UIC Law Review

Volume 21 | Issue 4 Article 5

Summer 1988

The National ID Card: Privacy Threat or Protection, 21 J. Marshall L. Rev. 831 (1988)

Elizabeth Friedheim

COMMENTS

THE NATIONAL ID CARD: PRIVACY THREAT OR PROTECTION?

Americans may begin carrying a national identification ("ID") card in the near future.[1] Most people react to the prospect within a range from horror to reluctant acceptance.[2] Detractors fear the card could strip United States residents of informational privacy.[3] Supporters believe a card could help the government fight those crimes

---

1. The Immigration Reform and Control Act of 1986, Pub. L. No. 99-603 (1986) (codified at 8 U.S.C.A. § 1324.274 (West Supp. 1988)), requires employers to verify the identity and work eligibility of all new employees. This requirement, effective June 1, 1987, puts employers in the business of evaluating identification documents. The new "Handbook for Employers," which instructs employers on how to develop proper verification records, lists 29 types of identification documents and allows for the possibility of others. 52 Fed. Reg. 21,455, 21,488 (1987) (to be codified at 8 C.F.R. § 274a). Practical necessity will create pressure for a single document. Furthermore, the Immigration Act itself authorizes feasibility studies of a single-card system. For details on the need for a single, secure card and the direction card feasibility studies will take, see *infra* notes 29-33, 43-49 and accompanying text.

2. The proposed Immigration Reform and Control Act of 1983, S.B. 529, required a national ID system to verify the status of all aliens. *See* Quade, *ID Card for All?* 69 A.B.A. J. 1370 (Oct. 1983). At that time, attorneys feared invasions of privacy because the government would create a massive data bank to verify immigrant identity. *Id.* Since other Americans would also have to prove their identity at work, the data system would include everyone. *Id.* Furthermore, the government would inevitably use the extensive system for other ID problems beyond employee verification to control immigration. *Id.* As of 1988, the United States still does not have a mandatory national ID card. The federal government does, however, use massive data banks to verify identity and document the behavior of residents. For details on the extent of the presently existing national data-bank system for identification, see *infra* notes 53-100 and accompanying text. Additionally, for an argument about how an ID card might actually help citizens regain some privacy in a world of data banks, see *infra* notes 101-120 and accompanying text.

3. If a card is tied to a system of data banks by a common identifier, then the card can become a link to any identified information in any of the banks. Numerous government and private data banks use the social security number ("SSN") for computer matches between banks. *See* Shattuck, *In the Shadow of 1984: National Identification Systems, Computer-Matching, and Privacy in the United States*, 35 HASTINGS L.J. 991 (1984). For federal purposes, computer matching often constitutes a "routine use" exception to the Privacy Act of 1974. 5 U.S.C. § 552a(b)(3) (1982). Many exchanges between private banks simply occur beyond the bounds of legal strictures. Shattuck, *supra*, at 996-97, 1003.

involving false identification.[4] Would such a tool for fighting crime be worth some loss of freedom and privacy for all Americans?[5] If asked that question, many would answer "no." This comment, however, asks a different question. Should card-carrying Americans who are already enmeshed in a complex ID system controlled by fraud, market forces, and government need,[6] exchange this system for a simpler one run by the federal government under strict legislative controls?

Both questions rest on the same assumption about informational privacy, but yield different answers because they posit different facts. Both questions assume that most Americans want to control dissemination of information about themselves.[7] In personal

---

4. The False Identification Crime Control Act of 1982 penalizes those who produce or traffic in false ID documents. Pub. L. 97-398, § 2, 96 Stat. 2009 (1982) (codified at 18 U.S.C.A. § 1028 (West Supp. 1988)). *See also False Identification: Hearings H.R. 352, H.R. 6105, H.R. 6946, and S. 2043 Before the Subcomm. on Crime of the Comm. on the Judiciary*, 97th Cong., 2d Sess. 21-89 (1982) (details techniques and types of identification fraud); J. EATON, CARD-CARRYING AMERICANS: PRIVACY, SECURITY, AND THE NATIONAL ID CARD DEBATE 74-77 (1986) (summarizes the use of false identification for immigration) [hereinafter EATON].

5. As travelers know, many governments require everyone to produce a passport when registering at a hotel. Some countries, Egypt for example, also require reports to the local police when foreigners visit private homes. MCGRATH, FROMMER'S DOLLARWISE GUIDE TO EGYPT 39 (1986).

Even a card by itself, divorced from any identifier or data-bank information, can effectively control private citizens. Pipko and Pucciarelli, *The Soviet Internal Passport System*, 19 INT'L LAW. 915 (1985). The Soviet internal passport system requires persons to request permission and get an official passport stamp (*propiska*) before changing residence. *Id.* at 917. Furthermore, all persons must carry their passports and show them on request. *Id.* at 916. Thus the internal passport alone enables the Soviet government to reward and punish people by controlling where they can live and travel. *Id.* at 916-18. *See also* T. B. SMITH, THE OTHER ESTABLISHMENT: AN IN-DEPTH STUDY OF WHAT INDIVIDUAL LIFE IS REALLY LIKE IN COMMUNIST-CONTROLLED COUNTRIES (1984) for full details on the *propiska* and other Soviet techniques for identifying and collecting data on individual citizens.

6. Americans use an elaborate ID system with numerous cards that show a person's right to drive, to borrow books, to swim in a local pool, to charge clothes, to rent a car, and to gain access to other facilities from the government and private purveyors. *See generally* EATON, *supra* note 4 (discusses the present American ID system, including its large private components). Each government agency and private company maintain records on its card holders. These records, in turn, form the data banks of information for the present national ID system. *Id.*

7. The Privacy Act of 1974, Pub. L. No. 93-579 (1974) (codified at 5 U.S.C. § 552a (1982)), embodies the idea of a closed system with maximum information privacy. In essence, the Act prohibits the federal government from disclosing information about a person without that person's consent. *Id.* § 552a(b). The operative provisions of the Privacy Act, however, are codified as part of the Freedom of Information Act ("FOIA"), *Id.* § 552, which embodies the opposite philosophy of an open system with maximum access for citizens who want information from their government. In effect, the Privacy Act forms an exception within FOIA. FOIA, in turn, is an exception to the Privacy Act that allows the government to release personal records required under FOIA without asking the person's consent. *Id.* § 552a(b)(2). Thus American law shows inherent tension between a closed system for private, personal records and an open system for government files.

matters, they prefer a closed system. If the government has personal details buried in a file, the government should release these details only with the permission of the person whom the details describe.[8] Such a closed system would not be feasible with an ID card anchored to a national data network of readily available personal information.[9] The facts, however, show that Americans already have a very open system which features numerous ID cards, free exchange of information among hundreds of data banks, and the near absence of informational privacy.[10]

This comment addresses whether Americans should modify the present free-wheeling identification system through legislated controls designed to protect informational privacy. Since the ID card would be part of the national ID system, the introduction of a card would present opportunities to impose such controls over the wider system as well. To present the legal problems involved, this comment first reviews the legal status of a possible national ID card in light of both the recent legislation for ID documents and the feasibility studies Congress has mandated to explore the possibilities of a national ID verification system.[11] This section places the future ID card within a verification system that will impinge on informational privacy. In the second section, the comment explores the extent and legal status of the present ID verification system, which is based on the social security number ("SSN") and related data banks.[12] This section exposes an open data network with weak legal controls to protect privacy. Finally, the comment suggests two models for a new

---

8. *Id.* § 552a(b).

