UIC Law Review

Volume 29 | Issue 4 Article 15

Summer 1986

Conceptualizing National Identification: Informational Privacy Rights Protected, 19 J. Marshall L. Rev. 1007 (1986)

Eric Grossman

CONCEPTUALIZING NATIONAL IDENTIFICATION: INFORMATIONAL PRIVACY RIGHTS PROTECTED

Identification fraud is a criminal activity[1] causing an estimated loss of 24 billion dollars a year in the United States.[2] The term "identification fraud" includes a wide range of activities relating to an individual's use of false identification to illegally receive economic benefits. The means and instances of identification fraud are pervasive and legion.[3] Welfare fraud artists, fugitives, illegal aliens, "hot-check writer[s]" and even terrorists and foreign spys use false identification to commit identification fraud.[4] Imagination is the only limitation on the different ways in which a false social security card can be used to commit identification fraud.[5]

Identification fraud is firmly rooted in the United States and persists because of inadequate control and coordination of identification systems.[6] An identification system is the means by which a record holder associates an individual with information about that individual in a computer data bank.[7] While the federal government relies on computers to store information about citizens,[8] the current identification systems used with the computerized records are unre-

---

1. The False Identification Crime Control Act of 1982, 28 U.S.C. 1028 (1982), imposes fines and imprisonment for production of a false identification document, for transferring an identification document knowing it to be false or stolen, and for producing, transferring, or possessing a document-making implement with the intent to produce false identification documents.

2. *Federal Identification Systems: Hearings on S. 1706 Before the Comm. on the Judiciary*, 98th Cong., 1st Sess. 5 (1983) (opening statement of Sen. Robert Dole) [hereinafter cited as *Federal Identification Systems*].

3. *See generally False Identification: Hearings on 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) [hereinafter cited as *False Identification*] (the hearings reprinted numerous articles and reports detailing the means and forms of identification fraud).

4. *False Identification*, *supra* note 3, at 21 (Franks, Documents of Deceit: Birth Certificate Serves as "Breeder" for Acquiring False Identity (Mar. 21, 1982)).

5. *Id.* at 23 (Franks, Documents of Deceit: Bogus Social Security Fraud Mounts, Houston Chronicle (Mar. 22, 1982)). There are at least six million false social security accounts. *Id.* at 29 (Franks, Documents of Deceit: Bogus ID Penalties Pushed-Bill Would Set Stiff Penalties for Bogus ID's, Houston Chronicle (Mar. 25, 1982)).

6. *Id.* at 8 (statement of Sen. Dole). Senator Dole also stated that "identification systems are rushing headlong into the computer age" with no concern for privacy protection or abuses resulting from inadequate safeguards. *Id.*

7. *See infra* notes 23-33 and accompanying text.

8. *See infra* note 22.

liable and subject to abuse.[9] In the past Congress has proposed legislation to improve the identification systems in order to curtail identification fraud.[10] No legislation, however, is currently pending. The national legislature must act to develop a secure identification system and should consider a uniform national identification system that is based on a national identification card or number.[11]

---

9. *Federal Identification Systems*, *supra* note 2, at 7 (statement of Sen. Dole). For example, the Food Stamp Program loses an estimated one billion dollars annually to fraud. *Id.* The lack of a secure identification system is a major source of the problem. *Id.* The Program issues food stamps to eight million households and serves approximately 95 million meals per day. *Id.* at 24 (testimony of Robert Leard, Administrator, Food and Nutrition Service, U.S. Department of Agriculture). The Program uses 17 different identification systems to determine eligibility for the various programs. *Id.* at 35-41.

10. In 1983, the Senate held hearings on S. 1706. *See generally Federal Identification Systems*, *supra* note 2. S. 1706 was a bill that called for the enactment of comprehensive legislation on federal identification systems. The bill provided that all federal identification documents "shall utilize common descriptive terms and formats designed to reduce the redundancy and duplication of identification systems by providing information which can be utilized by the maximum number of authorities possible and facilitate positive identification of bonafide holders of identification documents." *Id.* at 4-5. Additionally, S. 1706 instructed the President to recommend legislation on identification systems. *Id.* The bill stated the recommended legislation must consider the privacy interest of those subject to an identification system and recommend sanctions for unauthorized use and disclosure of identification information. *Id.*

In the area of identification fraud associated with illegal immigration, the Simpson-Mazzoli bill proposed the development of a secure system to identify individuals lawfully entitled to employment. *See* H.R. 1510, 130 CONG. REC. H6149 (daily ed. June 20, 1984); *and* S. 529, 129 CONG. REC. S6969-70 (daily ed. May 18, 1983). *See also* Quade, *ID Card for All?* 69 A.B.A. J. 1370 (1983); Note, *Federal Employer Sanctions*, 1984 *U. Ill. L. Rev.* 97 (discusses the House and Senate versions of the Simpson-Mazzoli Bill). For the House debate surrounding the ramifications of adopting a work eligibility verification system, see 130 CONG. REC. H5633, H5633-5670 (daily ed. June 12, 1984). *See also infra* note 12.

11. The concept of a national identification card or number contemplates the use of a single universal identifier. *See* U.S. DEPT. OF HEALTH, EDUC. AND WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS 109 (1973) [hereinafter cited as RECORDS]. A national identifier is a unique, permanent number that distinguishes an individual from all others. *Id.* Others have conceptualized an identity number as a birth number that is issued at birth and stays with a person throughout life. A. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 4 (1971); Solomon, *Privacy and "1984"*, 7 W. NEW ENG. L. REV. 753, 760-61 (1985).

A national identifier should not be confused with the method of identification that a worker identification card or driver's license uses. Those documents use personal information on the face of the document itself for identification. For example, a Palm Beach, Florida ordinance that was recently declared unconstitutional required various classes of employees working in the city to carry identification cards. *See* Frank, *Worker I.D.s—"Pass Law" Struck Down*, 72 A.B.A. J. 22 (March 1, 1986). In order to obtain an identification card the employee was photographed, fingerprinted and was required to provide other personal information. *Id.*

On the other hand, a national identifier would contain no personal information. *See Federal Identification Systems*, *supra* note 2, at 172 (statement of Joseph Eaton, Professor, University of Pittsburgh) (a national identification card would contain no personal information and would reveal nothing about the personal traits or characteristics of the individual holding the document). A national identifier is a completely arbitrary number or label that contains no information. RECORDS, *supra* at 110. Be-

Emotions run high when individuals consider the concept of a national identification system in the United States.[12] The spectres of Nazi Germany,[13] Japanese internment,[14] and the police dossiers of the 1960's[15] are raised. The use of a national identification system in the United States is said to be "inimical to the democratic system."[16] In fact, the proponents of these emotional arguments fail to examine existing identification documents. Citizens in the United States already carry various indispensible identification documents.[17] Social security cards, credit cards and driver's licenses are such examples, none of which are alleged to be "inimical to the dem-

---

cause personal information often changes throughout an individual's life (for example, weight, age, address and appearance), that information is not incorporated into an identifier. *Id.* The identifier is a permanent label that will not have any mutable items or characteristics. *Id.*

For the purpose of this comment, it is not necessary to determine the methods used to issue and administrate a national identification number. The comment is limited in scope to an examination of how a national identification system based on a single identifier interacts with informational privacy. Practically, however, the cost of issuing a securing identifier to every citizen is estimated at far below the annual losses associated with the lack of a secure identification system. *See False Identification Hearings, supra* note 3, at 125 (report by the Comptroller General of the United States). The Comptroller General estimated that reissuing social security numbers to the entire population could cost as much as two billion dollars. If this is a fairly good estimate of issuing a secure identifier, then it is far below the 24 billion dollars lost to identification fraud annually.

12. During the debates on the House version of the Simpson-Mazzoli immigration reform bill, controversy centered on a provision of the bill that authorized the President to report to Congress on the changes and costs that "may be necessary to establish a secure system to determine employment eligibility." H.R. 1510, 98th Cong., 2d Sess. 130 CONG. REC. 5658 (daily ed. June 12, 1984). Various representatives felt this provision authorized the President to establish a national identification system and reacted strongly to that possibility. *See, e.g., id.* at H5659 (statement of Rep. Mitchell) ("[f]or God's sake . . . on this issue, let us move . . . to prevent the establishment of [a] national identification system which . . . is inimical to the democratic system."); *id.* at H5669 (statement of Rep. Richardson) ("[n]ational identifiers endanger our right to privacy . . . and there can be no freedom without privacy") *id.* ("a national ID card would violate the right of the individual to live and work free from the shadow of government surveillance").

