UHID would not directly benefit its assignees. Instead, commercial

---

254. *See* 45 C.F.R. § 164.512 (2002).

255. *See* Warren E. Leary, *Panel Cites Lack of Security on Medical Records*, N.Y. TIMES, Mar. 6, 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 records, and limiting access on a need-to-know basis because of the potential for abuse and misuse.

256. *See supra* note 254; Robert Pear, *Bush Acts to Drop Core Privacy Rule on Medical Data*, N.Y. TIMES, March 22, 2002, at A1.

257. *See* Sobel, *supra* note 23.

258. The HHS regulations prohibit the use of health information by employers for job related decisions. *See* Richard Sobel & Harold J. Bursztajn, *Ban Genetic Discrimination*, BOSTON GLOBE, Aug. 7, 2000, at A15. The U.S. military already takes DNA samples of its troops and the FBI and police have a national felons databank. In addition, New York City officials have proposed taking DNA samples of all arrestees for minor crimes, including fare-beating. *See* C.J. Chivers, *Pataki Presses More DNA Use Against Crime*, N.Y. TIMES, Feb. 24, 2000, at B1.

259. *See* Tiffany Danitz, *Deceit, Denial and the Fate of Privacy*, INSIGHT ON THE NEWS, Aug. 24, 1998, at 14–18.

concerns such as information technology vendors would profit from setting up and managing the information systems themselves, as well as health care insurers.[260] Concerns about the UHID plan were so prevalent that the Clinton administration delayed implementing the plan until Congress or HHS could develop privacy safeguards.[261] However, now that the HHS medical records regulations have been approved in 2001, the idea of a UHID is likely to reappear.

The FAA requirement for photo IDs and the CAPS profiling system have had limited effect on making air travel safer, though CAPS had identified nine of the nineteen 9/11 hijackers, including those who paid cash for one-way tickets.[262] Anyone clever enough to create a destructive device has the capacity to create or obtain false IDs under an assumed name, or to not travel on a compromised plane. Requiring photo IDs to travel and creating databanks for profiling passengers' personal travel habits invades the privacy of millions of ordinary passengers and threatens their right to travel without materially affecting the safety of the flying public. It diminishes the right to travel since it creates restrictions on passengers by permitting air travel only for those with government IDs, and perhaps those having passed a federal background check under the "trusted travelers system." X-raying checked baggage, matching baggage to passengers, and expanding explosive detection technology are more effective strategies for increasing air safety that do not pose such privacy concerns.[263]

The DOT's mandate to federalize the driver's license changes the purpose of the driver's license from a document that demonstrates ability to drive to that of a de facto national ID card and license to travel.[264] The move toward a federalized driver's license to meet the

---

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

261. *See* Robert Ellis Smith, *Health Identifier Stalled*, PRIVACY J., Oct. 1997, at 3; *see also* 142 CONG. REC. H9776–9801 (daily ed. Aug. 1, 1996) (statement of Rep. Stark) (expressing concerns about allowing insurance companies, who were major backers of the proposed bill, to have access to the private medical information that would be stored in the databases created by the bill) ("It could have been a great bill," Stark noted, "if it had truly addressed medical privacy issues.... And it holds terrible dangers for privacies of our citizens and their medical records being available to insurance companies across the country.").

262. *See, e.g.*, David Stout, *9 Hijackers Drew Scrutiny on Sept. 11, Officials Say*, N.Y. TIMES, March 3, 2002, at 20.

263. The Inspector General of the DOT, Kenneth Mead, estimated that passengers would check approximately one billion baggage per year and that the costs of implementing and integrating new equipment and of personnel could reach almost $7 billion. *See FY2003 Transportation Budget Before the House Subcomm. on Aviation of the House Comm. on Transp. and Infrastructure*, 108th Cong. (2002) (statement of Hon. Kenneth M. Mead, Inspector General, DOT). The administration needs to develop a statistical sampling regime that will catch with 1% a representative group of bags at a fraction of the cost to implement more cost-effective screening.

264. *See* EPIC Report, *supra* note 40, at 6. *See generally* SMITH, *supra* note 5.

requirements of IIRIRA undermines individual rights. Citizens in states that do not put SSNs on their driver's licenses may find it difficult to get a job, board a plane, vote, cash a check, obtain a student loan, purchase firearms, open a bank account, purchase insurance, or receive Medicare, Medicaid, or other federal benefits. Furthermore, the aggregation of personal information in one place would encourage and facilitate identity theft. Fortunately, the DOT and IIRIRA SSN requirements were suspended in 1999 due to complaints about their impact on privacy.[265]

Moreover, a NIDS would also be very expensive to establish, maintain, update, and extend. The costs of such a system would not be technical per se, or limited to problems such as the integration of driver's license registration systems. Even if the physical card were inexpensive, the administrative system and its creation would be enormously expensive. With costs of only $100 to $200 per person for setting up the technical system and devoting staff time for evaluating and processing each applicant, it could easily require $25 to $50 billion to establish, and billions of dollars more each year to administer. It would cost between $3 and $6 billion a year to operate, which amounts to $30 to $60 billion per decade.[266] A NIDS would never be cost effective.

Error rates similar to other government databanks could deny many Americans access to the workplace or healthcare based on whether or not someone's SSN was found in a database. Error rates between 1% and 3% for a labor force of over 120 million people would deny one to four million people the chance to work. When the INS tried a similar pilot system in 1992 as part of a planned databank containing the names of all eligible workers, it could not immediately find information on people in 28% of cases, and it took up to two weeks to find that information by hand. Furthermore, two-thirds of those missing workers were found eligible after the two-week

265. *See* Robert Ellis Smith, *SSNs Nixed From Licenses*, PRIVACY J., Oct. 1999, at 1, 8; *see also* Department of Transportation and Related Agencies Appropriations Act, Pub. L. No. 106-69, § 355, 113 Stat. 986, 1027 (1999) (repealing Section 656(b) of IIRIRA).

266. *See* John J. Miller & Stephen Moore, *A National ID System: Big Brother's Solution to Illegal Immigration*, THE CATO INSTITUTE, Sept. 7, 1995; *see also* Stephen Moore, *A National Identification System: Hearing on H.R. 231 Before the House Subcomm. on the Immigration and Claims*, 105th Cong. (1997) (statement of Stephen Moore, Economist, The Cato Institute), *available at* http://www.cato.org/testimony/ct-sm051397.html. In a 1997 report, the Social Security Administration estimates costs ranging from approximately $3.9 billion to $9.2 billion to issue enhanced Social Security cards. *See* Social Security Administration, *Report to Congress on Options For Enhancing the Social Security Card*, September 1997, Table 32; *see also* Smith, *supra* note 5, at 21.

search.[267] The error rate would certainly be higher for a broader NIDS. In congressional testimony against the 1996 law, Senator Abraham noted that "a mere 1 percent error margin in the database could, on an annual basis, affect 600,000 employment decisions in this country. . . . [T]hat means twice the number of total illegal aliens that come into this country each year."[268]

The existence of a government databank per se increases the likelihood of privacy infringements. For instance, in 1995, over 500 IRS agents were found checking the financial data of friends, relatives, and celebrities. While only a few agents lost their jobs, the IRS vowed that such misuse of confidential data would not happen again. However, a similar incident occurred in 1997.[269]

The major databanks that could make up a NIDS might be accessible to a wide range of users, perhaps through the Internet. This might make personal information available to those with Internet access and authority to enter the databases or the ability to hack into them. Indeed, one of the problems with electronic centralizing of information is that it makes it simpler for those with access, inappropriate as it might be, to get information that might otherwise require a physical search and a search warrant.[270] Here confidentiality may simply imply access for numerous authorized users while providing little or no privacy. The posting of SSNs online by P-TRAK, a part of Lexis-Nexis, and the Social Security Personal Earnings and Benefit Estimate System ("PEBES") for accessing wage and benefits data are examples where government data might be even more widely available than data within government databanks. These systems created so much controversy that they had to be stopped.[271]

Government databanks and identification schemes linked to an ID number also increase the likelihood of private collection of more data. Obtaining SSNs often shown on driver's licenses permit identity thieves to obtain purchasing profiles from credit card companies, as well as health information collected in private medical databases such as the Medical Information Bureau.[272] The tracking of personal in-

---

267. *See* Glenn Garvin, *Bringing the Border War Home*, REASON, Oct. 1995, at 18.

268. 142 CONG. REC. S3328 (1996) (statement of Sen. Abraham).

269. *See* Robert D. Hershey, *Snooping by I.R.S. Employees Has Not Stopped, Report Finds*, N.Y. TIMES, Apr. 9, 1997, at A16.

270. *See* Letter from Dick Armey, Majority Leader, House of Representatives, to the Honorable Tommy G. Thompson, Secretary of Health and Human Services (May 15, 2001), *available at* http://freedom.house.gov/library/technology/medletter3.asp.