9. The problems of preserving privacy in a world of computerized data banks has challenged both private thinkers and government task force experts. The collective wisdom of various privacy advocates includes the following principles:

1) The data subject should know whenever he or she is the subject of a data system;

2) Data should exist for a specific purpose, not simply because they might be useful at some, unspecified future time;

3) Old, incomplete, inaccurate data cause more trouble than no data at all;

4) Data subjects should not suffer the surprise of seeing data used for some new, unauthorized purpose;

5) Data need protection for accuracy and proper use; and

6) Data subjects need a chance to review and correct inaccurate data.

Trubow, *Information Law Overview*, 18 J. MARSHALL L. REV. 815, 822-23 (1985) [hereinafter *Overview*]. The principles are ideals, not descriptions of reality. The various exceptions to the Privacy Act show that statutory law approves data-matching and other disclosures that work against these principles. 5 U.S.C. § 552a(b).

10. For an overview of the ID card system in the United States, see EATON, *supra* note 4. *See also infra* notes 77-85, 97-103 and accompanying text for specific details on the American data-bank system as it is tied to personal identity.

11. For details on the national problems with illegal immigration and ID fraud as well as the various executive and legislative responses to these problems, see *infra* notes 14-52 and accompanying text.

12. For details on the present ID system and the minimal protection it provides for informational privacy, see *infra* notes 53-100 and accompanying text.

ID card system that would help the average person review and correct errors in the national data network.[13] This third section also suggests how the current system could be altered to provide the essentials for the protection of informational privacy.

I. Legislation for a National ID Card

At present, the United States Congress faces a major social problem that may require a national ID card backed by a comprehensive ID system.[14] This problem is illegal immigration[15] compli-

---

13. For two models of a national ID system that has more protections for privacy than the present system has, see *infra* notes 100-126 and accompanying text.

14. In an imaginary, fully private world, no one would learn about someone else without that person's permission. But such an imaginary, closed information system is neither possible nor socially desirable. Indeed, the truly closed system could never exist except in such bizarre situations as occur when hermits retreat into the desert or when Japanese soldiers stay hidden on islands for forty years after World War II. Even people in primitive tribes, far removed from the file drawer and computer, have little informational privacy. C. Turnbull, The Forest People 109-25, 166-83 (1962). People inside their thatched huts, for instance, know that they share their whispered secrets with anyone standing outside and play any louder activities to an audience of the entire village. *Id.* at 109-25. When these people walk outside the village to seek greater privacy, they leave a record of footprints to show where they went and body prints as evidence of any stops along the way. *See also* Gregor, *Exposure and Seclusion: A Study of Institutionalized Isolation Among the Mehinaku Indians of Brazil* 81-99 in Secrecy: a Cross-Cultural Perspective (S. Tefft ed. 1980). Thus the entire group knows who romps with whom and how often, along with any other details that could possibly interest people who love to gossip among themselves. Turnbull, *supra*, at 109-25, 180-83. In effect, everyone has a complete dossier, with intimate details, on life in the entire tribe. *Id.*

In small village or tribal groups, people know so much about each other that they can exert control over wayward members. *Id.* When someone misbehaves, everyone else gossips, teases, and threatens the deviant. *Id.* at 110-14. People usually cannot afford to cheat other members of the tribe because such wayward behavior would incur the censure of the whole group. *Id.* at 118-25.

More complex societies, like ours, offer much more privacy day-to-day. In these societies, people have doors to close. Modern society also separates work from home and allows people to move away from the small town, suburb, or neighborhood where they are known. Thus, no one person has a complete file on someone else. *See generally* J. Rule, Private Lives and Public Surveillance: Social Control In The Computer Age (1974) (details how criminal records, driver records, and credit histories help the government to control citizens and allow creditors to control borrowers in both Britain and the United States). Thus, modern people must constantly deal with strangers: they choose a doctor on the first visit; they lend money after a mere introduction; they marry after a few months of friendship. Modern governments and private information systems fulfill some of the information needs of such a society by identifying people and keeping basic information about them. *Id.*

15. No one knows how many illegal aliens now live within the United States. The Population Reference Bureau, which normally records fractional detail, estimates the illegal population at 2-12 million. Haupt, *Amnesty Day Is Coming*, 15, no. 4 Population Today 4 (Apr. 1987). The wide variation in total figures occurs because population experts must use indirect techniques to estimate the number of uncounted people within a counted population. Corwin, *The Numbers Game: Estimates of Illegal Aliens in the United States, 1970-1981*, 45 Law & Contemp. Probs. 223 (1982). For instance, experts may compare actual birth and death rates in an area to the rates that they would expect from the counted population. *Id.* at 240. In any event, as of

cated by identity fraud.[16] The important question for Congress is whether it can create a secure system to identify legal U.S. residents without eroding everyone's informational privacy.[17] In this section, the comment outlines the Congressional solution in terms of: (1) the need to verify eligibility for employment; (2) the need for ID documents; (3) problems with fraud in the ID documents; (4) the possibility of a secure ID card; and (5) the possibility of an ID verification system.

First, Congress has decided to control illegal immigration through control of the jobs that attract illegal aliens to this country.[18] Exerting this control through job applications[19] seems more effective and less intrusive than conducting periodic raids for hapless immigrant workers in the field or factory line.[20] To exercise this

---

1981, these various techniques yielded figures between 7,150,000 and 9,040,000. *Id.* at 248-49. Any modern government, even a government that maintains the world's most open immigration policy, would want to control such a massive border problem.

16. See *supra* note 4 for citations to the present federal legislation and Congressional hearings on the problem of ID fraud in the United States.

17. There are approaches to the problem of illegal immigration that do not reduce privacy for legal residents. For instance, patrolling the borders need not impinge on privacy for anyone except illegal border crossers. *See generally*, E. HULL, WITHOUT JUSTICE FOR ALL: THE CONSTITUTIONAL RIGHTS OF ALIENS 79-114 (1985) [hereinafter HULL] for the legality of the various ways that the federal government has tried to curtail illegal immigration. Each strategy, however, has problems. Controlling the borders would require that the Immigration and Naturalization Service ("INS") patrol key points along thousands of miles of border and among unnumbered airports and landing strips. Such an impossible task would invite selective enforcement. *Id.* For instance, border patrols could concentrate on the lower-class Mexicans slipping in from Tijuana or Juarez.

18. Another job-related strategy, enforcing laws for minimum wages and decent working conditions, might reduce the supply of substandard jobs that often attract illegal aliens. Schwartz, *Employer Sanction Laws, Worker Identification Systems, and Undocumented Aliens: The State Experience and Federal Proposals*, 19 STAN. J. INT'L L. 371, 391-93 (1983). Unfortunately, this enforcement strategy singles out poor illegals. *Id.* It also presupposes that some disgruntled employee will risk both job and residence in the country by reporting conditions in his labor camp or sweat shop. *Id.* Finally, enforcement of working conditions would overlook large numbers of illegals who hold standard jobs. *Id. See also*, HULL, *supra* note 17.

19. For federal laws that attempt to curtail immigration by preventing immigrants from taking jobs, see *infra* note 20.

20. Since jobs attract most immigrants, legal or illegal, catching illegal aliens on the job seems like an efficient technique for enforcing the law. *See* Schwartz, *supra* note 18, at 371-73. However, federal efforts to approach the work place directly pose the threat of violating civil rights and invading the privacy of workers. INS v. Delgado, 466 U.S. 210 (1984) (Brennan, J., dissenting) (federal authorities cannot question workers simply because these people appear to have racial or ethnic traits common among illegal aliens); Blackie's House of Beef, Inc. v. Castillo, 480 F. Supp. 1078 (D.D.C. 1979) (the INS cannot raid a work site without probable cause to search out illegal aliens).

The Farm Labor Contractor Registration Act, 7 U.S.C. § 2041 (1982) (current version at 29 U.S.C. 1801 (1982)), and the old Immigration and Nationality Act, 8 U.S.C. § 1324(a) (1982), used a less direct approach. Both laws required employers to screen illegal aliens out of the work force. The Farm Labor Act specifically required employers to review ID documents. 29 C.F.R. § 40.51 (1987). The "Texas Proviso"

necessary control, however, the government must collect some information about the identity of workers.