13. *Id.* at H5660 (statement of Rep. Roybal) ("[a] national identification system is going to affect every man, woman and child in the United States . . . we may face the danger of ending up like Nazi Germany.").

14. *See id.* at 5669 (statement of Rep. Roybal) (discusses registration of Japanese during World War II).

15. *Id.* (statement of Rep. Mitchell) ("espionage police surveillance" during the civil rights movement would have increased if a national identity card were available).

16. *Id.* at H5659 (statement of Rep. Mitchell).

17. Driver's licenses, passports, social security cards, and other documents are all used for identification in government programs ranging from unemployment compensation to student loans and tax refunds. *Federal Identification Systems, supra* note 2, at 5 (statement of Sen. Dole). The Immigration and Naturalization Service alone issues seven different identity documents. *Id.* at 207 (statement of Robert Brademuehl, Associate Commissioner for Enforcement, Immigration and Naturalization Service). The INS issues a total of approximately 14 million identity documents per year. *Id.*

ocratic system." Perhaps the real fear, and a valid concern, relates to the impact of national identification on the individual's right of informational privacy.[18]

This comment considers the potential impact of a national identification system on informational privacy. The societal need for identification is examined first.[19] The law and policy of informational privacy are explored.[20] Finally, the concept of national identification is analyzed in light of existing protections for informational privacy.[21] The courts have adopted a balancing test to determine whether the right to informational privacy outweighs the government's information practices. This balancing test, along with other statutory regulations, ensures that a new national identification system would serve societal interests while also providing sufficient protection for the individual's right to informational privacy.

IDENTIFICATION IN THE INFORMATION AGE

The government holds vast amounts of personal information about individuals in the form of computerized records.[22] The government has collected personal information for one basic reason: citizens in the United States are dependent on the government for a variety of goods, services, benefits and obligations.[23] Such dependency necessitates the collection of information[24] because administrative actions must precede each benefit received or obligation incurred. The action taken depends on the content of the information that the beneficiary discloses. It is impossible to determine if an individual is eligible for a benefit without collecting the appropriate

18. *See infra* notes 76-107 and accompanying text.
19. *See infra* notes 22-44 and accompanying text.
20. *See infra* notes 45-75 and accompanying text.
21. *See infra* notes 76-108 and accompanying text.
22. A recent Office of Technology Assessment report stated that federal law enforcement agencies have 288 million records on 114 million people. OFFICE OF TECHNOLOGY ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 69 (October, 1985). There are 200 million active files in the Social Security Administration. *Federal Identification Systems, supra* note 2, at 52 (statement of Louis Enoff, Acting Deputy Commissioner, Social Security Administration). As early as 1966, a government survey indicated three billion federal files existed with information on individuals, nearly half of which were computerized. Project, *Government Information and the Rights of Citizens*, 73 MICH. L. REV. 971, 1223 (1975) (citing *Staff of Subcomm. on Administrative Prac. and Proc. of the Senate Comm. on the Judiciary*, 90th CONG. SESS., *Government Dossier* 1 (Comm. Print 1967)). It is now estimated that the government holds four billion computerized records on individuals: 17 records for each and every individual in the United States. D. BURNHAM, THE RISE OF THE COMPUTER STATE 51-52 (1983).
23. Soloman, *supra* note 11, at 757.
24. *See* Linowes, *Must Personal Privacy Die in the Computer Age*, 65 A.B.A. J. 1180, 1182 (Aug. 1979) ("[a]dministrators responsible for furnishing . . . services must satisfy themselves of a person's eligibility by demanding and getting much personal, often sensitive, information.").

information.[25] The individual expects and deserves an intelligent and correct administrative action,[26] and errors can only be minimized if relevant information is disclosed and accumulated.[27]

A correct administrative action also depends on accurately identifying the individual to which the action pertains.[28] It is necessary to maintain a separate account for each individual.[29] The identification of the individual with a record in the data base requires the use of an identification system. There are two aspects to an identification system. An "identification" is, first of all, an unauthenticated assertion of identity.[30] "Authentication" is the necessary second step in determining that an asserted "identification" is, in fact, a valid one.[31] "Identification authentication" verifies that a record, and the corresponding administrative action, pertains to the correct individual.[32] "Identification authentication" is, therefore, a necessary element in any transaction with the government.[33]

---

25. *See* Rule, *Preserving Individual Autonomy in an Information Oriented Society*, in COMPUTERS AND PRIVACY IN THE NEXT DECADE, 65, 66 (L. Hoffman ed. 1980) (information is used to take "authoritative actions"); RECORDS, *supra* note 11, at 9-10 (information is necessary for managing individual transactions); Halls, *Raiding the Databanks: A Developing Problem for Technologists and Lawyers*, 5 J. CONTEMP. L. 245, 245 (1979) (informed decisions require information).

26. Rule, *supra* note 25, at 66-68.

27. *Id.* "[D]iscriminating decision making can only take place by reliance on detailed recorded information on the persons concerned." *Id.* Consider, for example, the decisions the Internal Revenue Service must make. The IRS must assess the precise obligations and benefits for every taxpayer. *Id.* In 1982, the IRS received 170.4 million tax returns and issued 74.5 million different refunds totalling 75.2 billion dollars. *Federal Identification Systems*, *supra* note 2, at 117 (statement of James Owens, Deputy Commissioner, Internal Revenue Service).

28. The Privacy Protection Study Commission ascertained three methods of identification: through physical attributes, through a possession (e.g., a driver's license or passport), and with a label such as a name, number, or address. PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY, 605 (1977). This comment focuses on the use of a national identifier for identification. The identifier is a numerical label that falls under the label method of identification.

29. For example, the IRS must maintain separate accounts for every taxpayer, and must use an identifier to operate the tax administration system. *Federal Identification Systems*, *supra* note 2, at 118 (statement of James Owens, Deputy Commissioner, Internal Revenue Service).

30. PRIVACY PROTECTION STUDY COMMISSION, *supra* note 28, at 605-06. An organization uses the identification to make an initial determination that records pertain to the individual asserting the identification. *Id.* The organization then uses the identification (e.g., a social security number on a tax return) to select the record corresponding to the individual asserting the identification. *Id.*

31. *Id.* at 607.

32. "Identification authentication" is also used when information is transferred from one organization to another. *Id.* For example, when a bank sends interest information to the IRS, the information is labelled with a taxpayer identification number. *Id.* The number is a label that both identifies the record pertaining to the taxpayer and authenticates the record identification. *Id.*

33. *Id.* at 606-08. "Identification authentication" becomes crucial as an organization increases in size and complexity. *Id.* at 607. Numerical labels facilitate the effective operation of any large and complex organization. *Id.* at 608. An organization such as the Internal Revenue Service cannot possibly rely on the physical attribute or

Identification fraud occurs when the identification system fails or is otherwise unable to authenticate. An individual asserts an identification, facilitates an invalid authentication, and a false identification arises. For example, obtaining a social security number requires documentary evidence of age, identity and citizenship.[34] The documentary evidence, such as a birth certificate, serves to authenticate the identification of the individual. If the birth certificate was fraudently obtained,[35] however, the authentication is invalid. The individual asserting the identification perpetrates a fraud, and escapes the intrinsic purpose of identification systems: authenticating identifications in order to render benefits to those lawfully entitled to receive the benefit.