271. *See* George Mannes, *Angry Callers Want Off Online File*, N.Y. DAILY NEWS, Sept. 20, 1996, at 22; *see also* John Schwartz, Barbara J. Saffir & Staff, *Privacy Concerns Short-Circuit Social Security's Online Service; Agency Unplugs Web Feature as It Reconsiders Security*, WASH. POST, Apr. 10, 1997, at A23.

272. *See* Robert Kuttner, *Why Not a National ID Card?*, WASH. POST, Sept. 6, 1993, at A23. The Medical Information Bureau does not use SSNs. *Id.*

formation by state and federal governments and private corporations reinforces the development of a NIDS. Furthermore, the clearinghouse provision of the HHS medical records regulations could centralize health information in depositories with relatively easy administrative access for law enforcement and national security agencies.

Rather than spending billions of dollars on an ID system destined to fail in its most serious purposes, law enforcement should focus its resources to find the few serious perpetrators. The cost-effective targeting and marshalling of law enforcement resources that respect probable cause and due process standards constitute one of the strongest ways to address social ills while maintaining fundamental rights. A NIDS instead would contribute to misuses and would create an increasingly costly and self-perpetuating bureaucracy.

In short, despite pressure for technical fixes for complex social problems such as terrorism, a NIDS is unlikely to solve the problems that its features are intended to fix. Yet the laws and databanks of a NIDS, once established, are likely to remain permanent bureaucratic systems with detrimental consequences. The creation of a NIDS develops the possibility of expanded access to personal data without consent or due process. As Amitai Etzioni noted in *The Limits of Privacy*, a NIDS provides the U.S. system with greater information on individuals than the Stasi (the East German secret police) ever had at the height of their power.[273]

VIII. FUNDAMENTAL CRITIQUE OF A NATIONAL ID AND PROFILING

Beyond practical problems, there are fundamental reasons why both a national ID and a NIDS demean personhood and identity.[274] Both American practicality and principles suggest that a national ID card is fundamentally foreign to our country.[275] A national ID reverses the proper relationship between citizens and the state. The federal government was created by and derives its powers from the people; under a national ID system, the government creates — and denies — identities, and thus expands its powers. In an age where information is power, centralized information in a national databank increases government power.

> The issue is not just privacy; it is government power.... "What ID numbers do is centralize

273. *See* AMITAI ETZIONI, THE LIMITS OF PRIVACY 10 (1999).

274. Richard Sobel, Why a National ID is a Bad Idea, Presentation at Harvard University, John F. Kennedy School of Government (Nov. 8, 2001).

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

> power, and in a time when knowledge is power, then centralized information is centralized power.... [P]eople have a gut sense that this is not a good idea".... Whether that "gut sense" will find effective political voice is the troublesome question.[276]

Contrary to the Preamble's goal to "secure the Blessing of Liberty to ourselves and our posterity," a NIDS represents a fundamental constitutional violation.[277] There is no constitutional basis for a national ID since it is not among the enumerated powers in the Constitution,[278] nor is it necessary and proper for carrying out any enumerated power. Moreover, requirements to carry and produce an ID on demand violate Fourth Amendment protections that people be left alone in the absence of reasonable suspicion. Increased requests for identification without individualized suspicion diminish the security owed to Americans in their persons and papers and could deny the right to travel under the Fourteenth Amendment.

No matter how stringent the standards for checking national IDs, the existence of national IDs may expand their uses. This would increase the likelihood that they would be used for surveillance of individuals even though public opinion opposes random searches of citizens.[279] Moreover, under current Supreme Court doctrine not always followed, the police may only ask for ID when there is at least reasonable suspicion of criminal activity. Requiring a national ID would erode this standard.[280]

A federalized NIDS presents large-scale problems because a national ID requires a national ID number and a single national or interconnected databank. Current pressures to expand the New Hires Databank, already extended to student loan defaulters, sets the basis for a centralized information repository. Drawing personal data from private databanks for government purposes without constitutional protections further weakens personal privacy protections supposedly guaran-

---

276. Twight, *Watching You*, *supra* note 13, at 185 (quoting Richard Sobel).

277. *See* Richard Sobel, *Not for Identification Purposes: National Identity Numbers Don't Belong in an Open Society*, 1.2 THE FILTER (Aug. 12, 1998), *at* http://cyber.law.harvard.edu/filter/081298/ids.html.

278. *See* Miller & Moore, *supra* note 266 ("Nowhere in the Constitution is the federal government conferred authority to establish a computer registry, to compel citizens to obtain a national i.d. card, or to involve itself this intimately in the everyday business decisions of employers."); *see also* Moore, *supra* note 266.

279. In a study conducted from late 1978 to early 1979, 72% of the public said they felt that the police should not have the right to stop people on the street to demand identification if the person was not doing anything illegal. *See* LOUIS HARRIS & ASSOCIATES & ALAN F. WESTIN, THE DIMENSIONS OF PRIVACY 70 (1981).

280. A later article by this Author will critique the idea of a national ID as constitutionally infirm, especially under a series of Amendments (3–5, 13–15). *See generally* AKHIL REED AMAR, THE BILL OF RIGHTS: CREATION AND RECONSTRUCTION (1998).

teed in the Privacy Act of 1974. Data dossiers will provide detailed descriptions of each individual's habits and actions, even though such collections will not be fully accurate or secure from unauthorized uses, inappropriately authorized users, or hackers. The system would be prone to mistake, arbitrariness, and loss, the consequences of which could be devastating in terms of everything from lost jobs to lost freedom. Once in place, such a system would be almost impossible to dismantle, while the imperatives of efficiency and wider use would expand its reach.

Specific aspects of a NIDS are also troublesome. For example, biometrics, like fingerprints on national IDs, in themselves invade privacy. This occurs because the process of developing biometrics requires the capture of a person's features. Moreover, biometric representations of those features imply criminal behavior. Biometrics can be counterfeited, and if centralized in a national databank, inappropriately accessed and reproduced.[281]

Closely related to the debate over a national ID is the preference to expand the profiling of airline passengers. The debate over passenger profiling requires evaluation of the justification behind profiling. The practice of profiling harms individuals in the legal system because it reverses the presumption of innocence. In the absence of profiling, each person acts as an innocent agent in the system and the amount of authority or police power that may be exerted over him is limited directly by that innocence. Someone reasonably suspected of a crime may be subject to a stronger level of police power as suspicion and evidence of individual guilt increases. This spectrum preserves individual personhood when it only subjects the individual to the authority of the state where suspicions of individual guilt increase beyond a reasonable threshold.

Yet profiling conflicts with this spectrum because, though based on somewhat more objective factors, it creates a generalized presumption of likely guilt without actual illegitimate behavior. Profiling, both in racial and nonracial forms, sets up a status or behavior model that allows for the exertion of state power regardless of whether there is any basis for questioning an individual's personal presumption of innocence.[282] Breaking the connection between individual presumption

---

281. *See* Dana Hawkins et al., *Tech vs. Terrorists: New scanners might foil some plots, but every fix has its flaws*, U.S. NEWS & WORLD REP., Oct. 8, 2001, at 56; David Banisar, *A Review of New Surveillance Technologies*, PRIVACY J., Nov. 2001, at 1; John Fried, *Biometrics: Ready for PrimeTime?*, PRIVACY J., June 2000, at 1 for reports on the failings of new technologies such as biometrics.

282. An example of this is an 86-year-old Medal of Honor winner carrying his medal of honor who matched a security profile set up by an airline. He faced the exertion of power by the airline security forces even though there was no individualized suspicion of guilt. *See* Richard Lowry, *Profiles in Cowardice: How to Deal with the Terrorist Threat — and How Not To*, NAT'L REV., Jan. 28, 2002, at 32; *see also* David

of innocence and the right to exert police power has significant implications for personhood because of the generalized nature of associated guilt. It allows people to be treated as members of a group or class identified by a presumed suspect status or behavior model instead of specific individuals presumed innocent under the law. This is particularly harmful when the profiling is preventative and penalizes individuals for meeting status or behavior models. Fitting a model raises the level of individual suspicion. However, this is only true in a limited sense. Profiling models do not look at an individual's actions and ask, for example, does this person have an alibi or a motivation? Rather, profiling substitutes suspicion based on data for suspicion based on elements of a crime. It devotes attention and hence resources to the vast majority of innocent individuals rather than focusing on actual or likely misdeeds. It typically involves relative probabilities where the predictability is quite low.