The New Immigration Reform and Control Act of 1986 ("Act")[21] places the burden of collecting this worker information directly on the employers. Under the Act, employers must scrutinize documents for each person hired to verify who that person is and whether he or she is authorized to work in the United States.[22] Employers who fail to keep records face civil penalties.[23] Employers who make a practice of employing one or more illegal aliens may also suffer criminal sanctions for each person employed.[24]

Second, identity documents form the linchpin of this system. At an ideal minimum for a closed information system, each worker could flash a single card with a name, picture, and the words "authorized to work in the United States." Since this minimalist card does not exist at present, workers will need to present more revealing documents such as passports, drivers licenses, and birth certificates.[25]

On March 19, 1987, the Federal Register published a prototype of "Form I-9" for employers to use when reviewing ID documents to verify employment eligibility for workers hired after November 6, 1986.[26] For this review, employers must examine either one document that shows both identity and right-to-work status or a set of documents that combine to verify identity and status.[27] For example, a citizen might present a U.S. passport, which confirms identity with a picture and confirms right-to-work status with an affirmation of U.S. citizenship. Workers who do not possess passports might

---

amendment to the Immigration Act, by contrast, excused employers from liability as long as they conducted "usual and normal practices incidental to employment." 8 U.S.C. § 1324(a) (1982). Unfortunately, neither act has had much effect. Federal prosecutions under the Farm Labor Act yielded only $241,000 in penalites during 1980 and federal prosecutions under the Texas Proviso have proved close to impossible. Schwartz, *supra* note 18, at 373-74. If the government wants to reach the illegals through their employers, it needs more explicit rules for the employers and better enforcement by the INS.

21. Pub. L. No. 99-603, 100 Stat. 3359 (1986) (to be codified at 8 U.S.C. § 1324).

22. *Id.* § 274A(b).

23. *Id.* § 274A(e).

24. *Id.* § 274A(f).

25. Acceptable ID documents fall into three categories: (1) those that identify a person with a photo, fingerprint or other unique sign; (2) those that testify to a person's authorization to work in the United States; and (3) those that do both. *Id.* § 1324. 274 A(b)(1). The new Employment Elgibility Verification Form (I-9) lists specific documents for employee IDs. 52 Fed. Reg. 8,795 (to be codified at 8 C.F.R. § 274a). Many of these documents reveal more than an employer needs to know. For example, the ID may expose the job applicant's travel experiences (visa stamps on a passport), citizenship status (various immigration documents), or driving restrictions (state driver's license).

26. 52 Fed. Reg. 8,795 (to be codified at 8 C.F.R. § 274a).

27. *Id.* at 8,762-95.

present a state ID card or driver's license which has a picture, and a social security card, which verifies the right to work.[28]

Third, all such documents are either easy to counterfeit by themselves or are dependent on breeder documents which are easy to counterfeit.[29] For example, both the U.S. Passport Office and the Social Security Administration ("SSA") prefer to issue documents based on a birth certificate, which verifies citizenship, and one ID document, which verifies identity through a picture or other distinguishing trait.[30] Unfortunately, when thousands of agencies issue birth certificates on different paper with different forms, an enterprising criminal need only manufacture an official looking certificate or request the certificate of a dead person with the right race, age, and sex.[31] The most common picture ID card, the state driver's license, also depends on questionable breeders.[32] The SSN card is

---

28. *Id.* at 8,795.

29. The credit industry pioneered the use of large data banks to check the identity of strangers. RULE, *supra* note 14, at 175-222. In effect, a major credit card is now an international ID card for credit transactions. *Id.* The cards record data on users that include not only the amount of money owed and paid but also the specific purchases made and the various places where a user travelled to make these purchases. *Id.* Thus credit companies maintain surveillance data on a large segment of the population. *Id.* Even people who do not hold major credit cards may become subjects in the credit banks. As an experiment, the comment author (who does not have major cards), tried to pay for a store purchase by check. Store personnel used the author's Illinois driver's license to verify deposits in a Chicago bank. In other words, without the consent of the data subjects, local banks and the state ID system set up data matching to verify bank accounts.

For further details on the problem of breeder documents, see J. EATON, *supra* note 4, at 38-41, 203-04. For a brief description of the ID forgery industry in the United States, see *infra* note 31 and accompanying text.

30. The "Application for a Social Security Number Card" lists the birth certificate as the "preferred document to give evidence of age and citizenship" for those born as U.S. citizens. Form SS-5 (8-85). Even so, the form allows a large number of other ID documents to give "evidence of identity." *Id.* at 1. These include: driver's licenses or state IDs, welfare ID cards, marriage records, nursery school records, vaccination certificates, and other documents that a person could forge. *Id.*

The "Passport Application" requires a "previous passport or *certified* birth certificate" as the only application document for a person born in the U.S. unless the applicant does not have a birth record. Form DSD-11 (12-85). The passport application also requires "proof of identity" in the form of a document with both a signature and a physical description or a good likeness. *Id.*

31. The forgery of ID documents is an industry in the United States and an occupational specialty for some white collar criminals. *See* EATON, *supra* note 4, at 74-77. The ideal breeder document for ID cards, the birth certificate, issues from roughly 8,000 agencies, which use a variety of forms. *Id.* Furthermore, anyone can research old obituaries and then request the birth certificate of an infant who died some time ago. *Id.* This birth certificate, in turn, can become the chief breeder for adult ID papers. *Id.* Fraudulent ID papers then serve to hide the terrorist, illegal alien, and white collar criminal.

32. Illinois, for example, provides a photocopied list of "acceptable identification" documents for driver's license applicants. J. Edgar, *Driver's License Identification* (1987) (a sheet listing ID alternatives available from license application facilities in Illinois). The list requires three documents which, between them, provide the applicant's date of birth and signature. *Id.* These documents could include: a birth cer-

even less secure than the passport and state ID. Prior to 1978, anyone could obtain the card by mail; even today, the card is printed on common paper stock that invites reproduction and forgery.[33]

Fourth, given the massive fraud problem, the government cannot rely on existing documents taken at face value. This leaves the alternatives of a tamper-proof card or documents verified against existing data bases.[34] Of these alternatives, the first would involve less intrusion on informational privacy but would still require more than a simple card with name and work status.

At a minimum, a secure ID card would need to add unique biometric indicators.[35] The technology for this now includes fingerprints, voice prints, retina prints, and much more—all machine readable with very high accuracy. In addition, a good picture with a good view of the ear, which like the fingerprint, is unique, would serve the small employer, store clerk, and border inspector who do not have ready access to advanced technology.[36]

A primitive, relatively secure ID card already exists. The Immigration and Naturalization Service ("INS") issues the Alien Documentation, Identification, and Telecommunications ("ADIT") card to alien border crossers.[37] As of February, 1985, the INS had issued 5.3 million cards; at the present rate and with present funding, the INS could issue enough cards to identify the legal migrants currently arriving.[38] A similar card could authenticate the identity of long-term alien residents and U.S. citizens.

The Immigration Act, however, does not authorize such a single card or document with minimal information. Instead, it assures Americans that: "[n]othing in this section shall be construed to authorize, directly or indirectly, the issuance or use of a national iden-

---

tificate, which is easy to counterfeit; a health club ID; and a recent utility bill. *Id.*

33. *See* EATON, *supra* note 4, at 77-82 for a discussion about the lack of security in the current ID system.

34. Verifying documents against existing data bases would be easier because it would use the system already in place. On the other hand, a data-verification system would perpetuate the privacy invasions that now exist. *See generally* Shattuck, *supra* note 3 for a discussion of computer matching as a threat to informational privacy.