A national identification system would reduce or eliminate identification fraud through ensuring the authenticity of the identification asserted in a government transaction.[36] The system would provide an authenticated identifier to every citizen in the United States.[37] The identifier is a number that is unique to every individual and it validates any asserted identification.[38] It becomes ex-

---

possession methods of identification (*see supra* note 28) because the organization uses computers to digest its huge volume of transactions. The numerical label has thus become the preeminent method of identification in the information age. *Id.*

34. Prior to the date of the enactment of this law, social security numbers were issued on a bare assertion of identity. *Federal Identification Systems, supra* note 2, at 60 (statement of Louis Enoff). No supporting documents were necessary in order to receive a social security number. Thus no authentication of the identification took place. Presently, 90 percent of all social security numbers issued to date were issued under this method. *Id.* In an effort to make the social security number a more reliable identifier Congress enacted a law that requires all applicants to produce documentary evidence of identity and citizenship. *See* Social Security Administration, Evidence Requirements, 20 C.F.R. 422.107 (1985). Because the law only requires that new and replacement cards be issued in a new format, the Social Security Administration estimates it will take 80-100 years before all social security cards in use are replaced. *Federal Identification Systems, supra* note 3, at 110-14, 137 (report by the Comptroller General of the United States).

35. It is relatively easy to obtain a fraudulent birth certificate because of the lack of uniformity among the issuing authorities. Seven thousand agencies use a thousand different formats to issue birth certificates. *Federal Identification Systems, supra* note 2, at 5 (statement of Sen. Dole).

36. *See Federal Identification Systems, supra* note 2, at 169, 171 (statement of Joseph Eaton, Professor, University of Pittsburgh) (a secure identification document will significantly deter any criminal activity associated with false identification).

37. RECORDS, *supra* note 11, at 111.

38. For a discussion of the characteristics of a national identifier, see *supra* note 11. When the identifier is issued to an individual, the government would create a computerized record containing information about the individual to whom the number was issued. That record is contained in a national population register, or a national data base. *Federal Identification System, supra* note 3, at 179-81 (statement of Joseph Eaton, Professor, University of Pittsburgh). Then, when an individual presents his/her identifier for a transaction requiring identification, the agency that receives the identifier would access the national population register in order to verify the asserted identification. Because there would be only one identifier for each individual, it would become extremely difficult to assert an identification based on a false identity, or a false document.

tremely difficult for an individual to obtain identification documents under false pretenses.[39] Consequently, the fraud associated with the use of false birth certificates, social security numbers, and other government identification documents, is severly curtailed.

Our information based society has created an estimated four billion computerized records on individuals.[40] The numerical labels used to identify those records, such as the social security number, have increased in importance and use because automated data systems rely on numerical labels for identification.[41] The dehumanizing effect of becoming a mere number in the eyes of the government is an inescapable result of modern society.[42] Individuals must remember, however, that benefits result from the efficient use of a numerical label. Prompt and correct administrative action is a direct result of efficiently using and requiring a numerical label. While a national identification system enforces the use of a numerical label, society benefits from the creation of a secure identification system.[43] The societal benefits that flow from a national identification system merit a careful consideration of creating such a system. An examination of the status of informational privacy policy and law will determine whether national identification is, or is not, inimical to democratic society.[44]

---

39. *See supra* note 38.
40. *See supra* note 22.
41. *See supra* note 33.
42. PRIVACY PROTECTION STUDY COMMISSION, *supra* note 28, at 608.
43. Elimination of identification fraud and a 24 billion dollar a year problem is one benefit. *See supra* note 36-38 and accompanying text. A single uniform identification system also promotes efficiency in record-keeping, record retrieval, updating and correcting erroneous information, and interactions with the government. RECORDS, *supra* note 11, at 111. *See also* A. MILLER, *supra* note 11, at 4 (a birth number would "expedite the business of society"); A. WESTIN, DATABANKS IN A FREE SOCIETY, COMPUTERS, RECORD KEEPING AND PRIVACY 398 (1972).
44. This comment focuses entirely on the informational privacy aspects of national identification. Many other issues are involved, though the issues are perhaps not germane to using a national identifier solely for record identification purposes. The issues beyond the scope of this comment include the following:

(1) Would the burden imposed from the bureaucratic apparatus created to administer a national identification system prove unworkable and overwhelming?
(2) Is it possible that the loss of an identification card would pose such a serious inconvenience and burden to an individual (so) as to outweigh the benefits from using the card?
(3) Would the threat of official confiscation of a card produce administrative intimidation?
(4) Would an identity card become an internal passport or a tool to curtail freedom of movement?

For a discussion of these omitted issues see Shattuck, *In the Shadow of 1984: National Identification Systems, Computer-Matching, and Privacy in the United States*, 35 HASTINGS L.J. 991, 998-1001 (1984) (the government's police powers are sufficient to use a national identity document as a tool to threaten freedom of movement); RECORDS, *supra* note 11, at 112 (the dangers inherent in the use of a national identifier outweigh any practical benefits). *See also* PRIVACY PROTECTION STUDY COMMISSION, *supra* note 28, at 618 (any standard universal label linked with a central

INFORMATIONAL PRIVACY: POLICY AND LAW

The right to informational privacy is succinctly defined as the right of the individual to maintain control over personal information concerning one's "physical and individual characteristics, knowledge, capabilities, beliefs and opinions."[45] A national identification system implicates a conflict with an individual's right to informational privacy because identification is intrisically tied to the government's collection and disclosure of personal information.[46] When the government collects and disseminates information, the individual loses control over that information.[47] Thus, governmental information practices may invade the right of informational privacy. These practices may violate informational privacy in three instances: when the individual discloses information to the government, when a government agency releases information to another government agency, and when the information is released to the public.[48] If there is a violation of the right to informational privacy, there are different injuries which may result.

First, a violation of the right can cause psychological harm.[49]

---

population register implicates a serious conflict with American civil liberty traditions).

45. Project, *supra* note 22, at 1225. *See* A. MILLER, *supra* note 11, at 25 ("privacy is the individual's ability to control the circulation of information relating to him"). *See also* Comment, *The Use and Abuse of Computerized Information: Striking a Balance Between Personal Privacy Interests and Organizational Needs*, 44 ALB. L. REV. 589, 601 (1980); Comment, *Intrusions on Informational Seclusion in the Computer Age*, 17 J. MARSHALL L. REV. 831, 838 (1984) (informational privacy gives an individual the right to control the collection, maintenance, and dissemination of personal information). *Cf.* Warren and Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890) (each individual has a common law right to determine "to what extent his thoughts, sentiments and emotions shall be communicated to others").

46. *See* PRIVACY PROTECTION STUDY COMMISSION, *supra* note 28, at 607 (mediating interactions between an individual and society requires identification; identification is essential when organizations exchange and disclose records). *See also supra* notes 28-33 and accompanying text.

47. Comment, *The Interest in Limiting the Disclosure of Personal Information: A Constitutional Analysis*, 36 VAND. L. REV. 139, 144 (1983). *See* Comment, *Informational Privacy: Constitutional Challenges to the Collection and Dissemination of Personal Information by Government Agencies*, 3 HASTINGS CONST. L.Q. 229, 257-58 (1976) (it is impossible to monitor the information in the hands of public officials).

48. *See* Comment, *The Constitutional Right to Withhold Private Information*, 77 NW. U.L. REV. 536, 557 (1982). The author asserts that there are two points in which government information practices implicate privacy: the initial release of information to the government and the government's subsequent disclosure of the information. It is necessary, however, to distinguish the two ways in which the government can disclose information. The government can disclose information to another government agency (*see infra* notes 95-105 and accompanying text) and the government can disclose information to the public (*see infra* notes 107-08 and accompanying text). The potential harm to informational privacy interests are different under each disclosure, and thus a distinction is necessary. *See infra* notes 68-69 and accompanying text.

49. Project, *supra* note 22, at 1227. The Project noted that behavior modifica-

The revelation of embarrassing facts, either in the release or disclosure of information, can impair dignity.[50] The disclosure of personal information may also have a detrimental effect on social and professional interactions.[51] Facts that discredit a person can lead others to look unfavorably on that person.[52] A second possible injury, the failure to overcome attached stigma, is closely related to the disclosure of embarrassing facts. If personal information is never deleted from a record, that information can affect a person throughout his/her life.[53] For example, an arrest record may affect a person's chances for employment throughout life, making it impossible to obtain a fresh start.[54] Other injuries are also possible. The mere knowledge that someone retains personal records on oneself may impair psychological health.[55] The injuries that can result from the unwarranted collection and disclosure of personal information indicate that the right of informational privacy protects important interests.