The development of data mosaics and the profiling of passengers to determine whether they are likely to break the law raises troubling questions of efficacy and legitimacy. Mosaics and profiling presuppose the right to scrutinize citizenry in ordinary circumstances. They imply not only a criminalization of law-abiding citizens but also a justification for suspicion and intrusion on a broad segment of Americans based on a single heinous crime. Like ID requirements that presume everyone to be an illegal alien, airline ID requirements suggest that everyone is a potential hijacker until proven otherwise. They require a background check to exercise the right to travel based on information taken from interconnected and matched databanks. The use of a profiling technique for catching perpetrators after a crime will not necessarily identify future miscreants. While the elements that identify a particular group might be factual bases for heightened scrutiny, the use of racial elements per se in profiles add a discriminatory character. It also implies that the preponderance of terrorists would fall into a particular ethnic group, thus diverting attention and resources from appropriately investigating other individuals.

Across the board profiling fails the reasonable suspicion test for individuals on its face. Potential profiling claims were considered by the court in *Reid v. Georgia* about the profiling of two individuals who fit the "drug courier profile" established by the DEA and were traveling from a town known to be a source for drugs.[283] The court ruled it unconstitutional under the Fourth Amendment in a per curiam opinion with Justice William Rehnquist dissenting. Passenger profiling for the purpose of preventing terrorism may represent different issues, but the presumptions are similar. Prior to the application of

---

Armstrong & Joseph Pereira, *Flight Risks: Nation's Airlines Adopt Aggressive Measures for Passenger Profiling*, WALL ST. J., Oct. 23, 2001, at 1.

283. 448 U.S. 438 (1980).

profiling, there needs to be an objective standard for applying potentially travel-denying characterizations to the behavior of individuals involved in the legal activities of air travel.

Asking when profiling should be permitted presupposes that profiling is justified. Working from that assumption, however, the investigation of a single major crime would give enlarged discretion to state authority. The important feature here is that this profiling is reactive to the fact that such a crime has been committed and not proactive. The situation might include a single event so shocking to the conscience of the nation that it turns around our presumptions of innocence. Such an event changes the notion of personhood in our society as a whole and therefore systematically lowers the presumption of innocence for all individuals across the board.

Appropriate uses of police power should still operate with a general conception of individual innocence. Otherwise, some argue that 9/11 is such a core event that it turns our very notions of presumption of innocence. Relatedly, the profiling model assumes the recurrence of the circumstances of the single event that has already happened. For example, preventing potential terrorist acts like 9/11 would encourage efforts to catch future terrorists by looking at individuals with unclear justifications for flight school training. While reasonable, this represents focusing on a problem with a low likelihood of recurrence.

Another concern about having a national ID card is the risk of having one's identity denied (or revoked) accidentally or purposefully. One would be presumed not to be oneself without positive proof. Errors in the database could deny individuals their jobs or freedom. Incorrect information in a secure databank will be very difficult to correct. It would be even harder to get accurate data reentered or to get a new national ID if it were lost. Losing one's ID risks losing one's identity, livelihood, and liberty. Not showing up in the database or not carrying one's national ID at a crucial time, such as at a job check, border crossing, or traffic stop, or having small errors in the ID, could mean unemployment, detention, or arrest. The expectation of carrying an ID would likely increase the official exercise of arbitrary discretion on encountering someone without a card.

As noted above, a NIDS would also be very costly to establish, update, and extend. The combined costs of creating and administering the system would be enormously expensive even if the physical card were inexpensive. Just as the largest cost of education is the foregone earnings from not working, the largest cost of a national ID would be the foregone freedoms from intrusion. Expensive and unreliable technological fixes like "tamper-proof" ID systems inflate the sense, rather than the reality, of security when true safety and liberty may be lost.

A national ID would be unlikely to successfully solve problems of terrorism or illegal immigration. First-time or previously unknown terrorists can get false IDs or travel on foreign passports that don't tie into domestic databanks because, as Schneier notes, there is no "pre-existing database of bad guys."[284] For instance, the 9/11 terrorists entered on foreign passports and this prospect would be unaffected by a NIDS. Few terrorists are on intelligence watch lists and many of the names that appear there are approximated or misspelled.[285] It does not follow that 285 million American citizens should have to carry cards in order to try to find a few terrorists or illegal aliens.

A national ID has not solved terrorism elsewhere. The Soviet Union and South African pass systems prevented neither terrorism nor illegal immigration. These governments in transition have now modified or abandoned the types of surveillance systems the U.S. is contemplating. Israel's ID system hasn't prevented terror. Institutions like prisons where everyone is constantly monitored and identified are not free from crime or violence.[286] No ID system is foolproof. The implementation of better foreign policy, international coalitions, external intelligence, and undermining of terror abroad will remove the funding, bases, and perpetrators of terrorism and will better affect national and international security.[287]

Requirements for a national ID or for safe traveler cards will not make air travel safer than nonintrusive and physical solutions that do not undermine travel rights. Bag matching and complete screening increase air safety without undermining individual rights.[288] Most perpetrators motivated to create a destructive device can forge documents or choose not to travel on a plane that they have put in jeopardy. The few who choose to martyr themselves can be better prevented through physical protections such as cockpit security and sky marshalls and a careful observation of preloading and in-flight procedures.

Physical solutions like reinforced cockpit doors, air marshalls, retrained crews, and an alert flying public can protect against hijacking without treating constitutionally protected citizens as suspects or denying them the right to travel. Integrating watch-lists for law en-

---

284. Schneier, *supra* note 121, at 2.

285. *Id.* at 2.

286. *See* SMITH, *supra* note 5, at 6.

287. For a discussion of Americans' preferences in fighting terrorism, see Richard Sobel et al., *National and International Security*, *in* PUBLIC OPINION AND AMERICAN FOREIGN POLICY, (John E. Rielly ed., 1999); *see also* Richard Sobel et al., *Anti-Terror Campaign Has Wide Support, Even at the Expense of Cherished Rights*, CHI. TRIB., Nov. 4, 2001, at 1.

288. *See* Robert Ellis Smith, *False ID a Key Part of the Conspiracy*, PRIVACY J., Oct. 2001, at 5. *See also* Mary Lou Pickel, *War on Terrorism: Air Security: Impact unknown for new baggage screening*, ATLANTA J.-CONST., Jan. 17, 2002, at 6A.

forcement at border crossings or abroad would do a better job at keeping people out of the country than trying to keep them off airplanes through face recognition or ID technologies. A national ID or a nationalized driver's license would become a license to travel. The very trusted nature of such an air card would allow a terrorist who is able to obtain one to also avoid more direct investigation. Similarly, too great of a focus on air travel removes attention from other potential weak points subject to attack.[289]

Nor would a national ID end discrimination. Minorities would not be subject to less scrutiny because they would still be asked to provide a national ID to obtain work more frequently than white Americans.[290] A NIDS would also create a class system.[291] Moreover, if approval by a majority in a national survey led to the inclusion of religious or ethnic data on the card or in a databank, discrimination would increase.[292] While some might feel this discriminatory approach could be helpful in easily identifying Muslims, a similar approach would also have assisted in rounding up Japanese-Americans during World War II.

Terrorism is but the most recent justification for a national ID card, periodically proposed to stop threats ranging from communism to illegal immigration. A NIDS is most simply a means of keeping track of and controlling people that magnifies the power of governments and officials. Suggestions that an ID might be voluntary or that only terrorists' fingerprints or facial scans would be kept in a national database conflicts with the imperatives of productivity and efficiency: namely, that the card become mandatory and the information gathered be used repeatedly and more efficiently. Since there is no database of all terrorists, whose number is relatively small anyways, the databank would soon include lesser suspects or criminals; in the extreme, it could even lead to a national system that detains or denies travel for unpaid parking tickets. A nationalized driver's license system, where the license number becomes another national ID number, moves beyond the license as a credential to drive that has become a de facto national ID card, making it a de jure one. Requirements for even pre-

289. *See* Viktor Mayer-Schoenberger, Perspectives on Privacy and Security, Presentation to Conference on Building Effective E-Government, John F. Kennedy School of Government, Cambridge, MA (January 25, 2002).

290. *See* USGAO Report to the Congress, *Immigration Reform: Employer Sanctions and the Questions of Discrimination* 138, GAO/GGD-90-62, Mar. 1990.

291. *See* Joe Sharkey, *Class Consciousness Comes to Airport Security*, N.Y. TIMES, Jan. 6, 2002, § 4, at 3; *see also* Sara Rimer, *As Security Tightens, the Race Goes to the Savviest*, N.Y. TIMES, Jan. 20, 2002, § 1, at 18.