35. Because people can steal cards, each card must contain some way to prove that the card belongs to the person holding it. *See* EATON, *supra* note 4, at 4-7.

36. The technology for plastic ID cards has become very sophisticated. EATON, *supra* note 4, at 4-7, 166-68. Cards can record fingerprints and other unique traits. *Id.* In general, the technology can produce a sophisticated ("smart") card that will electronically verify whether the card holder is really the person he or she claims to be and whether the person is entitled to work in the United States or receive any particular benefit. *Id.* If such a card also contained the SSN, it would give people access to more detailed information about the card holder. *See also infra* note 71 for information about machine readable data on an ID card.

37. The INS can issue a long-term "border crossing identification card" to alien residents who cross the international border. 8 U.S.C. § 1101(a)(6) (1982).

38. *See* EATON, *supra* note 4, at 44-48.

tification card."[39] On the other hand, the Act does authorize the President to monitor the ID system and suggest "major changes" for Congressional review.[40] Furthermore, the Act anticipates that a possible major change might be "a new card or other document" for worker verification.[41]

Fifth, the prospective card might prove far less intrusive than other current proposals for an ID verification system.[42] In the Immigration Reform and Control Act of 1986,[43] Congress mandated two feasibility studies:

1) By April, 1989, the Attorney General must study and report on a phone system to verify alien ID cards against federal data banks.[44] This system could be run by either the federal government or a private contractor.[45] It should, of course, conform to guidelines in the Privacy Act of 1974.[46]

2) By November, 1989, the Comptroller General must report on technological alternatives for a tamper-proof social security card to replace the present, easily counterfeited cardboard card.[47]

In addition, the Comprehensive Crime Control Act of 1984[48] required the President to recommend legislation for federal systems to curb ID fraud with features such as: (1) protections for privacy; (2) civil and criminal sanctions for ID fraud; and (3) provisions for the exchange of personal ID information as authorized by federal or state legislation or by executive order.[49] Clearly, Congress expects a report that uses present data banks to verify IDs.

If these studies indicate the course Congress intends to take, then the SSN will assume new importance. The SSN card could become the new, tamper-proof national ID card. The SSN itself would then link the card to verifying data bases. The present card—supplemented with an ear picture, fingerprint, and the words "authorized to work," placed on unique paper stock with the latest in circuit chips, magnetic strips, and plastic protection—would serve the government's needs very well.[50]

---

39. Pub. L. No. 99-603 (1986) (codifed at 8 U.S.C.A. § 1324. 27A(a)(c) (West Supp. 1988)).
40. *Id.* § 1324.274A(a)(d).
41. *Id.* §1324.274A(a)(d)(3)(D).
42. *See* Shattuck, *supra* note 3, for a discussion of government surveillance possible through the use of ID numbers with computer matching between data banks.
43. Pub. L. No. 99-603 (1986) (to be codified at 8 U.S.C. § 1324.274).
44. *Id.* § 1324.274A(a)(d).
45. *Id.*
46. *Id.*
47. *Id.* § 1324.274A(e).
48. 18 U.S.C.A. § 1028 (West Supp. 1988).
49. *Id.*
50. For comments on ID card technology, see *supra* note 36 and *infra* note 71.

In short, the new Immigration Act will force Congress to chose from three alternatives. One, Congress can allow the employer to make private judgments about accepting present ID documents on their face. Two, it can create a national ID card with the necessary information. Three, it can establish a secure ID system by allowing employers to verify ID documents through the use of the SSN (or some other impersonal identifier) against personal information in large data banks.

This last solution, the apparent Congressional favorite, poses a grave threat to informational privacy. The SSN links together hundreds of data banks.[51] Any ID document bearing that number would provide the key for locating personal information in many of these banks.[52] Even worse, this threat is a present reality; the card, the number, and a massive network of data banks exist today. Consideration of a national ID card and its impact on privacy must take the entire ID system into account.

II. Legal Controls Over the National ID System

In other words, a national ID system is now in place. The system has grown piece-by-piece over time. Even the one component that does not exist today—the single, required ID card—has appeared in local form.[53] As the system developed, so too did legal controls to affect informational privacy. The question now is whether the legal protections that developed one at a time add up to an adequate safeguard for informational privacy in a comprehensive ID system.

In this section, the comment reviews system components and legal controls for: (1) the card itself; (2) information directly associated with the card; (3) the SSN requirement; (4) the use of the SSN in federal data banks; (5) the spread of the SSN to state and private banks; (6) the practice of file matching between identified banks; and (7) the extensive public and private data network linked to each identified person through his or her SSN.

First, the card itself could become an excuse for police searches of any person who does not have his or her card at hand.[54] An example of such card use occurs in the Soviet Union where one card serves all official ID purposes and loss of that card puts the citizen

---

51. For information about the extensive use of the SSN in various data banks, see *infra* notes 80-85 and accompanying text.

52. For details on the SSN identification system as a threat to informational privacy, see *infra* notes 86-96 and accompanying text.

53. For the story of one community's use of an ID card for local workers, see *infra* note 59.

54. The fourth amendment prohibits "unreasonable searches and seizures." U.S. Const. amend. IV.

at risk.[55] In the United States, police can frisk any suspicious person who fails to identify himself properly.[56] If the national ID card becomes the only proper identification, then loss of the card would leave anyone stopped by the police vulnerable to an extensive personal search.[57] The Constitution, as presently interpreted, would also allow the government to use information found during such a search in a criminal prosecution against the search victim.[58]

Fortunately, even the present Supreme Court has ruled against search procedures that can routinely affect the ordinary citizen.[59]

---

55. For citations to sources that detail how some governments use the ID card to control the movements of citizens and travellers, see *supra* note 5.

56. Terry v. Ohio, 392 U.S. 1 (1968).

57. W. LAFAVE, 3 SEARCH AND SEIZURE §§ 9.1-.6 (1978 & Supp. 1985) (details the development of the *Terry* search with numerous citations).

58. The chief remedy for an illicit seizure, excluding seized evidence from the government's case-in-chief, is a remedy for criminals during prosecution. Weeks v. United States, 232 U.S. 383 (1914). The remedy applies to the actions of state officials as well as federal ones. *See* Ker v. California, 374 U.S. 23 (1963) (the fourteenth amendment includes the fourth amendment by incorporation); Mapp v. Ohio, 367 U.S. 643 (1961) (people can exclude illicitly seized evidence from the state's case-in-chief). A principal effect of this remedy, however, is that courts now protect fourth amendment rights by freeing guilty criminals. In recent years, the Supreme Court has chosen to counter this effect by finding ever more exceptions to the exclusionary rule. *See generally* Wasserstrom, *The Incredible Shrinking Fourth Amendment*, 21 AM. CRIM. L. REV. 257 (1984) (details the decline of the fourth amendment as the Court finds exceptions to the exclusionary rule).

Unfortunately, law has not provided other effective remedies to secure fourth amendment rights. In theory, a victim can bring a tort action under state common law and several federal causes of action. *See* Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388 (1971) (a constitutional tort against federal officials); Federal Torts Claim Act 28 U.S.C. § 2680(h) (1982) (a federal cause of action); 42 U.S.C. § 1983 (1982) (a federal cause of action against state officials). In practice, these remedies bring little relief to a victim who must often prove malice before shaking damages out of the shallow pockets of some policeman. *See* J. HIRSCHEL, FOURTH AMENDMENT RIGHTS 9-13 (1979).