As the government collects more personal information, the threats to informational privacy increase.[56] Unregulated information practices within the federal government could create "Big Brother." Conversely, the government must retain personal records in order to deal efficiently with individuals and to effectively prevent fraud.[57] Thus, individuals are required to release control over information,

---

tion can result from unregulated government information practices. *Id.* Individuals will tailor behavior towards enhancing their record so as to receive maximum benefits from the government while minimizing behavior that could reduce benefits. *Id. See also* Comment, *Federal Government Data Sharing and the Threat to Privacy*, 61 J. URB. L. 605, 606 (1984) (potential denial of benefits may chill political expressions).

50. *See* Comment, *Damages Under the Privacy Act of 1974: Compensation and Deterrence*, 52 FORDHAM L. REV. 611, 621 (1982) (the interest the Privacy Act protects in avoiding embarrassment resulting from misuse of records is essentially a dignitary interest).

51. Kronman, *The Privacy Exemption to the Freedom of Information Act*, 1980 J. LEGAL STUD., 727, 739.

52. ID.

53. *See* Soloman, *supra* note 11, at 755 ("[p]eople tend to forget and forgive, computers do not").

54. Project, *supra* note 22, at 1229-30 (citing *Criminal Justice Data Banks, Hearings on S.2542, S.2810, S.2963, S.2964 Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 93rd Cong., 2d Sess. 18 (1974)). While an arrest record may brand a person for life, potentially greater harm can flow from an inaccurate record. The failure to include the dropped or dismissed status of prior charges can cause grave damage. *Id. See also* D. BURNHAM, *supra* note 22, at 33-34 (inaccurate data presents a severe potential for harm); Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information Oriented Society*, 67 MICH. L. REV. 1091, 1109-14 (1969) (denial of society and economic benefits result from inaccurate data).

55. Gordon, *The Interface of Living Systems and Computers: The Legal Issues of Privacy*, 2 COMPUTER L.J. 877, 889 (1981).

56. *Id.* at 887-88. *See* Shattuck, *supra* note 44, at 995 ("relentless growth of information technology that permits virtually unlimited permanent storage" of information creates grave privacy concerns).

57. *See supra* notes 23-27 and accompanying text.

and therefore the right of informational privacy is, itself, subject to inherent limitations.[58] Constitutional interpretation[59] and statutory

58. Comment, *The Interest in Limiting the Disclosure of Personal Information: A Constitutional Analysis*, 36 VAND L. REV. 139, 141 (1983) [hereinafter cited as *Disclosure of Personal Information*]. It is not socially desirable for an individual to maintain complete control over personal information. *Id.* Efficient decision making requires information. *Id.* An individual also has an interest in disclosing information because decisions based on the information often benefit the individual. *Id.* Thus, not every collection and disclosure of information violates an individual's informational privacy. Society would cease to function if an individual had an unmitigated right to determine all methods and forms of information disclosure. Government benefits, based on eligibility standards, require information and the individual must release control over personal information to obtain these benefits.

59. The United States Supreme Court has indicated that the right to informational privacy may warrant constitutional protection. Two of the Court's decisions, Whalen v. Roe, 429 U.S. 589 (1977), and Nixon v. Administrator of General Services, 433 U.S. 425 (1977), describe the privacy threats that the disclosure of information poses. These decisions illuminate the scope of the constitutional protection that the Court would give to the right of informational privacy.

In *Whalen*, the plaintiffs challenged the constitutionality of the New York Controlled Substances Act of 1972, 1972 N.Y. Laws 878; N.Y. PUB. HEALTH LAWS 300 (McKinney Supp. 1976-1977). The statute sanctioned the creation of a computerized record of the names and addresses of all persons for whom "Schedule II" prescriptions were written. 429 U.S. at 593. "Schedule II" drugs are drugs that have legitimate medical uses but are also subject to illegal use and abuse. The drugs include opium, cocaine, amphetamines, and methaqualone. *Id.* at 593 n.8. The statute required the prescribing physician to disclose the recipient's name, address and age, and the names of the prescribing physician and dispensing pharmacist. *Id.* at 593.

The plaintiffs alleged that the statute violated "a constitutionally protected zone of privacy." *Id.* at 598. The plaintiffs offered evidence at the trial level of the litigation that some patients had, in fact, declined medication involving "Schedule II" drugs because they feared stigmatization as a drug addict from the disclosure or misuse of the information. *Id.* at 595 n.16. Counter evidence was offered to prove that the statute had not had any effect on the majority of patients receiving "Schedule II" prescriptions. *Id.* In deciding the case, the *Whalen* Court recognized the potential threat to the plaintiffs' privacy and the correlative right of informational privacy.

The *Whalen* Court stated that a person has an "*interest in avoiding disclosure of personal matters.*" *Id.* (emphasis added). The Court, however, was satisfied that the statute did not "pose a sufficiently grievous threat to [the] interest in [avoiding disclosure] to establish a constitutional violation." *Id.* The Court indicated that the security precautions surrounding the data base were adequate and there was no reason to assume that improper administration of the statute that would result in disclosures. *Id.* The Court characterized the plaintiffs as having merely a "clearly articulated fear about the pernicious effects of disclosure." *Id.* at n.27. The Court noted that in no instance had other states' statutes with similar provisions failed to properly maintain security. *Id.* The initial disclosure of the information was characterized as another facet of a "host of unpleasant invasions of privacy . . . associated with many facets of health care." *Id.* at 602. The Court also indicated that the legislature's assumption that the disclosed information served an important public interest was reasonable. *Id.* at 597-98. The Court noted that the state has a responsibility to protect health in the community and disclosures of information that reasonably relate to this interest do not intrinsically invade privacy interests. *Id.* The plaintiffs' interest in nondisclosure of personal information, therefore, was not violated and the statute was constitutional. *Id.* at 603-04.

Despite the fact that the *Whalen* Court did not find the statute violated the plaintiffs' interest in nondisclosure, the Court recognized that there is a protectable interest, subject, however, to inherent limitations. The Court stated that "[w]e are not unaware of the threat to privacy implicit in the accumulation of vast amounts of

personal information in computerized data banks or other massive government files . . . much of which is personal in character and potentially embarrassing or harmful if disclosed." *Id.* at 605. The Court, however, also intimated that there may be no constitutional duty to weave security precautions into a statute that requires the release and accumulation of personal information. *Id.* The Court stated that the government's duty to avoid unwarranted disclosures may not be based on the Constitution. *Id.* Justice Brennan, in his concurring opinion, attempted to negate the effect of this dictum. He stated that "[b]road dissemination by state officials of such information . . . would clearly implicate constitutionally protected privacy rights." *Id.* at 606 (Brennan, J., concurring).

Commentators have noted the apparent limitations of the *Whalen* decision. *See* 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, 878 (1985) (the *Whalen* decision is ambiguous with regard to the nature of the privacy interest and the degree of scrutiny); Comment, *Federal Government Computer Data Sharing and the Threat to Privacy*, 61 J. URB. L. 605, 613-14 (1984) (because the Court applies a traditional rationality test, any government information practice is constitutional). *But see* Comment, *Disclosure of Personal Information, supra* note 53, at 178 (the *Whalen* decision provides a foundation for a constitutional interest in informational privacy).

In *Nixon v. Administrator of General Services*, 423 U.S. 425 (1977), the Supreme Court reaffirmed its recognition of informational privacy and expressly balanced the interests. In *Nixon*, former President Nixon had challenged a law requiring him to release tapes and records made during his term in office. Title I of Pub. L. 93-526, 88 Stat. 1699, 44 U.S.C. 2107 was entitled The Presidential Recordings and Materials Preservation Act. The Act directed the Administrator of General Services to take custody of approximately 42 million pages of documents and 880 tape recordings of conversation. *Id.*, 433 U.S. at 430. Government archivists would screen the material, return personal information, and release the rest of the information to the public. *Id.* at 435. Nixon alleged the law violated his constitutional privacy rights. *Id.* at 455. The former President also alleged the Act was unconstitutional on a number of other grounds: violation of separation of powers, first amendment association rights, presidential privilege doctrine, and the Bill of Attainder Clause. *Id.* at 429.