292. A significant minority of 35% supported including religion on a national ID. Other countries, like Russia, include nationality on national ID documents. *See* Robert Ellis Smith, *The Politics of the ID-card Debate*, PRIVACY J., Dec. 2001, at 4.

senting local IDs should stay tied to limited uses under constitutional standards.[293]

If there were a full realization of a NIDS in the U.S. and everyone received a national ID card, citizens would eventually be required to carry and produce it upon official demand. The regularity of such procedures would, in effect, make a police demand for ID a routine and reasonable request, without any expectation of privacy; this could further erode Fourth Amendment protections.[294] The phrase "Your papers, please" or television commercials such as American Express' reminding everyone "don't leave home without it" used to be humorous in the United States. The implications are no longer so amusing.

Rather than spending a tenth of the pre-9/11 defense budget on an ID system that covers everyone and is destined to fail in its most serious purposes, law enforcement should target its resources in cost-effective ways to find the few serious perpetrators of terrorism. Applying principles of reasonable suspicion and probable cause are both cost-effective and encourage professional law enforcement. Focused investigations that target the most probable suspects are better expenditures of money and result in a better protection of freedom. While willingness to bear any cost is understandable and admirable in the immediate aftermath of an attack on the United States, the principles of efficiency, cost-effectiveness, and constitutional firmity would be a better means to effective and sustainable ends.

Our Constitution of enumerated powers and reserved rights requires public officials to address problems like crime or terrorism without undermining these fundamental rights. Chief Justice Rehnquist, in his book on wartime civil liberties, notes that "it is all too easy to slide from a case of genuine military necessity. . . to one where the threat is not critical and the power either dubious or nonexistent."[295] Benjamin Franklin reminded us that even during the perilous era of our Revolutionary War, those who would give up liberty for a little security deserve neither.[296] Freedom and spontaneity, as noted by Justice John Marshall Harlan in his dissent in *United States v. White*, are undermined by the constant surveillance that a national ID represents.[297] If widespread civil unrest were to return to the U.S.,

---

293. *See* EPIC Report, *supra* note 40, at 7. For two instances where courts held unconstitutional attempts by local communities to require service workers to carry ID cards, see Wallace v. Palm Beach, 624 F.Supp. 864 (S.D. Fla. 1985) and Service Machine & Shipbuilding Corp. v. Edwards, 671 F.2d 70 (5th Cir. 1980).

294. *See* Shaun B. Spencer, *Security Versus Privacy: Reframing the Debate*, 79 DENV. U. L. REV. (forthcoming 2002); *see also* Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 79 DENV. U. L. REV. (forthcoming 2002).

295. REHNQUIST, *supra* note 189, at 234.

296. *Quoted in* Richard Sobel, *Anti-terror campaign has wide support, even at the expense of cherished rights*, CHI. TRIB., Nov. 4, 2001, at C1.

297. 401 U.S. 745, 787 (1971).

a NIDS would make surveillance, dossier creation, location, and invasions of privacy technologically simple.

In sum, a national ID undermines basic freedoms, fails to solve the problems better addressed in constitutionally sound and effective ways. The far-reaching implications of a national ID demean the very freedoms now under external attack that our leaders endorse as the basis for U.S. military response. It raises profound questions for prudent citizens and leaders alike.

IX. FUNDAMENTAL CRITIQUE OF A NIDS

Beyond pragmatic and fundamental problems for a national ID, a NIDS also contradicts basic American principles and freedoms. The Constitution and the Bill of Rights afford protections against the arbitrary exercise of governmental power. This scheme of protection encompasses federalism as the division of power among different levels of local, state, and national governments. It also includes a separation of powers that divides authority, thereby incorporating checks and balances among the legislative, executive, and judicial branches of government. One essential purpose of both federalism and separation of powers is the resistance to the threat to democracy that is posed by centralized power.[298] These structural provisions of governance consciously privilege liberty over efficiency. "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."[299]

Similarly, the presumption and presence of unimpeded individual action protected by the political buffer around personhood and undergirding individual rights clash with a national ID.[300] These "privileges and immunities" are represented by the right of citizenship, the burden of proof on the state, the presumption of innocence, the prohibition of unreasonable search (reasonableness based on particularized suspicion), and the privilege against self-incrimination.[301] These rights exist because the individual's nature as a person under the Constitution

298. GORDON SILVERSTEIN, IMBALANCE OF POWERS 30–31 (1997).

299. *See* Stolberg, *supra* note 23 (quoting Richard Sobel of Harvard University); *see also* CONG. REC., *supra* note 236 (statement of Sen. Abraham) (noting that IIRIRA and especially a pilot for checking work eligibility against a national databank set "in place the infrastructure necessary for a mandatory national system and establishes the principle that companies should gain Government approval before hiring any employee.").

300. *See* Christopher Pollmann, Capitalist Development, Personal Identity and Human Rights, Human Rights Program, Harvard Law School (Feb. 14, 2001) (on file with author).

301. *See* U.S. CONST. art. IV, § 2; *see also* U.S. CONST. amend. XIV, § 2, which states that "[n]o State shall make or enforce any law which shall abridge the privileges or immunities of the citizens of the United States."

is protected from arbitrary and unrestricted governmental action. They inhere in personhood and they become degraded when an individual may only exercise them by having an ID card, number, or place in a databank. In short, because political identity and personhood exist inherently in a free society, these rights exist by presumption, and are not subject to ID checks before they can be exercised. In the same sense, native citizenship is founded in birthright and it (as well as the legally naturalized form) is not subject to modification by governmental permission or action.

A NIDS creates bureaucratic hindrances for citizens and immigrants in a free country. A NIDS turns citizens into charges of the government. This effectively reverses the nature of democratic government by consent and the foundation of citizenship as expressed in the Fourteenth Amendment. Because consent by the governed undergirds active citizenship and personhood, the government's power under a NIDS to give or take away identities destroys the proper relationship of the government to the citizenry. Since the government would issue or deny a national ID card, it would effectively own and consent to people's identities. The proper balance of citizen and government would become distorted if the government bestows and deprives identity through documents, numbers, or locations in databanks.

National document requirements reverse the proper relationship of citizen to government articulated in the Declaration of Independence[302] and the Preamble,[303] and bestow ersatz political and personal identities. A NIDS substitutes for the proper relationship a system based on bureaucratic requirements rather than fundamental rights. The rights to life, liberty, and the pursuit of happiness and the right to travel precede the Constitution in their fundamental location in the Articles of Confederation. The Articles state that:

---

302. *See* 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.

303. *See* U.S. CONST. pmbl., "We the People of the United States, in Order to form a more perfect Union, establish justice . . . secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America."

> 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.[304]

The requirement for governmental identification in order to fly burdens this right to travel freely.

Centralization of extensive information makes abuse likely because the government possesses the power to coerce through the courts, police, and the military. Like the assurances that SSNs would only be used for tracking pension account payments, promises of limitations on national identity cards or health databanks would soon be compromised by expanding the number of agencies with access to some of its data.[305] This movement towards centralization has already been set in motion by the HHS health records regulations that would allow law enforcement and national security access to medical information.[306] The "USA PATRIOT Act" permits law enforcement to access medical, education, and financial information without appropriate procedural safeguards.[307] Under a NIDS, rights that a person under the law should realize cease to exist absent proper identification.

A NIDS has numerous constitutional infirmities. The Fourth, Fifth, Ninth, and Fourteenth Amendments' provisions on liberty require the government to leave constitutionally protected citizens alone. A person's privacy should not be invaded unless there is evidence about that individual amounting to a proper standard for intrusion. The Fourth Amendment protects individuals against unreasonable search and seizure unless there is probable cause and particularized suspicion of that individual. The combination of the right to remain silent in the First and Fifth Amendments and the prohibition against unreasonable search in the Fourth Amendment mandate against requirements for possessing and presenting identification. A NIDS makes it tempting to circumvent the Fourth Amendment by

---

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

305. *See* Jeffrey Rosen, *The Eroded Self*, N.Y. TIMES SUNDAY MAG., Apr. 30, 2000, at 46. It could also be possible for governments to identify people with certain partisan affiliations.

306. *See* 45 C.F.R. § 164.512 (2001).

307. *See* The Uniting and Strengthening America by providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) [hereinafter USA PATRIOT Act]; *see also* Amy Pagnozzi, *Uncloaking a Fleecing of Rights*, HARTFORD COURANT, Jan. 15, 2002, at B1.

rendering it technologically easy to get information that would have previously required physical searches and judicial authorization.

In this way, because of the ease of access, centralized databanks make ID checks simple and common. Requirements for photo identification to work or fly destroy a basic freedom accorded to all Americans by the Constitution: the right to be left alone in privacy and anonymity unless there is a particularly compelling reason for intrusion.[308] As Justice Louis Brandeis noted, "[the makers of our Constitution] conferred, against the government, the right to be let alone — the most comprehensive of rights and the right most valued by civilized men."[309]

The Fifth and Fourteenth Amendments prohibit the deprivation of liberty and property absent due process. However, a NIDS removes a person's identity and transfers it to cards, numbers, and databanks.[310] Consequently, identity exists in a document rather than in a person, as people become paper, plastic, or electronic subjects.[311] Thus, losing one's place in the NIDS risks losing one's identity, livelihood, and liberty.