59. Recent Supreme Court criminal decisions show the Court's attempts to protect the privacy rights of noncriminals. *See* O'Neill, *The Good, the Bad, and the Burger Court: Victims' Rights and a New Model of Criminal Review*, 75 J. AM. CRIM. L. & CRIMINOLOGY 363 (1984). For example, the Court has limited airport searches, which might affect the frequent flyer as well as the drug smuggler. United States v. Place, 462 U.S. 696 (1983).

The same respect for the law abiding citizen could limit the use of ID cards as an excuse for a search. For instance, the municipal ID ordinance in Palm Beach, Florida, required ID cards for local employees and allowed police searches for workers who could not produce the official card when asked. *See* Frank, *"Doonsbury"? Palm Beach Law Draws Fire*, 72 A.B.A. J. 27 (Jan. 1986). The local ACLU alleged that the ordinance presented several legal problems including: (1) an impermissible barrier to interstate commerce; (2) an unreasonable seizure of persons; (3) a violation of due process; (4) a violation of equal protection; and (5) an undue burden on blue-collar workers. *Id.* In 1985, the district court for the Sourthern District of Florida ruled against the ordinance as a violation of the commerce clause. Wallace v. Town of Palm Beach, 83-8268. *See* Frank, *Worker's I.D's "Pass Law" Struck Down*, 72 A.B.A. J. 22 (Mar. 1986) [hereinafter *Worker's I.D.'s*]. Later the eleventh circuit appellate court dismissed the case in a *per curiam* opinion because state legislation had eliminated the ordinance which was the subject of the suit. Wallace v. Town of Palm Beach, 809 F.2d 1525 (11th Cir. 1987).

For instance, in *Brown v. Texas*[60] the Supreme Court ruled that police may not ask a person for identification unless they already have some reasonable suspicion about that person's actions.[61]

Second, once an ID card exists, the card itself or the form used to apply for the card can expose private information. Plaintiffs in *Wallace v. Palm Beach*[62] and *Service Machine & Shipbuilding Corp. v. Edwards*[63] raised the issue of whether information required by local law for workers' ID cards violated informational privacy.[64] Instead of dealing with the privacy issue, the courts ruled that these local ID ordinances restricted the free movement of workers and, thus, presented impermissible barriers under the commerce clause.[65] Plaintiffs in *Doe v. Louisiana*[66] challenged racial identification on Louisiana birth records as a violation of equal protection.[67] The *Doe* court did address the privacy issue and ruled against the plaintiffs and in favor of the government's interest in accurate demographic statistics.[68]

These three cases on ID documents show that courts do not perceive ID documents *per se* as part of a privacy problem. The *Doe* court supported a governmental interest in collecting private information.[69] Although the *Wallace* and *Service Machine* courts found for the plaintiffs, they did so under the commerce clause, an approach which cannot be used to challenge the federal government in its future use of a worker's ID card.[70]

The national ID, in contrast to the Palm Beach card, would cover the entire country and apply to everyone. Thus it would not present problems under the commence clause. *See* U.S. CONST. art. I, § 8.

60. 443 U.S. 47 (1979).

61. *Id.*

62. The Palm Beach worker's ID card asked for race, occupation, employer, height, weight, birthplace, and next of kin, among other items that a person might not want to reveal. *See Worker I.D.'s, supra* note 59. For details about the case, see also *supra* note 59.

63. 617 F.2d 70 (5th Cir.), *aff'd*, 449 U.S. 913 (1980).

64. For some information required on the Palm Beach card, see *supra* note 62. A full list of information required on the *Service Machine* card appears in Service Machine & Shipbuilding Corp. v. Edwards, 466 F. Supp. 1200, 1211-12 (W.D. La. 1979); *see also* Note, *Constitutional Law—Workers' Identification Program Violates Commerce Clause*, 55 TUL. L. REV. 950 (1981).

65. 617 F.2d at 74-76.

66. Doe v. State Dept. of Health and Human Resources, 479 So. 2d 369 (La. Ct. App. 1985).

67. *Id.*

68. *Id.* at 374. *See also* Diamond and Control, *Codifying Caste: Louisiana's Racial Classification Scheme and the Fourteenth Amendment*, 29 LOY. L. REV. 255 (1983) (analyzes birth certificates as part of the racial caste system that developed in Louisiana after Reconstruction).

69. For Supreme Court views on the government's right to collect information about individuals, see *infra* notes 88-92 and accompanying text.

70. The Constitution gives Congress the right both to "regulate Commerce" and to "establish a uniform Rule of Naturalization." U.S. CONST. art. I, § 8.

Third, any national ID card would need some unique personal identifier,[71] like the SSN. Some people, however, object to numbers like the SSN on religious grounds.[72] In *Roy v. Cohen*[73] a district court held that parents could refuse a SSN number for their child and still collect welfare benefits if the parents based their refusal on a sincerely held religious belief.[74] The appellate court examined the Roy family's native American religion both for a history of sincere family practice and for doctrinal detail on the subject of evil numbers.[75] Nonetheless, the Supreme Court reversed on the grounds that religious belief, however sincere, does not give an individual the right to "dictate the conduct of the government's internal procedures."[76] This decision clearly does not promise any escape from the SSN for true believers in privacy.

Fourth, the SSN identifier now ties individual people to a huge number of data banks in federal archives. Originally, the SSN identified people for the Social Security Administration.[77] During a working lifetime, a person would use the number for making deposits to the system.[78] Hence, working people had no reason to falsify numbers. They also had no reason to fear for their privacy because the SSN file contained only wage data that could support a claim for benefits.[79] The use of the SSN has expanded greatly since then. At present, the federal government alone maintains more than 856 personal data banks with over four billion computerized records, or

---

71. The proposals for a national ID card assume a problem with verifying identities. EATON, *supra* note 4, at 4-7. Why use a card if people will properly identify themselves? For this reason, the ID card needs an identifier that confirms the identity of one person who is entitled to carry the card. *Id.* The biometric identifiers, for instance fingerprints, serve to verify that the card holder is the person named on the card. *Id.* In addition, the card could contain a small amount of visible information or many pages of data in machine readable form. *Id.* Such a card, however, could reveal all its information to anyone who borrowed it or stole it or used it to verify any single item. It would also contain outdated information unless the card holder updated it constantly.

The usual approach to ID information involves a unique numeric identifier that can locate relevant personal data stored in a data bank somewhere else. The federal government uses the SSN identifier to locate information both in its own banks and in private records. *See generally*, Comment, *Conceputalizing National Identification: Informational Privacy Rights Protected*, 19 J. MARSHALL L. REV. 1007 (1986) (details the need for an identifier and how law can safeguard some informational privacy attached to identifiers).

72. This is a constitional objection based on freedom of religion. U.S. CONST., amend I. Illinois, for instance, recognizes this objection in statutory law and excuses persons with verifiable religious objections from submitting the SSN in their application for a state driver's license or ID card. ILL. REV. STAT. ch. 95 ½, ¶ 6-106(b) (1987).

73. 590 F. Supp. 606 (M.D. Pa. 1984), *rev'd*, Bowen v. Roy, 476 U.S. 693 (1986).

74. 590 F. Supp. at 614-15.

75. *Id.* at 604-05.

76. *Bowen*, 476 U.S. at 693.

77. 20 C.F.R. § 422.103 (1987).

78. *Id.*

79. A. ALTMEYER, THE FORMATIVE YEARS IN SOCIAL SECURITY 70 (1966).

about seventeen files for each resident—and it uses the SSN as the identifier to retrieve these records.[80] Among other uses, the federal government itself has authorized or required the SSN identifier on records for federal employees, taxpayers, money depositors, welfare recipients, drivers, and deviants.[81]

Fifth, federal use of the national identifier would be problem enough; but this extensive federal use has turned the SSN into a common identifier even in private data banks. Employers, money lenders, agencies that receive federal funds or dispense them and all

---

80. *See* D. BURNHAM, THE RISE OF THE COMPUTER STATE 51-52 (1983); EATON, *supra* note 4, at 84-87.