The *Nixon* Court held the law did not violate any privacy rights. *Id.* at 465. The Court balanced Nixon's privacy interest against the public interest in subjecting the presidential materials to archival review and found that the public interest outweighed Nixon's limited interest in avoiding disclosure of personal matters. (This balancing test is discussed *infra* notes 61-72 and accompanying text). In balancing the competing interests, the *Nixon* court implicitly recognized that the former President had a valid interest in not disclosing personal information to the government. If the Court had declined to analyze Nixon's informational privacy interests, then it could be assumed that Nixon had failed to assert an interest worthy of protection. The Court, however, did analyze Nixon's privacy interests (*see infra* notes 61-62) and thus implied that there is a valid constitutional interest in informational privacy.

Whalen and *Nixon* provide support for the constitutional recognition of a right to informational privacy. Comment, *Disclosure of Personal Information, supra* note 58, at 178-79. The Court is willing to examine the competing interests and has indicated that several factors are involved. The constitutional scope of the right is not fully delineated, however, and lower courts have rendered inconsistent decisions in light of *Whalen* and *Nixon*. *Compare* J.P. v. DeSanti, 653 F.2d 1080 (6th Cir. 1981) (no general constitutional right to non-disclosure of juvenile court records) *and* St. Michaels Convalescent Hospital v. California, 643 F.2d 1369 (9th Cir. 1981) (law requiring disclosure of cost information to public affects no privacy interest) *with* United States v. Westinghouse, 638 F.2d (3d Cir. 1980) (applied balancing test to challenged law requiring disclosure of employee medical records) *and* Plante v. Gonzales, 575 F.2d 1119 (5th Cir. 1978), *cert. denied*, 439 U.S. 1129 (1979) (applied balancing test to determine whether interest in non-disclosure of financial records outweighs public interest).

For a discussion concerning the lower court opinions, *see generally* Seng, *supra*

law[60] resolve the conflict between the government's need to know information and the individual's right to control information.

When an issue involving informational privacy rights is litigated, the courts balance the probability of harm to the individual's privacy interests against the public's interest in disclosure.[61] If the

---

note 59, at 883-84; Comment, *A Constitutional Right to Avoid Disclosure of Personal Matters: Perfecting Privacy Analysis in J.P. v. DeSanti*, 653 F.2d 1080 (6th Cir. 1981), 71 GEO. L.J. 219 (1982); Comment, *The Constitutional Right to Withhold Private Information*, 77 NW. U.L. REV. 536, 547-57 (1982).

60. The Freedom of Information Act ("FOIA"), 5 U.S.C. 552 (1982), enables the public to request disclosure of government held records and information. The FOIA provides that federal agencies "shall make available for public inspection and copying" a diverse and extensive range of records that agencies maintain. *Id.* at 552(a)(2). The FOIA's privacy exemption prohibits the disclosure of any information "which would constitute a clearly unwarranted invasion of personal privacy." *Id.* at 552(b)(6). The section applies to "personnel and medical files and similar files, the disclosure of which would invade privacy." *Id.* The courts have interpreted the privacy exemption broadly, and any file containing personal information is included in the exemption. *See* U.S. Dept. of State v. Washington Post Co., 456 U.S. 595 (1982) ("similar files" encompasses any file in which an individual is identified from information contained in the file).

This exemption is a fertile area of judicial interpretations defining the general scope of the right to informational privacy, based upon statutory interpretation. Extensive litigation has arisen under this exemption. *See generally* Kronman, *supra* note 51, at 729 n.13 (provides compilation of significant FOIA privacy exemption cases). The privacy exemption of the FOIA protects informational privacy because the exemption restricts disclosure of personal information.

The congressional intent behind the FOIA's privacy exemption supports the use of judicial interpretations of the privacy exemption to define the scope of protection the courts give to informational privacy interests. The congressional intent for this exemption was to protect the privacy interests associated with the disclosure of personal information. Congress stated that the "limitation of clearly unwarranted invasion of personal privacy provides a proper balance between the protection of an individual's right of privacy and the preservation of the public's right to government information by excluding those kinds of files, the disclosure of which might harm the individuals." 1966 *U.S. Code Cong. and Admin. News* 2418, 2429.

61. The courts construing the privacy exemption of the FOIA have adopted the balancing test to determine whether to disclose records containing personal information. In *Rose v. Department of the Air Force*, 425 U.S. 352 (1976), the United States Supreme Court stated that the exemption applies if the probability of harm to the individual's privacy interest exceeds the public interest in disclosure. *Rose*, 425 U.S. 352, 380-81.

The plaintiffs in *Rose* requested that the Air Force Academy disclose all case summaries of Honor Code hearings. *Id.* at 354-55. The plaintiffs were members of the New York University Law Review and were seeking material for an article on discipline at military service academies. *Id.* The Air Force Academy denied the plaintiff's request on the basis that such a disclosure would constitute an invasion of the privacy rights of the cadets involved in the hearings. *Id.* at 355 n.2.

The issue before the *Rose* Court was whether the Court of Appeals erred in ordering an *in camera* inspection of the case summaries. *Id.* at 357. In upholding the order, the Court stated that an *in camera* inspection would balance the cadets' privacy rights with the public's right to government information. The Court noted that an *in camera* inspection would insure that most identifying information was deleted, and while an incidental invasion of privacy might occur, an *in camera* inspection would protect against clearly unwarranted invasions of privacy. *Id.* at 381-82. Thus, the Court gave meaning to the phrase "clearly unwarranted invasions of privacy." Because all apparent identifying information was to be deleted from the files, *clearly*

disclosure of information creates a clearly unwarranted invasion of personal privacy, then the information practice being scrutinized violates the right to informational privacy.[62] The courts have indicated that various factors determine whether the scrutinized information practice involves a clearly unwarranted invasion of informational privacy.

---

unwarranted invasion of privacy would not occur. There may be, however, instances in which someone closely associated with the cadets at the Academy could identify an individual from a case summary despite the deletion of all identifying information. *Id.* at 380-81. In the Court's view, this type of identification was an incidental invasion of privacy and the public interest outweighs an incidental invasions of privacy. The *Rose* Court then held that the district court was to examine the requested material and weigh the competing interests to determine whether to allow the disclosure of the requested material. *Id.* at 380.

Numerous lower court decisions involving the FOIA's privacy exemption have applied the Supreme Court's balancing test and balanced the probability of harm to privacy interests against the public interest in disclosure. Prior to the *Rose* decision, lower courts had adopted a similar balancing test. *See* Kronman, *supra* note 51, at 744 n.63 (noting cases prior to *Rose* using balancing approach). Decisions after the *Rose* decision unanimously apply the balancing approach. *See, e.g.*, Minnis v. U.S. Dept. of Agriculture, 737 F.2d 784, 786 (9th Cir. 1984) (balancing test applies); Height Community Congress v. Veterans Ad., 732 F.2d 526 (6th Cir. 1984) (same); Church of Scientology of California v. U.S. Department of Army, 611 F.2d 738 (D.C. Cir. 1979) (same).

The Supreme Court's decisions in *Whalen* and *Nixon* also indicate that the balancing test is used when non-statutory informational privacy interests are in issue. For the facts, issue and holdings in these decision, see *supra* note 59. In *Whalen*, the Court implicitly balanced the competing interests. *See* Comment, *The Constitutional Right to Withhold Private Information*, 77 NW. U.L. REV. 536, 547 (1982) (the *Whalen* Court did not expressly adopt a balancing test, yet implicitly weighed the privacy interest against the public interest). The *Nixon* Court expressly balanced *Nixon* privacy interest against the public interest in subjecting the presidential materials to archival review. *Nixon*, 423 U.S. at 455-64.

62. The "clearly unwarranted" standard is mandated by the FOIA's privacy exemption. *See supra* note 60. The *Whalen* and *Nixon* Courts also appear to have applied a clearly unwarranted standard. Neither decision found that the plaintiff's privacy interest's would suffer such a grievous privacy invasion as to cause the statutes involved in each case to be unconstitutional.