The creation of a NIDS poses more threats to the principle of federalism embodied in the Constitution and Tenth Amendment, wherein powers that are not delegated to the federal government are reserved to the states.[312] Under their police powers, states have the authority to set their own requirements for law enforcement and licensing. However, under a NIDS, as in the case of federalizing the driver's license, an ID would become a national document. The imposition of federal standards on something as fundamental as identification would circumvent the states' police power and discretion to serve and identify their residents.

The spontaneity of human existence, Robert Smith argues, disappears in the requirement constantly to carry "papers."[313] Simply get-

---

308. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1891); *see also infra* note 360; Robert Ellis Smith, Remarks in Montreal, Canada on Privacy and Airline Services: Requirement for Identification on Airlines (Sept. 23–26, 1997) (transcript on file with author).

309. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (warning about beneficent government actions).

310. *See, e.g.*, HENRY LOUIS GATES, JR., THIRTEEN WAYS OF LOOKING AT A BLACK MAN xx–xxi, 207–08 (Vintage Books 1998).

311. *See id.*

312. *See* Roberto Suro, *Rehnquist: Too Many Offenses are Becoming Federal Crimes*, WASH. POST, Jan. 1, 1999, at A2 (related analysis of expansion of state responsibilities into the federal realm); *see also* William Rehnquist, C.J., *1998 Year-End Report of the Federal Judiciary*, (Jan. 1, 1999), *available at* http://www.uscourts.gov/ttb/jan99ttb/january1999.html ("The trend to federalize crimes that traditionally have been handled by the state courts . . . threatens to change entirely the nature of our federal system.").

313. Robert Ellis Smith, *The True Terror of Freedom Is In the Card*, N.Y. TIMES MAG., Sept. 8, 1996, at 58; *see also* United States v. White, 401 U.S. 745, 790 (1971)

ting on a plane, traveling around major cities or getting a new job would become impossible without government ID. Getting in and out of one's office becomes an occasion for surveillance through the use of electronic ID cards, whose use is regularly recorded. Traveling with "E-ZPass" on toll roads records a driver's route.

By combining information previously available only from multiple sources, a full NIDS would create personal mosaics and dossiers. These would infuse information that, standing alone, might have been inconclusive with meaning gleaned from other sources. These collections of details on individuals' lives constitute serious invasions of privacy, imply ongoing surveillance of lawful activities, and result in chilling effects on political involvement and expression; furthermore, they demean personhood cumulatively.

Each provision combining into an informal NIDS constitutes bureaucratic surveillance under the name of solving social problems that such a system cannot fix or that can be better addressed in other ways. A national ID and NIDS constitute a general invasion of privacy by collecting and making accessible too much information about citizens and other residents.

Especially because of the history of discriminatory and oppressive uses of identity badges and numbers against Jews in Germany, slaves through the Civil War, and blacks under Apartheid in South Africa, all Americans need to be wary of the problems that quick fixes such as identity documents are likely to create. Any NIDS would ultimately offend and intrude upon fundamental rights. Those desiring to maintain an open society need to recognize a national ID and NIDS, particularly integrated with private, law enforcement, and national security databanks, imperil rights more than they serve useful purposes. In essence, because a NIDS itself is a bureaucratic mechanism utilized to collect people's private and public information, it cannot be adequately safeguarded to prevent privacy invasions and abuses of personhood. Such a system is fundamentally flawed.

X. POST-9/11 ANALYSIS: CHANGES IN PREMISES SINCE THE ATTACKS

Before 9/11, the U.S. experienced a momentum toward privacy and away from racial profiling. In a 1999 interview about the threat of terrorism, President Clinton noted that "we've got to preserve civil liberties, resolve all doubt in favor of that. . . ."[314] During the 2000 presidential campaign, both Governor George W. Bush and Vice

(Harlan, J., in dissent) ("[A]n ordinary citizen . . . may carry on his private discourse freely, openly, and spontaneously without measuring his every word. . . .").

314. Judith Miller & William J. Broad, *Clinton Describes Terrorism Threat for the 21st Century*, N.Y. TIMES, Jan. 22, 1999, at A1.

President Al Gore agreed that personal privacy was a critical issue in the 21st Century. Gore went so far as to call for an Electronic Bill of Rights, to include "the right to choose whether personal information is disclosed; the right to know how, when, and how much of that information is being used; the right to see it yourself; and the right to know if it's accurate."[315] When asked to give his position on privacy during the campaign, Bush proclaimed: "I believe . . . every American should have absolute control over his or her personal information."[316] William Safire asked in the *New York Times* if Bush would be "[t]he Privacy President?" because he approved the HHS medical records regulations and a spokesman claimed he would generally take the pro-privacy side in controversies.[317]

During the second presidential debate in October 2000, Governor Bush supported a federal law banning racial profiling by police and other authorities at all levels of government. In February of 2001, he promised to look "at all opportunities" to end racial profiling.[318] Similarly, during his confirmation hearings in January of 2001, Attorney General designate John Ashcroft said, "I think racial profiling is wrong. I think it's unconstitutional. I think it violates the 14th Amendment. . . . I will make racial profiling a priority of mine."[319]

This momentum towards privacy slowed sharply when immediate concerns about national safety and security surfaced on 9/11. In an ABC News/*Washington Post* poll taken on September 13, 2001, 71% of those polled said they would support legislation making it easier for the FBI and other authorities to investigate suspected terrorists even if the proposed laws would require giving up personal liberties and privacy.[320] While public preferences were heightened by the proximity to the tragedy of 9/11, an overwhelming majority of Americans showed support for the restrictions on civil liberties imposed in the name of the war on terrorism.[321]

---

315. *Bush, Gore Outline Positions to IEEE-USA On Technology and the National Economy*, IEEE-USA News (Institute of Electrical and Electronics Engineers, Inc., Washington, D.C., Oct. 27, 2000), *available at* http://www.ieeeusa.org/releases/2000/001030pr.html (last visited Feb. 26, 2002).

316. Dana Hawkins, *Medical Privacy Rules Give Patients and Marketers Access to Health Data*, U.S. NEWS & WORLD REP., Jan. 29, 2001, at 47.

317. *See* William Safire, *The Privacy President?*, N.Y. TIMES, Apr. 19, 2001, at A25. But see Pear, *supra* note 256, for a reversal of the Bush position.

318. *See* Sen. Russell Feingold, *Racial Profiling*, 147 CONG. REC. S2270, S2272 (daily ed. Mar. 14, 2001).

319. *Id.*

320. *ABC News/Washington Post Poll.* (Sept. 13, 2001), *available at* http://www.pollingreport.com/terror6.htm (last visited Feb. 26, 2002).

321. *See Newsweek Poll*, Jan. 31–Feb. 1, *available at* http://www.pollingreport.com/terror.htm; *see also* Richard Sobel, *Anti-terror campaign has wide support, even at the expense of cherished rights*, CHI. TRIB., Nov. 4, 2001, at C1.

The shift in public opinion and media coverage following the attacks on the World Trade Center and the Pentagon was accompanied by a dramatic change in rhetoric and policy concerning privacy and civil liberties. Analyzing the Aviation and Transportation Security Act,[322] legislation designed to reform air security, one public official explained:

> We're so accustomed to personal freedoms and trying to keep government out of our lives and out of our business or personal affairs and that's appropriate. When it comes to issues of national security when you have someone that is willing again to die to take down a plane and passengers and thousands of people on the ground, we have to balance [personal freedoms] with our security needs. . . .[323]

The idea that the new challenges facing America require giving up privacy and civil liberties has been embodied in much new legislation. Perhaps the most important is the USA PATRIOT Act.[324] Gregory T. Nojeim, Associate Director of the ACLU's Washington office, clarified that "[t]hese new and unchecked powers could be used against American citizens who are not under criminal investigation, immigrants who are here within our borders legally and also against those whose First Amendment activities are deemed to be threats to national security by the Attorney General."[325] Among the bill's provisions that affect non-terrorist suspects are an expanded ability of the government to conduct secret searches in routine criminal investigations unrelated to terrorism, and a grant of broad access to the FBI to review sensitive medical, financial, mental health, and educational records about individuals without having to show evidence of a crime and without a court order.[326] The ACLU remarked that "the USA PATRIOT Act (H.R. 3162) [gives] enormous, unwarranted power to

---

322. Aviation and Transportation Security Act, Pub. L. No. 107-71, 115 Stat. 597 (2001).

323. *What Regulations are Needed to Ensure Air Security: Hearing of the Energy Policy, Natural Resources, and Regulatory Affairs Subcomm. Of the House Government Reform Comm.*, 107th Cong. 2001 (statement of Rep. John L. Mica).