81. Many authorized uses for the SSN developed over the years. These include:
— 1943: The President authorized all federal agencies to use the same number (Executive Order 9379);
— 1961: Civil Service began to use the SSN for all federal employees;
— 1961: the Internal Revenue Service began using the SSN as the taxpayer ID number;
— 1963: the Treasury Department used the SSN to register U.S. securities other than savings bonds;
— 1964: the Treasury Department required SSNs from buyers of series H bonds;
— 1964: the Social Security Administration issued SSNs to 9th grade students if requested by a school;
— 1965: the SSA used SSNs to administer state old age assistance programs;
— 1965: Congress required SSNs for medicare clients;
— 1965: the Civil Service Commission used SSNs for annuitant programs;
— 1966: the Veterans Administration used SSNs for hospital admission and record keeping;
— 1967: the Department of Defense established the SSN as the service number for military personnel;
— 1970: the Treasury Department required banks, savings and loan companies, labor unions, and brokers to get SSNs from customers;
— 1972: Congress encouraged all recipients of federally funded benefits to provide their SSNs; and
— 1973: the Treasury Department required SSNs from buyers of series E bonds.
See EATON, *supra* note 4, at 77-84; R.E. SMITH, REPORT ON THE COLLECTION AND USE OF SOCIAL SECURITY NUMBERS 8, 15-17 (1985) [hereinafter REPORT].

In the Privacy Act of 1974, Congress recognized the growing use of the SSN as a threat to privacy. 5 U.S.C. § 552a (1982). The Act specifically allows people to withhold this number when they apply for benefits from the federal, state, or local government unless the SSN is required by federal statute or was already required prior to January 1, 1975. *Id.* In other words, this Act, grandfathered in the existing SSN uses. Then Congress and federal agencies added more:
— 1974: Congress required SSNs for recipients of Aid to Families with Dependent Children (AFDC) funds;
— 1976: Congress authorized states to use SSNs for taxes, welfare, driver's licenses, and motor vehicle registration;
— 1980: the Selective Service System required the SSN as an ID number for draft registration;
— 1986: Congress required all taxpayers claiming dependents age five or older to identify the dependent with a SSN. Pub. L. 99-514 § 1524 (to be codified at 26 U.S.C. § 1609);
— 1986: Congress authorized the INS to use SSNs for identifying aliens entitled to employment. Pub. L. 99-603 (to be codified amending 8 U.S.C. § 1324.274A).
See EATON, *supra* note 4, at 77-84; REPORT *supra*, at 8, 15-17 and the specific sources cited.

report to the federal government using the SSN.[82] Once the SSN penetrates a private data system, it infects other uses as well.[83] What is even worse is that the SSN data system lacks any central control. Data accumulates as credit bureaus, insurance companies, police departments, and others file information.[84] Data subjects have no easy routines for finding out what information exists, whether it is accurate, or who has been perusing the files.[85]

Sixth, these various data banks exist in an era of rapidly growing computer technology[86] and relatively weak legal controls on the free exchange of information. The Supreme Court has reviewed governmental data collection in terms of the fourth and fifth amendments.[87] In effect, the constitutional protections for informational privacy are protections from criminal prosecution.[88] Furthermore, state and federal officials may peruse private data banks either to confirm the suspected criminal activity of a specific individual or to search for possible criminality by some unknown person, somewhere in a group.[89] The Supreme Court also allows the press and public to

---

82. *See supra* note 81.

83. Health agencies, for example, need the SSN to use medicare and other federal funding. *See supra* note 81. Recently, the health industry organized the National Electronic Information Corporation ("NEIC"), which uses the SSN to track claims on patients by doctors and hospitals. *See* REPORT, *supra* note 81, at 18.

84. For instance, large private industries have grown to report on the fiscal stability of credit applicants and to issue credit cards. RULE, *supra* note 14, at 175-268. Both activities depend on masses of data about each individual. Small pieces of data, unimportant in themselves, form statistical profiles of creditworthy or unacceptable applicants. *Id.* These profiles form the basis of discrimination. *Id.* at 352-58. Credit companies exclude people with bad-risk profiles even if the individuals have proved trustworthy in the past. *Id.* Of course one could argue that without these profiles creditors would probably make such judgments on a single trait like race, age, or marital status. For a description of the national network of data banks which all use the SSN, see *infra* notes 97-100 and accompanying text.

85. The *Privacy Journal* and the Social Security Complaint Office both collect stories from outraged people who thought they had exclusive use of their own SSN. *See* REPORT, *supra* note 81, at 3-7. Illegal aliens borrow a number to seek work or to collect benefits. *Id.* at 3. Criminals file under other people's numbers to collect tax refunds. *Id.* Employers submit the number to run credit checks on job applicants. *Id.* at 5. Shops use it to verify the existence of bank accounts when people cash checks. *See supra* note 29 for a personal experience involving the author.

86. Computer technology has allowed easy exchange of data between banks. Technology has transformed a laborious paper-shuffling exercise for extraordinary circumstances into a simple process for routine review of all files. *See* Shattuck, *supra* note 3.

87. *See* J. NOVAK, R. ROTUNDA, & J. N. YOUNG, CONSTITUTIONAL LAW 716-17 (3d ed. 1986).

88. For comments on the relation between protecting criminals and protecting informational privacy, see *supra* notes 54-61 and accompanying text.

89. The Supreme Court ruled that government agents may retrieve personal information from bank records. United States v. Miller, 425 U.S. 435 (1976). In his dissent, Justice Brennan stated that bank depositors had a "reasonable expectation of privacy." *Id.* at 448. Unfortunately, such expectations will become less and less "reasonable" as government and private agents use the SSN for data matching from someone's ID. The same year, the Court allowed the IRS to retrieve tax data from an

access and use governmental files under both the first amendment and the Freedom of Information Act.[90] In general, the Supreme Court leaves the protection of privacy to tort law[91] or to the safeguards provided by federal statute.[92]

Unfortunately, even the federal statute specifically designed for that purpose does not provide overall privacy protections. The Privacy Act of 1974, enacted to close the federal data system and restrict disclosures of federal files, permits all federal government agencies to share files for many reasons.[93] For instance, the disclosure exceptions in the Privacy Act open SSA files to other federal agencies, local governments, and any members of Congress with curiosity.[94] The SSA routinely uses the SSN to run computer matches

---

attorney's client files. Fisher v. United States, 425 U.S. 391 (1976). Later, the Court allowed state requests for the computerized records of medical patients who used certain controlled drugs under a doctor's prescription. Whalen v. Roe, 429 U.S. 589 (1977). The Court ruled that New York's interest in tracking possible drug abusers outweighed any privacy rights or expectations of patients under a doctor's care. *Id.* at 597-600. All three cases recognized privacy rights for people whose files existed in private data banks. In each case, however, the Court found that the government's interest in data was more compelling than the data subject's right to privacy. *See also* Seng, *The Constitution and Informational Privacy, or How So-Called Conservatives Countenance Governmental Intrusion into a Person's Private Affairs*, 18 J. MARSHALL L. REV. 871 (1985).

90. *See* R. ROTUNDA, J. NOVAK, & J. N. YOUNG, 2 TREATISE ON CONSTITUTIONAL LAW: SUBSTANCE AND PROCEDURE § 18.30(b) (1986) (reviews case law about the accumulation and distribution of data concerning individual citizens).

91. *See* M. POLELLE & B. OTTLEY, ILLINOIS TORT LAW 196-99 (1985) (illustrates the wide latitude that case law in one state allows for state and local government in privacy disputes); L. TRIBE, AMERICAN CONSITUTIONAL LAW § 15-17 (1978) (discusses the Supreme Court reviews of privacy in records and reputation).