In *Whalen* the Court noted that unwarranted disclosures were improbable because only 41 people had access to the computerized data: 17 Department of Health Employees and 24 state investigators. *Whalen*, 429 U.S. at 594-95. Moreover, in a twenty-month period the data was only reviewed twice. *Id.* The statute's security provision protected the disclosed information from unwarranted disclosures.

The *Nixon* Court, in examining the competing interests, found that Nixon's disclosure of information would not result in a clearly unwarranted invasion of privacy. The Court compared Nixon's privacy interest with the privacy interest asserted in Whalen v. Roe. The Court noted that Nixon's privacy interest was weaker because the government was not going to retain long-term control over the personal information. *Nixon*, 423 U.S. at 459. All private materials were to be returned to Nixon. *Id.* In *Whalen*, the state maintained control over the released personal information for a lengthy period of time. *Id.* at 458-59. The Court also noted that of the 42 million documents subject to disclosure, Nixon had seen no more than 200,000 items. *Id.* at 459. He could only assert a privacy claim to those items previously seen and of those only "a very small fraction related to extremely private communications." *Id.* Thus, Nixon's disclosure of the Presidential materials would not result in a clearly unwarranted invasion of informational privacy.

First, the content of the information is examined.[63] Highly personal information creates a greater probability of harm to privacy interests than information devoid of personal content.[64] The probability of harm is greater when personal information is involved because the likelihood of injury to the interests that informational privacy protects increases as information becomes more personal.[65] The disclosure of highly personal information can impair dignity and attach a stigma to an individual causing psychological harm.[66] Conversely, impersonal information has little potential for harm and thus, has weak privacy implications.[67]

The extent of the disclosure of information also has an effect on the probability of harm to informational privacy.[68] Informational privacy protects against injuries associated with the disclosure of in-

---

63. *See* Providence Journal Co. v. Federal Bureau of Investigation, 450 F. Supp. 778, 784 (D.R.I. 1978) (the privacy exemption of the FOIA is concerned with the content of information).

64. *See Minnis*, 737 F.2d at 787 (address list revealing personal interest in outdoor activities involves more than minimal privacy interests); *Height Community Congress*, 732 F.2d at 529 (addresses of veterans receiving loans implicates important privacy interests); *Church of Scientology of California*, 611 F.2d at 747 ("disclosure of religious affiliations and activities would constitute an . . . invasion of privacy"); Wine Hobby U.S.A., Inc. v. U.S. Internal Revenue Service, 502 F.2d 133, 137 (3d Cir. 1974) (address list revealing family and personal activities involves invasion of privacy); Professional Review Organization of Florida, Inc. v. U.S. Dept. of Health and Human Services, 607 F. Supp. 423, 427 (D.D.C. 1985) (resumes revealing professional credentials an other personal information raises legitimate privacy interests); Hemenway v. Hughes, 601 F. Supp. 1002, 1005 (D.D.C. 1985) ("blanket disclosure of citizenship information" is invasion of privacy); Hock v. Central Intelligence Agency, 593 F. Supp. 675, 689-90 (D.D.C. 1984) (substantial privacy interest in disclosure of personal letters).

65. The right of informational privacy protects individuals from injuries associated with the disclosure of personal information. *See supra* notes 49-54 and accompanying text. If information is impersonal, then an individual cannot suffer embarrassment of emotional harm from the disclosure of that information.

66. *See supra* notes 49-54 and accompanying text.

67. *See, e.g.*, Van Bourg, Allen, Wemberg and Roger v. National Labor Relations Board, 728 F.2d 1270, 1273-74 (9th Cir. 1984) (list of employee names and addresses involves minimal privacy interests); Sullivan v. Veterans Administration, 617 F. Supp. 258, 260 (D.D.C. 1985) (minimal privacy interest if information contains no intimate personal details); Citizens for Environmental Quality, Inc. v. U.S. Dept. of Agriculture, 602 F. Supp. 534, 538-39 (D.D.C. 1984) (no privacy interest if information does not reveal identity of the individual that is the subject of the information); Ditlow v. Schultz, 517 F.2d 166, 170 n.16 (D.C. Cir. 1975) (disclosure of names and address on customs forms involves minimal privacy interests).

68. The Supreme Court's interpretation of informational privacy supports this premise. In *Whalen*, the Supreme Court noted that the initial disclosure of personal information in the health care area was unpleasant, but necessary. *Whalen*, 429 U.S. at 602. The Court suggested that little, if any, privacy interest was at stake in the initial disclosure. In *Nixon*, the Court emphasized that the disclosure of presidential materials was limited to the archivists reviewing the materials. *Nixon*, 433 U.S. at 459. The archivists had "an unblemished record for discretion," *id.* at 462, and there was no public access to personal information. Therefore, under the Supreme Court's interpretation of informational privacy, a partial disclosure limits probability of harm to informational privacy interests.

formation.[69] When personal information is disseminated to the public, there is a wide disclosure and a greater probability for harm. When there is no public access to personal information, there is less potential for harm to informational privacy.

After scrutinizing the probability of harm,[70] the court will examine the strength of the public interest in the disclosure.[71] If the public interest outweighs the probability of harm, then informational privacy interests are not infringed. The balancing test is applied on a case-by-case basis, and the facts of each case determine the outcome.[72] While the result of the balancing test depends on the facts applied, certain principles arise from the courts' examination of the interests involved.

First, the privacy interest and the purpose for the disclosure of

---

69. *See supra* notes 49-54 and accompanying text.

70. Other specialized factors may also play a role in creating a probability of harm to privacy interests. The security of the database is one factor. *See Whalen*, 429 U.S. at 594-95 (access to data was limited to small number of people that only reviewed the data twice in a twenty-month period). Another factor involves the status of the person alleging the infringement of privacy interests. Public figures, or individuals involved in public service, have opened their lives to public scrutiny. There is less probability of harm to a public figure. *See Nixon*, 432 U.S. at 455, 465.

71. The public interests in disclosure are varied and broad in scope. *See, e.g., Whalen*, 429 U.S. at 597-98 (public health interest minimizing the abuse of prescription drugs); *Nixon*, 432 U.S. at 462 (public has a recognized interest in preservation of public materials); *Van Bourg, Allen, Weinberger and Roger*, 728 F.2d at 1273-74 (public interest in gathering information about unlawful union election); National Association of Atomic Veterans, Inc. v. Director, Defense Nuclear Agency, 583 F. Supp. 1483, 1488 (D.D.C. 1984) (public interest in ascertaining effects of nuclear radiation on war veterans); Clug v. National Railroad Passenger Association, 425 F. Supp. 946, 951 (D.D.C. 1976) (public interest in information about individuals who receive compensation from public funds).

72. *Compare Minnis*, 737 F.2d at 787-88 (privacy interest outweighs commercial interest in disclosing names and addresses of applicants for permits to travel on a scenic river) *and Church of Scientology of California*, 611 F.2d at 747 (plaintiff's purpose to seek information regarding government investigation of plaintiff does not outweigh information about employment and personal history) *and Wine Hobby USA*, 502 F.2d at 137-38 (private commercial interest in disclosure of individuals licensed to produce wine for home consumption does not outweigh privacy interests) *and* Shaw v. U.S. Dept. of State, 559 F. Supp. 1053 (D.D.C. 1983) (privacy interest in documents detailing arrests and police interrogations outweigh plaintiff's interest in investigating President's assassination) *with Van Bourg, Allen, Weinberger and Roger*, 728 F.2d at 1273-74 (public interest in unlawful union election outweighs privacy interest in names of those eligible to vote) *and* National Association of Atomic Veterans, Inc. v. Director, Defense Nuclear Agency, 583 F. Supp. 1483, 1488 (D.D.C. 1984) (public interest in effects of atomic radiation on veterans outweighs privacy interest in names of those veterans participating in atomic tests) *and* Disabled Officer's Association v. Rumsfeld, 428 F. Supp. 454, 457-59 (D.D.C. 1977) (plaintiff's interest in increasing membership outweighs privacy interest of disabled officers in names and addresses) *and* Clug v. National Railroad Passenger Corporation, 425 F. Supp. 946, 951 (D.D.C. 1976) (public interest in information about persons compensated with public funds outweighs privacy interests in that information). *See generally* Kronman, *supra* note 51, at 729 n.13 (lists numerous decisions under FOIA's privacy exemption).

the information are both closely scrutinized.[73] Neither interest automatically outweighs the other.[74] Thus, in deciding to use such a balancing test, the courts presume that a true conflict exists between informational privacy and the need to collect and disseminate information. Second, the courts do not view the voluntary release of the information to the government as implying consent to disclose that information.[75] Even though an individual releases information, the individual does not release a blanket right to disseminate that information. Thus, an expectation of privacy in released information exists despite the voluntary disclosure of that information. These principles indicate that the courts are not paying mere lip service to privacy interests and allowing unwarranted disclosures of government held information. Individuals should be assured that their informational privacy interests will be protected when the privacy interest is strong enough to warrant protection. The balancing test reconciles the conflict between an individuals right to control information and the government's need to obtain information. The result for the individual is the receipt of benefits from the government and protection from clearly unwarranted invasions of privacy.