324. *See* USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 1(a), 115 Stat. 272 (2001).

325. Stephanie Olsen, *Patriot Act Draws Privacy Concerns*, CNET News.com (Oct. 26, 2001), *available at* http://news.com.com/2100-1023-275026.html?tag=prntfr (last visited Feb. 26, 2002).

326. *See* HIPAA, *ACLU Pledges to Monitor Impact on Civil Liberties, Continue to Work with Administration Officials*, (Oct. 26, 2001), *available at* http://www.hipaadvisory.com/news/2001/1026patriot.htm; *see also* USA PATRIOT Act, *supra* note 324.

the executive branch unchecked by meaningful judicial review."[327] William Safire called the President's original plan for military tribunals as "assum[ing] what amounts to dictatorial power to jail or execute aliens."[328]

In the post-9/11 climate, the call for a national ID has been revived with more intensity and larger public approval than in the past.[329] In the Pew poll taken immediately after the World Trade Center attacks, 70% of those surveyed favored "requiring that all citizens carry a national identity card,"[330] though the September polling data were affected by a proximity to the terrorist attacks.[331] While other surveys show that "a majority of Americans express . . . support for . . . [national ID] cards as a way to improve security — a turnabout in sentiment from before the terror attacks," by early 2002 support was significantly lower than right after the attack.[332]

It was not surprising that the war on terrorism brought proposals to create a national ID card. The information that "some Sept. 11 hijackers used false identities and obtained driver's licenses illegally"[333] made the prospects for passage of such a proposal more likely, in part because the proposal was presented as increasing information displayed on driver's licenses and linking existing databases to create a

---

327. *See* HIPAA, *supra* note 326; *see also* USA PATRIOT Act, *supra* note 324, §§ 209, 358, 503, 507 (2001).

328. William Safire, *Seizing Dictatorial Power*, N.Y. TIMES, Nov. 15, 2001, at A31.

329.

> "Sept. 11 made the public more receptive to an idea that in calmer times they would not accept," says Charlotte Twight . . . . "It has come up many times in the past, and over the years ordinary Americans have expressed considerable hostility to the idea of a national ID card."

Leinwand, *supra* note 85.

330. *Supra* note 85 and accompanying text.

331. By January 16, 2002, a Gallup poll showed that only 54% supported required carrying of a "government-issued national identification card." Forty-three percent opposed such a requirement. *See* Leinwand, *supra* note 85.

332. Robert O'Harrow, Jr., *States Seek National ID Funds: Motor Vehicle Group Backs High-Tech Driver's Licenses*, WASH. POST, Jan. 14, 2002, at A4. In a 1985 poll, only 39% favored requiring "all U.S. citizens to carry a national identification card." Yankelovich et al., Poll (May 2, 1985) (available on Westlaw POLL database). By February 2002, only a bare majority (50%) were "willing for the government to require carrying a national ID card." Forty-four percent were not willing. CBS News Poll, Air Travel Safety (Feb. 27, 2002), *available at* http://www.cbsnews.com/stories/002/02/27/opinion/polls/main502371.shtml (last visited Feb. 26, 2002). In 1979, 72% of the public felt that police should not have the right to stop people on the street and demand identification if the person in question was not doing anything illegal. Eighty-four percent of Congressmen and 45% of law enforcement officials agreed. LOUIS HARRIS & ASSOCIATES, INC. & DR. ALAN F. WESTIN, THE DIMENSIONS OF PRIVACY: A NATIONAL OPINION RESEARCH SURVEY OF ATTITUDES TOWARD PRIVACY 70 (1981).

333. O'Harrow, Jr., *supra* note 332.

NIDS.[334] The AAMVA had already been pressing for changes to the driver's license system for years, but their spokesman, Jason King, noted that "it took Sept. 11 to [bring] the importance of the driver license into view[.]"[335] At that point they asked Congress for $100 million and authorizing federal legislation.

Senator Richard J. Durbin's (D-IL) proposal for federal funding to develop a national ID from the driver's license would "authorize a study on which biometric identification methods — fingerprint, palm print, iris scan, face scan, or DNA, among others — should be used as the national standard."[336] The legislation also provides steps toward the linking of several federal databases. State motor vehicle authorities would be granted access to the databases of the INS, SSA, and certain law enforcement agencies. The theory is that a combination of these databases could be used to verify the legal status and identity of applicants.[337] Durbin articulated the purpose of his bill as "making the driver's license, which some consider as a de facto national ID card, more reliable and verifiable as a form of personal identification than it is today."[338] This national legislation in the guise of a state initiative undermines privacy, fair information practices, and federalism.

While proposed legislation seeks to create a national ID system, the frequency with which governmental agents ask to see current identification is continuously increasing, particularly at transportation nodes. Although the FAA does not directly forbid airlines from allowing a passenger without identification to board a plane, passengers who are unable or refuse to present identification are subject to additional security measures outlined in an FAA directive not available to the public.[339] FAA passenger identification regulations may be replaced by those of the newly created Transportation Security Administration, which, as of February 17, 2002, has primary responsibility for civil aviation security.[340] The Transportation Security Administration is the product of Senate Bill 1447, signed into law by President Bush on November 19, 2001, in the attempt to "federalize" airport security.[341] The bill authorizes the Undersecretary of Transportation for Security to perform "any such additional screening of passengers and property" on all flights originating in the United States that "the

334. *See* Jennifer 8. Lee, *Upgraded Driver's Licenses Are Urged as National ID's*, N.Y. TIMES, Jan. 8, 2002, at A13.

335. O'Harrow, Jr., *supra* note 332.

336. Leinwand, *supra* note 85.

337. *See generally id.*

338. *Id.*

339. *See supra* notes 25–29 and accompanying text.

340. E-mail from Ned Preston, Historian, Federal Aviation Administration, to Wendy J. Netter, Student, Harvard Law School (Feb. 11, 2002) (on file with author).

341. *See* Brian Blomquist, *Bush: New Air Security Law Greatly Reduces Flight Risk*, N.Y. POST, Nov. 20, 2001, at 2.

Under Secretary deems necessary to enhance aviation security."[342] "We as a people are willing to trade a little less privacy for a little more security," said Stewart Baker, former general counsel to the National Security Agency.[343]

While the Transportation Security Administration begins to change air carrier regulations, airlines and airports are taking their own initiative to impose identification requirements upon passengers. For instance, Boston's Logan Airport, the origin of two of the hijacked planes, has announced the introduction of an identification system called "BorderGuard," which aims to use pattern and facial recognition technology to verify passenger identification.[344] Other airports have interpreted current FAA regulations to require photo identification.[345] Thus, while various proposals for national identification systems are debated, the American people are becoming accustomed to having to present identification in the course of their everyday lives, from airports to athletic events. They are also becoming acclimated to intensive searches of their luggage at airports and government buildings as well as to armed soldiers patrolling air terminals.

As Justice Brandeis reminded us, even well-intentioned official actions in response to major dangers deserve scrutiny. "Experience should teach us to be most on guard to protect liberty when the government purposes are beneficent. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding."[346]

---

342. H.R. 3150, 107th Cong. § 102 (2001) (H.R. 3150 is the House complement of S. 1447).

343. David Streitfeld & Charles Piller, *Response to Terror, A Changed America: Big Brother Finds Ally in Once-Wary High Tech*, L.A. TIMES, Jan. 19, 2002, at A1.

344. *See* Massport Moves Forward With Security Enhancements at Logan; To Begin Testing Document Authentication Technology Immediately, Massport.com, *at* http://www.massport.com/about/press01/press_news_doctest.html (last visited Feb. 26, 2002). Another similar system, "BodySearch," conducts a photographic strip-search of passengers. *See* Dana Hawkins and David LaGesse, *Tech vs. Terrorists: New Scanners Might Foil Some Plots, But Every Fix Has Its Flaws*, U.S. NEWS & WORLD REP., Oct. 8, 2001, at 56; *see also* David Banisar, *A Review of New Surveillance Technologies*, PRIVACY J., Nov. 2001, at 6.

345. For instance, the Port Authority of New York and New Jersey's website informs passengers that a government-issued photo ID is required for check-in at JFK, Newark, and LaGuardia airports. *See* Passenger Security Awareness Tips/Airport Security Bulletin, *at* http://www.panynj.gov/aviation.html (last visited Feb. 26, 2002).

346. Olmstead v. United States, 277 U.S. 438, 479 (1928). Another recent ID requirement with potentially unforeseen consequences for political identity and NIDS is the election reform requirement for first-time voters to provide identification such as a driver's license, utility bill, or pay stub. *See* Edward Walsh, *Senate Eyes Compromise to End Election Bill Deadlock*, WASH. POST, Mar. 2, 2002, at A5. For a discussion of Michigan Attorney General's ruling that a Michigan state law requiring identification to vote is unconstitutional on equal protection grounds, especially for non-drivers and the homeless, see Robert Ellis Smith, *Unconstitutional to Require ID to Vote*, PRIVACY J., Feb. 1997, at 1.