92. The *Miller* decision, 425 U.S. at 435, aroused legislative action in the Right to Financial Privacy Act of 1978. 12 U.S.C. § 3401 (1982). Apparently Congress believed that bank depositors should be able to keep a few secrets from the federal government. *Overview*, *supra* note 9, at 825. Nonetheless, data subjects must assume that courts will allow private data banks to crossmatch with government data banks whenever the government can rationalize a need to know.

93. 5 U.S.C. § 552a(b) (1982). Although the Privacy Act sets a policy of nondisclosure, exceptions vitiate the Act so thoroughly that commentators argue that the Act provides almost no protection at all. *See* Ehlke, *The Privacy Act After a Decade*, 18 J. MARSHALL L. REV. 829 (1985); *see also supra* note 7 for a discussion of the relationship between the Privacy Act and the FOIA.

94. First, the present federal regulations allow the SSA to disclose its data for several reasons, including:

1) crosschecking Department of Health and Human Services files;

2) submitting data as mandated by law to other government groups;

3) answering questions submitted under the Freedom of Information Act (FOIA);

4) helping other programs with "compatible" functions or purposes; and

5) promoting health, safety, and law enforcement.

20 C.F.R. § 401 (1987). These disclosures have to balance factors like the "public interest" in exposing data against the "rights and expectations of individuals" in having personal data kept confidential. *Id.* § 401.300.

In compliance with the Privacy Act, the SSA printed a form that lists specific instances when the SSA can release personal data, to whom it can make these disclo-

with state and federal files in order to uncover welfare fraud, tax evasion, and other irregular activities among the citizenry.[95]

If most citizens favor a closed data system, Congress might want to repeal the last half-century of data use. If, however, most Americans favor the war against fraud, good use of the tax dollar, and government benefits for citizens, then the federal government needs an open information system complete with data matching to compare private files.[96]

Seventh, components of the present information system—the SSN identifer; federal, state, and private data banks; and the practice of data matching—form a national data network with private information. In April, 1984, Robert Ellis Smith presented this system as a chart in his testimony to the House Judicial Subcommittee on Courts, Civil Liberties, and the Administration of Justice.[97] The chart pictured a network with twenty-nine types of banks.[98] These represented thousands of data sites, including payroll offices, school register offices, police departments and many others.[99] As a whole, the chart outlined a national network of data banks, linked by the SSN and ready to ship personal data from site to site.[100]

---

sures, and under what authority. SSA-5000 (1975). The form lists 36 types of privacy exceptions. *Id.* Some of these many disclosures seem specific and innocuous, like releasing records of deceased veterans to the VA so that soldiers' widows can get their benefits. *Id.* at no. B.1. Other exceptions seem far more dangerous to privacy: releasing data about someone who is "amnesiac, mentally incompetent or unconscious;" informing local agencies about "legally reportable" medical conditions; and telling members of Congress about "matters within their jurisdiction." *Id.* at nos. B.10, B.3, and B.11. In effect, the 36 types of permitted disclosures, grandfathered in under the Privacy Act, allow the SSA to tell all.

95. At present the SSA routinely matches data with state and federal agencies in at least five major instances. Smith, *Social Security Information* 11 PRIVACY J. 6 (1985). The SSA verifies SSNs and federal benefits for 37 states that are policing their own welfare recipients. *Id.* The SSA reports to the IRS weekly about name changes, corrections, and deletions of taxpayers. *Id.* The SSA also tells Selective Service semi-annually about the SSN and birth date of draft-age males. *Id.* In addition, the SSA informs the INS yearly about aliens who have earned incomes without work authorization. *Id.* Finally, the SSA transmits data to the Secret Service and FBI whenever these agencies want to investigate threats to national security or federal officialdom. *Id.*

96. For example, the Veteran's Administration ("VA") uses matching programs extensively. REPORT, *supra* note 81, at 21. One program matched the SSN of known dead persons with the SSN of VA beneficiaries and yielded 1500 matches or "hits." *Id.* Further investigation, however, revealed that 80% of the hits were widows who, incorrectly, used their deceased husbands' numbers when collecting widows' benefits. *Id.* This example reveals both the power of computer matching and the possibility of error. Nonetheless, even with the high error rate, the VA discovered 300 cases of fraud with one computer match. Clearly, computer matching saves the taxpayers' money.

97. Smith & McCarthy, *Data-Bank Chart, (#2),* 10 PRIVACY J. 5 (1984), *reprinted in* REPORT, *supra* note 81, at 13.

98. *Id.*

99. *Id.*

100. *See* REPORT, *supra* note 81, at 11-21 for a description of SSN data net-

A new chart rearranged from the data victim's point of view would show that each person identified by SSN is linked to an unknown number of data sites among the twenty-nine types of banks. This chart would reveal the key policy problem that the United States faces in any planning for a national system of personal identification. The SSN is a promiscuous personal identifier which has been having intercourse with every data bank within reach and which has infected all Americans with an incurable invasion of privacy. Americans all have informational herpes. Any policy concerning ID cards and identifiers should consider this infection. At the very least, new law should not make the privacy condition worse. At best, legislators might devise policies to control outbreaks within tolerable levels.

III. Toward a National ID Policy

The most immediate need for an ID card comes from the need to control immigration. Even though the new Immigration Act does not authorize a national ID card, it may require one as a passport to work in the United States.[101] However, none of the present cards would serve as an ideal passport due to the massive amount of fraud and forgery involving IDs.[102] A useful card would also require some data backup that could be tied to the card by a unique personal identifier.[103] The SSN already serves this purpose far too well. It ties the individual to numerous ID cards and unnumbered data banks.[104]

Planners, then, face two essential choices. They can tinker with some variant of the present ID system, complete with its endemic fraud and privacy invasion. Alternatively, they can outline principles, construct parts of a more protective ID system, and try to pro-

---

works, the types of banks involved, the kinds of information held in the banks, and the mode of transmission between banks.

101. *See supra* note 1 for statutes and regulations that appear to require a national ID card.

102. In addition to fraud and forgery problems committed within the United States, a new ID system will have to control fraud that occurs before a card holder enters this country. *See* Fedorenko v. United States, 449 U.S. 490 (1981) (use of a "material" failure to disclose facts when applying for a visa application); Note, *Fedorenko v. United States: A New Test for Misrepresntation in Visa Applications*, 7 N.C.J. Int'l L. & Com. Reg. 129 (1982) (the *Fedorenko* Court left the standard for "material" misrepresentation unclear). *See also* United States v. Dangdee, 616 F.2d 1118 (9th Cir. 1980) (the statute against forging U.S. entry documents also applies to foreign documents that support entry into the U.S.); Note, *Forgery of United States and Foreign Passports Prohibited by 18 U.S.C. 1543, United States v. Dangdee, 616 F.2d 1118 (9th Cir. 1980)*, 5 Suffolk Transnat'l L.J. 273 (1981) (policy would form a firmer base for the *Dangdee* decision than statutory construction because the statute is silent on its application to foreign documents).

103. *See supra* note 71 for the minimum essentials of an ID card.

104. *See supra* notes 97-100 and accompanying text for details of the relationship between the SSN and the national data-bank system.

mote its more protective features. This section will cite some privacy principles and then suggest two models for an improved ID system—one based on a new administrative structure and the other based on a new data bank coupled with new legal requirements for protecting informational privacy.

Any model rooted in the principle of a fully closed data system with maximum informational privacy, would require a card with only a name, side picture,[105] and numeric identifer. To verify the card, the system would include a file which contained only information like "born a citizen" or "naturalized in 1978." The official national ID card itself would be very closed and very protective, but the unofficial and very open system would continue with all of its present dangers to privacy. Fortunately, the prospect of a new ID card provides a chance to plan an official system that helps protect card holders from the unofficial one.