INFORMATIONAL PRIVACY AND NATIONAL IDENTIFICATION

The concept of a national identification system involving the use of a secure identifier arouses the fear of unprincipled information practices. It is alleged that because identification systems are always linked to record keeping and data collection, a national identifier would provide incentives to link records.[76] An individual identifier could make location of records easier and increase unwarranted disclosures. It is argued that the increase in administrative convenience that a national identification system provides would produce unprincipled incentives to gather greater amounts of information.[77] Such unjustified information practices, and the concommitant loss of control over personal information would, in fact, violate recognized informational privacy rights. An analysis of the actual impact of the use of a national identifier, however, indicates that

---

73. The Court in *Nixon* carefully examined all interests involved. *See Nixon*, 432 U.S. 459-65. In examining challenges to the use of the FOIA's privacy exemption, the competing interests are always scrutinized. *See Kronman, supra* note 51, at 760 (balancing test gives equal weight to both privacy interest and public purpose).

74. Kronman, *supra* note 51, at 760.

75. When an individual discloses information, for example on a welfare application, the individual does not necessarily consent to further disclosure of the information on the application.

76. RECORDS, *supra* note 11, at 111-12.

77. *See, Id.*, at 111 (the use of an identifier makes a womb to tomb dossier possible and would make it simple to trace, monitor and control an individual's behavior).

informational privacy is only minimally implicated.[78] Existing statutory regulations[79] will protect any privacy rights that the use of a

78. *See infra* notes 80-108 and accompanying text.

79. In general, The Privacy Act of 1974, 5 U.S.C. 552(a) (1982), evinces a broad Congressional recognition and concern for informational privacy. The Congressional findings stated:

> (1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal Agencies;
> (2) the increasing use of computers and sophicated information technology while essential to the efficient operation of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;
> (3) the opportunities for an individual to secure employment, insurance and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;
> (4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and
> (5) in order to protect the privacy of individuals identified in information systems maintained by Federal Agencies it is necessary and proper for Congress to regulate the collection, use, and dissemination of information by such agencies.

5 U.S.C. 552(a) (1982).

Section 552(a)(b) of the Privacy Act prohibits the disclosure of a record contained in a system of records that a federal agency maintains without the consent of the individual or pursuant to a written request from that individual.

There are twelve exceptions to the non-disclosure provision. *See Id.* at 552(a)(b)(1-12). Under the exceptions no consent is required if the disclosure (1) is to another employee in the agency that holds the record and the disclosure is pursuant to performance of employment, (2) is required under the Freedom of Information Act, (3) is for a routine use of the record, (4) is to the Census Bureau, (5) is for use as statistical data with all identifying characteristics of the information deleted, (6) is to the National Archives for historical use, (7) is to another agency for the purpose of civil or criminal law enforcement, (8) is for compelling health or safety reasons, (9) is to Congress, (1) is to the General Accounting Office, (11) is pursuant to a court order, or (12) is to a consumer credit agency pursuant to a debt collection statute.

While these exceptions to the consensual disclosure requirement of the Act do tend to provide an opportunity for disclosures, this comment focuses entirely on the "routine use" exception. The "routine use" exception is a broad exception and is the basis of most controversy involving the actual effect of the Act on informational privacy. *See* Ehlke, *The Privacy Act After a Decade*, 18 J. MARSHALL L. REV. 829, 831 (1985) (the routine use exception is broadly defined and there are minimal restraints on an agency's use of this exception). Further, five of the exceptions are inoffensive to privacy interests. *See* Project, *supra* note 22, at 1325 n.2118. The other six exemptions present potential problems, but none as great as the "routine use" exception. *See Id.* at 1325-26 (generally, he need for information under these exceptions is justified, or the harm to privacy interests is minimal).

The "routine use" exception sanctions disclosure of information between agencies the information disclosed is used "for a purpose for which it was collected." *Id.* at 552(a)(7). The government has used the "routine use" exception to sanction the computer-matching of records held in the databases of different agencies. Shattuck, *supra* note 44, at 1003. Computer-matching involves comparing unrelated computerized files, with the use of a computer, to detect a common or disparate element in the files compared. PRESIDENT'S COUNCIL ON INTEGRITY AND EFFICIENTCY, *Long Term Computer Matching Project, Questions on Computer Matching* 1 (July 1, 1982). Computer matching is a quick, cost effective and efficient means of detecting fraud in connection with various government programs. *Id.* Computer-matching, used to match social security benefit rolls against Medicare deceased patient records, detected 25 million dollars worth of error and fraud. Kusserow, *The Government Needs*

national identification system threatens. If the government evaded these regulations, the balancing test that the courts have used would extinguish any unwarranted invasions of informational privacy.

Acquisition of Information

Governmental information practices first implicate informational privacy upon the acquisition of personal information.[80] The acquisition of information is the initial disclosure. Identification is a necessary component in any transaction involving a computer-based record system[81] and the identifier thus becomes an integral element of the initial disclosure.

The initial disclosure of the identifier presents two potential areas of conflict with informational privacy interests. One area of conflict arises because the release of the identifier is a disclosure of information.[82] Any disclosure of information implicates informational privacy concerns. Secondly, a conflict arises because of the allegation that a national identification system sanctions widespread increases in information collection.[83]

The first potential area of conflict with informational privacy presents the question of whether the required disclosure of an identifier violates informational privacy. No statutory provision prohibits the government from requiring the disclosure of an identifier. Consequently, the balancing test the courts have adopted becomes applicable to determine the strengths of the competing interests. If the public purpose involved with the use of a national identifier outweighs the privacy interest at stake, then requiring the disclosure of a national identifier to the government would not violate informational privacy.

Computer Matching to Root Out Waste and Fraud, 27 COMMUNICATIONS IN THE ACM 542 (June, 1984). Computer-matching has been used in conjunction with a number of programs. *See generally* 1 *Computer Matching* 1-15 (July, 1982) (the newsletter presents a compilation of many state and federal computer-matching programs).

There is considerable controversy over the effect of computer matching programs on civil liberties. *Compare Shattuck*, *supra* note 39, at 1001-04, *and* Comment, *Computer Matching Programs: A Threat to Privacy?*, 15 COLUM. J.L. & SOC. PROBS. 143 (1979) *with* Kusserow, *supra*, at 542-45. Although reconciliation of the competing views is beyond the scope of this comment, this comment takes the position that the regulations placed on computer matching programs are sufficient to safeguard the informational privacy concerns associated with national identification. Thus, the Privacy Act's regulations are sufficient to protect the privacy interests associated with a national identification system.

80. *See supra* note 48 and accompanying text.

81. *See supra* notes 28-37 and accompanying text.

82. An identifier is a label that identifies an individual's record. *See supra* note 28. The information content of the identifier is equal to that of any other existing identifier such a name or social security number.

83. *See* RECORDS, *supra* note 11, at 111-12.