XI. COUNTERVAILING TENDENCIES AWAY FROM A NIDS

Yet, even in this environment of war, there are signs of resistance to a NIDS. President Bush, for instance, has denied the necessity of a national ID card.[347] In a poll taken only two months after the terrorist attacks, airline passengers revealed their belief that a policy requiring ID cards improves safety about as effectively as a ban on restaurant cutlery.[348] In addition, many legislators who voted for the USA PATRIOT Act oppose a national ID card. As Representative Janice D. Schakowsky (D-IL) put it:

> The events of September 11th show us that systems like national identification cards will not deter crazed terrorists from their mission. Those terrorists all have driver's licenses, credit cards and Internet accounts. I urge [those suggesting a national ID card] to pay close attention to the effects your proposal will have on the fundamental freedoms on which this country was founded: freedom of speech and religion, freedom to assembly, freedom of the press, freedom from unreasonable search and seizure, and freedom from imprisonment without due process. Those freedoms cannot be ignored in the name of homeland security. As members of Congress we must evaluate any proposal offered in the name of enhanced security. Does it do what it claims to do? What is the burden on the public in terms of time consumed and freedom lost? Do the benefits outweigh the cost? Is there an incremental gain in security and does it justify the loss of freedom?[349]

Schakowsky proposes that under a rational balancing test a National ID System would fail. Somewhat encouraging are Attorney General Ashcroft's promises to "harmonize the constitutional rights of individuals" with security measures and even Secretary of State Colin

---

347. *See* Robert O'Harrow, Jr., *Rights Groups Oppose ID Card: State Agencies Want More Secure Driver's Licenses*, WASH. POST, Feb. 13, 2002, at A15.

348. *See* J.D. Power and Associates & Yahoo!, Inc. Report: Travelers Strongly Prefer Federal Involvement in Airport Security Screening Process (Nov. 19, 2001), *available at* http://www.jdpa.com/presspass/pr/pressrelease.asp?ID=1104 (last visited Feb. 26, 2002).

349. *Does America Need a National Identifier?: Hearing Before the Government Efficiency, Financial Management and Intergovernmental Relations Subcomm. of the House Government Reform Comm.*, 107th Cong. 3 (2001) (statement of Rep. Janice D. Schakowsky).

Powell and Defense Secretary Donald Rumsfeld's movement toward procedural protections for military detainees.[350]

Amidst the dire prospects of terrorism and a NIDS, there are also countervailing tendencies and efforts to limit their detrimental consequences. First, the principles and bulwarks of the American constitutional system remain substantially in place. Even when the bulwarks are under attack, the existence and articulation of the principles are reminders of their value. The recognition that a NIDS is a peril to liberty motivates countervailing actions. Public sentiment in the polls shows that most Americans do not want their own rights denied even in the pursuit of terrorists. Support for a national ID has dropped in the polls.[351] Opposition to "allowing government agencies to monitor the telephone calls and e-mails" of ordinary Americans has risen from half to two thirds.[352] Voices from across the political spectrum raise questions about the extent of the restrictions.[353] Mindful of the threats the nation faces, citizens call for measured and effective actions that respect our constitutional traditions and defend the very freedoms under attack by those who would use terror.

Particularly important is the recognition that the war on terrorism will be long but finite, and hence that the restrictions on civil liberties need not become a permanent part of American society. As with the USA PATRIOT Act, any legislative restriction should have a sunset provision. Similarly serious concerns, both international piracy in the 19th Century and the Cold War eventually came to an end. Statements that the war on terrorism will be lengthy and that other attacks are possible are realistic reminders that need not become immutable predictions. As in the cases of defeating piracy in the nineteenth century and communism in the twentieth century, it is important to recognize that multilateral international cooperation can bring international terrorism under control and end the need for restrictions on civil liberties. Kathleen Sullivan articulated the reality that the U.S. Constitution is resilient and need not be effectively suspended to deal with

---

350. Attorney General John Ashcroft, Press Briefing at FBI Headquarters (Sept. 18, 2001), *available at* http://www.usdoj.gov/ag/speeches/2001/0918pressbriefing.htm (last visited Feb. 26, 2002).

351. *See* Leinwand, *supra* note 85; *see also supra* notes 331, 332.

352. In CBS News/*New York Times* polls, opposition to monitoring calls and emails of ordinary Americans rose between September 13–14, 2001 (53%) and December 7–10, 2001 (65%). *See* CBS News/*New York Times*, *Poll: Revenge and Return* (Sept. 15, 2001), *at* http://www.cbsnews.com/stories/2001/09/15/opinion/main311417.shtml (last visited Feb. 26, 2002); CBS News/*New York Times*, *Poll: Doubts on Military Tribunals* (Dec. 11, 2001), *at* http://www.cbsnews.com/stories/2001/12/11/opinion/main320935.shtml (last visited Feb. 26, 2002).

353. *See, e.g.*, Jack Dunphy, National ID Cards, Not Worth the Pain, NAT'L REV. ONLINE (Nov. 14, 2001), *at* http://www.nationalreview.com/dunphy/dunphy111401.shtml (last visited Feb. 26, 2002). Dunphy is the pseudonym for a Los Angeles police officer.

terrorism.[354] It is possible to address the present emergency within the framework of the Constitution. "The nation ought not suspend the Constitution to deal with the emergency on different terms, thereby creating a constitutional 'black hole.' We do not need a new constitution with new emergency powers," Sullivan maintained, "We just need to make wise and vigilant use of the Constitution we've got."[355]

XII. A WORLD WITHOUT A NIDS

The spontaneity of human existence, the right to be let alone, the seclusion of privacy, and the pursuit of happiness need to be revered and preserved.[356] Most individuals move freely around their homes, offices, and places of study without considering the need for ID or that their movement might be recorded. The ease of getting a new job and flying anywhere in the United States reflect aspects of a free society. Individuals should feel free to exercise their liberty. Personhood and political identity are enhanced when ID checks are infrequent and conducted only with due process.

Persons should be free in their actions unless there is particularized probable cause or reasonable suspicion to detain or to search them or their records. Profiling, video-surveillance, facial recognition, national identification systems, and national ID cards are inherently contrary to personhood and cannot be justified on a wholesale basis. To be reasonable, intrusion must be individualized and personalized, lest personhood and identity be demeaned. Current and prospective intrusions fundamentally degrade and transform personhood within an open society. Enforcement data collection should be limited by due process to established offenders. Similarly, identification should be governed by local standards.[357] While serious problems require serious solutions, they need to be sculpted within the framework of ordered liberty.

The passage of the Privacy Act of 1974, the suspension of the unique health identifier, and the slowing of federalization of the driver's license show that the tide against a NIDS can be halted and reversed. When most people do not have to carry and show ID, the likelihood that it will be inappropriately requested is greatly reduced. When the standards of probable cause are respected before ID can be requested, the buffer around individuals is protected, the demand for

354. *See* Christopher Reed, *Are American Liberties at Risk?*, HARV. MAG., Jan.–Feb. 2002, at 100 (summarizing Kathleen Sullivan's address, War, Peace, and Civil Liberties, Tanner Lectures, Harvard University, Nov. 8, 2001).

355. *Id.*

356. *See* United States v. White, 401 U.S. 745 (1971); *see also* Robert Ellis Smith, *The True Terror Is In the Card*, N.Y. TIMES MAG., Sept. 8, 1996, at 58.

357. *E.g.*, databanks that include information limited to proven offenders minimize the reach and perils of NIDS.

ID is necessarily reduced, and criminal justice is more justly and effectively pursued.

The Supreme Court upheld this principle in *Kolender v. Lawson* in 1983.[358] 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."[359] The statute involved an inappropriate demand for identification because it circumvented the Fourth Amendment's requirement of probable cause and reasonable suspicion to search and detain a suspect.[360] 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 on the individual's credibility, such as the ability to answer questions or provide one's name and address, rather than on the nature or presence of a government-issued ID. It is essential to free movement that the police may only ask for ID when there is reasonable suspicion of criminal behavior and demand it only when there is probable cause for an arrest based on criminal activity.

Where and whether government officials can request or compel identification (including airline officials under color of governmental authority) is again an important issue today. Officers may stop an individual and request identification only under a *Terry*[361] reasonable suspicion standard.[362] An official may not compel someone to provide identification or use their authority to arrest him in an open society. The Supreme Court appropriately addressed this issue by affirming the Ninth Circuit's holding in *Kolender v. Lawson.*[363] The appellate court decision that the Supreme Court affirmed relied on the Fourth Amendment requirement for probable cause in demanding ID and arresting a plaintiff for refusal.