This official system should follow principles set by privacy advocates for protecting privacy in a world of open data networks:[106]

1) Maintain no secret files;

2) Collect only data needed for authorized purposes;

3) Use data for the authorized purpose only;

4) Change data to keep them accurate, timely, and complete;

5) Safeguard the integrity of data against inaccurate and unauthorized uses; and

6) Allow data subjects the right of access to review data for accuracy.

This comment suggests two possible models for a national ID system rooted in these principles: first, the *Data-Czar* system, a centralized national data bank designed to follow all six privacy principles; and second, the *Alert-Citizen* system, the present open system redesigned to follow principles one and six. Both models assume that Americans must protect their informational privacy through legislation rather than through reliance on the Constitution and the Supreme Court.[107]

The *Data-Czar* model would feature high-tech ID cards, easy routines for access by data subjects, and a centralized federal data

105. *See supra* notes 36 and 71 for biometric indicators used in machine reading and used in visual inspection.

106. *See Overview, supra* note 9 for comments on the minimum requirements to protect privacy in data banks.

107. *See supra* notes 89 and 92 and accompanying text for a discussion of the Supreme Court position on informational privacy. Since the mid 1970's, the Court has become more conservative, more likely to favor the government's of interest in information over the data subject's right to privacy from federal intrusion. *See,* Smith, *Rehnquist on Privacy,* 12 PRIVACY J. (1986).

bank.[108] The ID card would control access from outside the government. A Czar would oversee the system and propose technical and bureaucratic improvements. The central bank would combine the more than 800 existing federal data banks.

Under this system, the central bank would supply data for government use only on the condition that the request came from an authorized source and asked for specifically authorized information. For example, under the *Czar* system, the SSA could not simply crossmatch data with every welfare system in the country.[109] If the SSA wanted to share data with local welfare programs, it would need to get specific approval first.[110] The type of use would be a matter of record in a person's file before it occurred.[111]

Requests from outside the government would require authorization from the data subject and use of the subject's ID card.[112] The card would contain some biometric coding so that only the cardowner could use it. The same high-tech card could also contain an invisible numeric code that would link with the central bank. Then if lenders, employers, doctors, or others wanted information, they would have to ask the cardholder to request the specific information for them.

The cardholder should also be able to request a personal data-use profile. This profile should include a list of all data sources and data requests involving the cardholder's file. If this profile revealed a surprise—perhaps CIA data going back to 1970,[113] or some other anomaly—the data subject should be able to correct the error.

A *Czar* system would contain several protective features lacking under the present uncontrolled ID system: a secure card; government data use limited to specific purposes; non-government use limited to requests by the cardholder; and—most importantly—a practical way for the card holder to know and correct personal data in the far reaches of the central bank.

Unfortunately, the system would also introduce new threats to

---

108. Comments by G. Trubow, Information Law and Policy Seminar at the John Marshall Law School (March 31, 1987).

109. For a list of current SSA matching routines, see *supra* note 95.

110. Unfortunately, the various exceptions to the Privacy Act allow crossmatching as a form of "routine use" which does not require specific approval. 5 U.S.C. § 552a(b)(3) (1982).

111. *See generally* Ehlke, *supra* note 93 for a discussion of the lack of privacy under the Privacy Act.

112. Privacy advocates do not like the surprise revelations that often occur when data collected for one purpose is used somewhere else. *See Overview, supra* note 9, at 823. The present national data-bank system provides ample opportunity for such unpleasant surprises. *See* REPORT *supra* note 81, at 11-21.

113. For instance, for years the CIA maintained a secret file on journalist Penn Kimball because his wife, a real estate agent, had once sold a house to some people the CIA was tracking at the time. *The Secret File*, FRONTLINE (Apr. 14, 1987).

privacy. A data Czar could become a surveillance expert. After the system is in place, Congress could change the rules,[114] once again eroding protection through exception. The system might not be truly secure unless it rested on constitutional protection, as the Census Bureau does.[115] On the other hand, seeking a constitutional amendment for a data bureau would arouse the dangers of wider constitutional change.

The *Alert-Citizen* model would provide less privacy protection but at less risk. If Congress places a tamper-proof SSN card into the present ID system, it could also add one more data bank to the federal roster. This bank could list all government files for each cardholder, record all requests for data, log in new information, and provide a data-use profile at the cardholder's request.

The new data bank could require the federal government to list all of its data activity on a person in one place. The central listing would safeguard the minimum privacy essentials of an information system: no secret data banks and some easy methods for the data subject to access and correct errors in whatever data exists.[116] The new data bank would, at least, help data subjects find and police their own files.[117]

Eventually the *Alert-Citizen* system might evolve into a more protective one. As people review their own data profiles, they might become more aware of just how much data the government records and how far the public record travels along the private data network. This knowledge might inspire more statutory control.[118]

Both system models require statutes that provide quick, easy, and cheap legal remedies for data subjects. At the least, these reme-

---

114. Congressional requests form an exception to the Privacy Act. 5 U.S.C. § 552a(b)(9) (1982). When the SSA developed its list of permissible disclosures, it included the release of information to members of Congress and their staffs. *See* Form SSA-5000, *supra* note 94, at no. B.11.

115. U.S. CONST. art. I, § 2. The Census Bureau has a deserved reputation for safeguarding privacy. Consequently, when the census requests private information, people must reveal it or face criminal charges. United States v. Little, 321 F. Supp. 388 (D.Del. 1971).

116. Two important acts secure this right for subjects in certain types of data banks: the Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 (1982) (requires credit investigating and reporting agencies to make files available to data subjects for inspection); and the Family Education Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (1982) (gives students and parents access to personal information in school files).

117. Under the Fair Credit and Reporting Act, for example, the credit reporting industry must give consumers certain information about their own files on request. 15 U.S.C. § 1681g (1982). This information includes: the fact of file preparation, details on file sources and contents, and procedures for correcting a file. *Id.* §§ 1681d(a), g, i.

118. *See supra* note 92 for an account of how the federal use of bank records lead to both a Supreme Court decision favoring the federal government in one dispute and a Congressional Act prohibiting such easy federal access in the future.

dies would need to include a routine that corrects error at its source and sends a notice of the correction to all recent data users.[119] Beyond that, statutory law could penalize data managers for careless error, deliberate error, and habitual error.[120]

IV. CONCLUSION

The national ID card creates both a threat and a promise. It threatens more government surveillance but also promises a chance for the citizenry to exert some control over the network of information that is already tied to the national American identifier, the SSN. Therefore, legislation should not treat the ID card as an isolated item. Instead, Congress should recognize the card as one feature in an extensive system for identifying Americans and recording their actions. If lawmakers place the ID card in its data context, they can write legislation to help cardholders as well as the government. The card will identify American residents. It should also help them discover and correct any information tied to their identity and placed in the national data network.

Elizabeth Friedheim

---

119. *See* the Fair Credit and Reporting Act, 15 U.S.C. § 1681i(d) (corrections for data error must be sent to specified data users); the Privacy Act, 5 U.S.C. § 552a(g)(4) (1982) (damages in civil actions against federal officials who violate informational privacy require proof of intent); Ehlke, *supra* note 93, at 833-35 (the intent requirement makes civil remedy difficult under the Privacy Act). *See also*, Paul v. Davis, 424 U.S. 693 (1976) (the Constitution does not protect privacy from state officials who damage a person's reputation in the community); L. TRIBE, *supra* note 91, at § 15-17 (protecting informational privacy is a task for individual states, not the Supreme Court).

120. The Privacy Act includes criminal sanctions against federal officials. 5 U.S.C. § 552a(i) (1982). Prosecutions, however, have been rare. *See*, Ehlke, *supra* note 93, at 833.