The balancing test first examines the probability of harm to privacy interests. In this case, the probability of harm to privacy interests that is associated with the mere release of identifier information is minimal. First, the release of the identifier upon the collection of information involves a single, limited disclosure.[84] When disclosure is quantitatively limited, the probability of harm is reduced. Informational privacy protects against injuries associated with the disclosure of information.[85] The greater the extent of the disclosure, the greater the potential for harm. A single transaction involving the mere release of an identification number presents an extremely limited risk of harm because the disclosure is so minimal.

The lack of highly personal information in the identifier itself further limits the probability of harm. The identifier itself is an impersonal label that contains no personal information,[86] and merely accompanies the release of information. Because it is the personal content of information that creates a risk of harm to informational privacy interests,[87] the national identifier itself does not present a strong probability of harm to privacy interest. Disclosure of the identifier does not involve a disclosure of personal information.

After the probability of harm to privacy interests is examined, the public purposes underlying the use of a national identification system are examined. Eliminating the economic cost of identification fraud is the main purpose for creating a uniform national identification system.[88] The economic cost to society, 24 billion dollars a year,[89] indicates the strength of the purpose. Another purpose behind national identification is to attack identification fraud, which is a criminal activity.[90] The public interest in minimizing criminal activity, is at the very least, an important purpose. Other benefits associated with the adoption of a national identification system, such as the efficient collection of information and the administrative convenience of uniform identification systems,[91] also lend strength to the public purpose.

It is apparent that the public purpose outweighs the probability of harm to privacy interests. The probability of harm to privacy interests is minimal and there are important public purposes. Clearly unwarranted invasions of privacy do not result from disclosure of a

---

84. The disclosure, accompanying the release of other information, is singular. The disclosure is only to one individual agency, and at this point, is not subject to dissemination beyond that agency.

85. *See supra* notes 49-55, 68 and accompanying text.

86. *See supra* note 11.

87. *See supra* notes 63-67 and accompanying text.

88. *See supra* notes 2, 11, 36-37 and accompanying text.

89. *See supra* note 2 and accompanying text.

90. *See supra* note 1 and accompanying text.

91. *Westin, supra* note 43 and accompanying text.

national identifier. Therefore, the adoption of a national identification system does not violate the informational privacy rights associated with the use of a national identifier for identification purposes.

The use of a national identifier as a sanction for unwarranted information collection is the second potential area of conflict with informational privacy. Should the government desire to use a national identifier as a tool to collect more information, the government must first comply with the "relevance" and "need" standards of the Privacy Act of 1974.[92] The Privacy Act requires agencies to maintain "only such information as is *relevant* and *necessary* to accomplish a purpose of the agency required to be accomplised by statute or by executive order of the President."[93] An agency cannot collect irrelevant and unnecessary information. These standards effectively place all federal agencies on notice that it is necessary to justify requests for information. Therefore, the "need" and "relevance" standards prevent unprincipled informational requests and would apply in the event that a national identification system were adopted. Given the awareness that the courts and Congress evince towards informational privacy,[94] a national identifier system could not serve as a sanction for unprincipled increases in information collection.

A national identification system, as it relates to the disclosure of the identifier, does not violate informational privacy. Nor could such a system provide a sanction for unwarranted increases in information collection. Therefore, an individual's informational privacy is protected when a national identifier is released during the acquisition of information.

Disclosure of Information Within the Federal Government

A national identifier is associated with intergovernmental information discloses because the identifier is the means by which the government identifies a requested record.[95] A uniform national identification system promotes the efficiency and ease of disclosing records.[96] An identifier also provides an easy means of linking records associated with an individual.[97] Commentators, therefore,

92. See 5 U.S.C. 552a(3)(1) (1982).

93. *Id.* The "relevance" and "need" standards have been the subject of criticism. *See generally*, Project, *supra* note 22, at 1305-10 (the relevance and need standards are unsatisfactory standards and do not limit the collection of information). It should be noted, however, that the probability of harm to privacy interests upon the initial disclosure of information is limited. *See* note 84 and accompanying text.

94. *See supra* notes 59-75, 79, and accompanying text.

95. The identifier is part of the identification system. *See supra* notes 28, 36-39 and accompanying text.

96. RECORDS, *supra* note 11, at 111.

97. *Id.*

assert that this will lead to increasingly unprincipled disclosures.[98] The Privacy Act of 1974, however, regulates governmental information practices[99] and any disclosures that a national identification system promotes are subject to the Act's regulations.

A national identifier has the greatest potential for increasing disclosures through the use of the identifier in conjunction with computer-matching programs. Computer-matching involves numerous disclosures of information without notice to the individual concerned.[100] While a uniform identifier might increase the efficiency and ease with which a computer-match was conducted, a higher level of ease and efficiency would not necessarily increase matching programs.

Agencies contemplating the use of computer-matching are subject to numerous regulations.[101] Agencies are requires to conduct scope and purpose research and must estimate the costs and benefits of a proposed matching program.[102] The agency is required to verify all information gained from a match in order to avoid errors in subsequent administrative actions.[103] Public notice of the intent to conduct a computer match is published in the Federal Register.[104] An individual whose records are subject to disclosure through a computer-match has constructive notice that his/her records will be disclosed.

These regulations apply whether the means of identification is with a uniform identifier or another identification system. The regulations prevent agencies from conducting computer-matches without justification.[105] A national identification system, therefore, could not automatically increase intergovernmental disclosure of records.

If, for some reason, the government used the national identifier to conduct unjustified matching programs, the courts would prohibit the programs. The courts, using the accepted balancing test, would closely examine the public purpose and probability of harm to privacy interests in any challenged program. An unjustified matching program necessarily has little, if any, public purpose. There is a strong probability of harm to privacy interests, however, because personal information is released in a computer-match. The courts, in

---

98. *See Id.* at 111-12 (a permanent identification number provides incentives to link records).

99. *See supra* note 79.

100. *See supra* note 79.

101. *See* PRESIDENT'S COUNCIL ON INTEGRITY AND EFFICIENCY, LONG TERM COMPUTER MATCHING PROJECT, QUESTIONS ON COMPUTER MATCHING 7-8 (listing Office of Management and the Budget guidelines).

102. *Id.*

103. *Id.*

104. *Id.*

105. Kusserow, *supra* note 79, at 544.

balancing these interests, would hold that the privacy interest outweighs the public purpose. Thus, a national identification system could not become a tool for unjustified intergovernmental disclosures of personal information.

Disclosure of Information to the Public

Litigation under the Freedom of Information Act's (FOIA) privacy exemption indicates that the courts carefully scrutinize all interests involved when a disclosure of information to the public may constitute a clearly unwarranted invasion of personal privacy.[106] A national identification system may facilitate the ease with which the government can locate requested information,[107] but disclosures that violate informational privacy will not occur just because it is easier to access information.

The FOIA applies to any requests from the public for information contained in government files. Numerous judicial interpretations of the privacy exemption indicate that informational privacy interests are closely scrutinized and balanced against the public interest in disclosure.[108] The courts are aware of the potential harm that can result from the public dissemination of highly personal information and actively prohibit such disclosures.

A national identification system would have no impact on a court's determination of whether privacy interests prohibit disclosure. Even if a national identifier facilitated the ease of locating requested information, that information becomes subject to the existing balancing test. Therefore, a national identification system would not change the status of information practices in the area concerning the disclosure of information to the public.

CONCLUSION

The fears associated with national identification and informational privacy are without substance. A national identifier does not infringe informational privacy *per se* because there is no personal information in the number itself. The only possible privacy implications involved arise through the use of the number as a tool to facilitate unjustified and unwarranted collection and disclosure of information. Existing statutory regulations and judicial scrutiny, however, prohibit uncontrolled and unprincipled information acquisition and dissemination. These limitations on government information practices apply to any change in information practices that a

106. *See supra* notes 59-75 and accompanying text.
107. *Westin*, *supra* note 11, at 398.
108. *See supra* notes 60-75 and accompanying text.

national identification system would produce. Furthermore, these limitations protect individuals from injuries associated with the violation of informational privacy. A national identification system would improve the efficiency, accuracy and integrity of existing government information practices without sacrificing informational privacy rights. A national identifier would not necessarily increase information collection, but would curtail identification fraud and its associated economic costs. The protections afforded to information privacy are sufficient to justify the creation of a national identification system.

Eric Grossman