---

358. Kolender v. Lawson, 461 U.S. 352, 361–62 (1983).

359. *Id.* at 353–54.

360. Lawson v. Kolender, 658 F.2d 1362 (9th Cir. 1981). In a concurring opinion of *Kolender v. Lawson*, Justice William Brennan concurred that the requirement for identification violated the Fourth Amendment prohibition against unreasonable search. *Kolender v. Lawson*, 461 U.S. at 362–69. "[M]erely to facilitate the general law enforcement objectives of investigating and preventing unspecified crimes, States may not authorize the rarest and criminal prosecution of an individual for failing to produce identification or further information on demand by a police officer." *Id.* at 362.

361. 392 U.S. 1 (1968).

362. *See* Florida v. Royer, 460 U.S. 491, 498 (1983); *see also* United States v. Hensley, 469 U.S. 221, 229 (1985).

363. Kolender v. Lawson, 461 U.S. 352 (1983).

The Ninth Circuit reaffirmed *Terry* and *Kolender* in its decision in *Carey v. Nevada Gaming Control Bd.* by holding that it violates the Fourth Amendment to compel identification from an individual when the investigation does not require the individual's name.[364] The *Carey* analysis warns that under *Lawson,* compelling identification would allow the authority seeking to arrest someone to move from the well-established "probable cause" standard to the *Terry* "reasonable suspicion" standard; the lesser standard would increase the dangers inherent in a NIDS. Though other circuits split on this question, in light of the Supreme Court's affirmation, the Ninth Circuit's *Kolender* principles in *Carey* should be further persuasive.[365]

Apparently under similar standards, the FAA has only instructed the airlines to request ID to permit passengers to fly.[366] Passengers may not be forced to provide ID, and alternative procedures must be available for security, so that travelers may not be kept off planes simply for identification reasons but only for particularized suspicions of danger. The same standard for search and seizure should apply to any Transportation Security Agency identification regulations regardless of an impetus to interpret them differently. Just as the police may not coercively question citizens on the street, only reasonable questioning by trained security personnel of passengers about the purpose of their travel and their ultimate destination may be permitted. These reasonable questions may elicit indications of the need for further scrutiny, or lack thereof. The erosion of these standards by requiring identification at airports and potentially other transportation terminals suggest a fundamental erosion of personhood protections under the Constitution and steps toward an internal passport system.

The lessons of prior times may be instructive in this debate. Congress wisely decided in 1965 to abandon the plan for a National Data Center in deference to citizen and leadership opposition.[367] The 1973 HEW establishment of the Fair Information Principle requires consent to use information obtained for on purpose for different purposes.[368] The HEW Report's then rejection of the SSN as a national identifier

364. Carey v. Nev. Gaming Control Bd., 279 F.3d 873 (9th Cir. 2002).

365. The Tenth Circuit criticizes the line of reasoning by the Ninth Circuit about this issue. *See* Albright v. Rodriquez, 51 F.3d 1531, 1538 (10th Cir. 1995). This is an issue that could be attractive enough for the Supreme Court to consider soon since there is a circuit split. The circuit split emphasizes the critical importance of dealing with the NIDS system. The *Carey* decision is based on both *Lawson* and another Ninth Circuit decision, *Martinelli v. City of Beaumont*, 820 F.2d 1491 (9th Cir. 1987).

366. *See* Letter from Adm. Cathal L. Flynn, Associate Administrator for Civil Aviation Security, Federal Aviation Administration, to Robert Ellis Smith (Jan. 14, 1996) (on file with author); *see also* Civil Aviation Security, *Passenger Information* (Oct. 11, 2000), *at* http://cas.faa.gov./faq.html that ID is not required; *see also supra* notes 25–29 and accompanying text.

367. *See* GARFINKEL, *supra* note 128, at 14.

368. HEW REPORT, *supra* note 45.

also pointed the nation in the direction of privacy and protected personhood.

Similarly, adviser Martin Anderson convinced President Reagan in a 1981 cabinet meeting not to require a worker ID card. Rather than set up such an apparatus, he alerted the cabinet to a simpler and insidious solution: "All we have to do is tattoo an identification number on the inside of everybody's arm."[369] Anderson helped prevent a major step toward a NIDS. In a similar manner, in 1998, former Clinton adviser Ira Magaziner helped table the UHID plan after protests in public hearings and prominent media criticism.[370] The reasons that Senator Russell Feingold articulated against racial profiling may resonate with larger groups as time goes on: "Central to our sense of who we are is our firm belief that we are free to . . . move about as we please, free from the intrusion of the government in that movement."[371] The acts freezing funding for both the DOT federalized driver's license proposal and the UHID requirements provided examples and time for thoughtful actions and remind us even today that encroachments on fundamental rights can be stopped and reversed.[372] The polls provide evidence that a majority of citizens want to maintain their own liberty against wiretaps and Internet intrusions. Moreover, there is declining support for the idea of a national ID.[373]

Today, U.S. citizens can again assert their political identities and rights to privacy and liberty by monitoring the collection of and access to data by the government and ID requirements.[374] While recognizing the serious nature of the problems the nation faces, Americans must require their elected officials, through public and media pressure, legislation, and litigation, to find cost-effective governmental and private methods that maintain, and even enhance, civil liberties.

---

369. MARTIN ANDERSON, REVOLUTION 276 (1988).

370. *See* Ira Magaziner, Remarks at the Harvard University Third Biennial International Conference on Internet & Society (June 1, 2000); *see also* Ira Magaziner, Remarks at The Harvard Information Infrastructure Project, *Creating a Competitive Global Electronic Marketplace* (Feb. 22, 1999). Concern about the UHID plan was so widespread that Clinton tabled implementing the plan until Congress could safeguard privacy. *See* Al Gore, Remarks by the Vice President at New York University Commencement (May 14, 1998), *available at* http://clinton3.nara.gov/WH/EOP/OVP/speeches/nyu.html; *see also* Tipper Gore, *From Discovery to Recovery,* Remarks at the National Alliance for the Mentally Ill (July 16, 1998), *available at* http://clinton3.nara.gov/WH/EOP/VP_Wife/speeches/19980716.html (last visited Feb. 26, 2002); James, *supra* note 33; Stolberg, *supra* note 23.

371. 147 CONG. REC. S2270 (daily ed. March 14, 2001) (statement of Sen. Feingold).

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

373. *See supra* note 352; *see also* Leinwand, *supra* note 85.

374. *See* GARFINKEL, *supra* note 128, at 257–71.

XIII. CONSIDERATIONS AND CONCLUSIONS

The creation of a NIDS contradicts the fundamental principles of liberty, burden of proof, and federalism. When personhood depends on governmental identification systems, individuals lose both the fundamental right to political and personal identity and the buffer around them that protects them from state intrusion. The implementation of a formal NIDS, including a national ID, would erode liberty and personhood, and weakens constitutional protections against search and seizure. Databank and document requirements demean identity, personhood, and human dignity, the foundations of a free society. Even during serious and ongoing crises, these standards must guide responses if we want to retain an open society.

Federal laws and regulations that monitor citizens' lawful activities through national ID numbers, databanks, and cards increase the surveillance capacity and power of the government. The initiation by IRCA, IIRIRA, Welfare Reform Act, HIPAA, and CAPS of national databanks or national IDs as solutions for problems with illegal immigration, health costs, child support, and airline security have raised troubling prospects and questions. These databanks and others similarly devised become ineffective and overreaching reactions that degrade personhood, privacy, and liberty. Governmental actions that expand these intrusions rather than those that find rights-affirming and cost-effective alternative approaches only to extend the problem.

The increase in power that the government gets through the centralization and monitoring of personal information vastly outweighs the supposed benefits. The purported solutions via national databanks are illusory and should be abandoned in favor of fair and effective remedies that respect people's rights, identities, and personhood. A culture of freedom requires upholding rights that flow from the preservation of the nature of our Constitution. Personhood and identity can only thrive if a pervasive NIDS and the consequential degradation of political and personal identity are reversed. The genius of American democracy and republican government are based on individual sovereignty and limits on the power of the government.

The prevention of a full NIDS enhances the prospects for a society in which personhood remains fundamental, where individuals are judged on their actions, not on generalized suspicions or numerical places in databanks. A system of national identification hastens Kafkaesque or Orwellian futures by demeaning the nature of personhood that underlies basic liberties in a free society. It stands fundamentally opposed to the founding principles of the U.S. nation and government: to realize a new birth of freedom by facing contemporary challenges justly and effectively. For the benefit of the nation as a

beacon to the watching wider world, the alien notion and scheme of a national identification system must be reversed and abandoned.