UIC John Marshall Journal of Information Technology & Privacy Law

Volume 16
Issue 3 *Journal of Computer & Information Law - Spring 1998*

Article 2

Winter 1997

We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers, 16 J. Marshall J. Computer & Info. L. 529 (1998)

Flavio L. Komuves

WE'VE GOT YOUR NUMBER: AN OVERVIEW OF LEGISLATION AND DECISIONS TO CONTROL THE USE OF SOCIAL SECURITY NUMBERS AS PERSONAL IDENTIFIERS

by FLAVIO L. KOMUVES†

TABLE OF CONTENTS

† B.A., Rutgers University (Rutgers College); J.D., *summa cum laude*, Seton Hall University School of Law; member of the bars of New Jersey and Pennsylvania.

I. INTRODUCTION

In 1890, Professors Louis D. Brandeis and Samuel D. Warren wrote an article in the *Harvard Law Review* lamenting the decline of protections for the privacy of individuals.[1] "The right to be let alone," as they described it, was an important one.[2] Advances in technology, they claimed, threatened the right to privacy, and the law should protect individuals from such intrusions.[3] Accordingly, the authors declared that "[r]ecent inventions and business methods call attention to the next step which must be taken for the protection of the person."[4] If such protections were necessary in the 19th century, it follows that these protections are even more necessary today.[5] The existence of computers with mas-

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

2. *Id.* at 193.

3. *See id.* at 195.

4. *Id.*

5. *See* Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 3 (1996) ("Despite almost fifty years of experience with the information-management ability of computers, society has not yet reformulated traditional notions of privacy, which restrict third-party access to personal information, to accommodate the tremendous storage capacity and instantaneous retrieval ability afforded by computers.").

sive data storage capabilities, and perhaps more importantly, the interrelatedness of computer networks, allows for the storage and sharing of information on individuals in an unprecedented way.[6] However, in the face of this technology, individuals still maintain certain rights—both legally and morally—to informational privacy.[7] This paper deals with a subset of those issues—the use of personal identification numbers ("PIN"s) to identify people and keep track of personal records.

In the United States, a person's social security number ("SSN")[8] has

6. *See generally* WARREN FREEDMAN, THE RIGHT OF PRIVACY IN THE COMPUTER AGE (1987); JOHN M. CARROLL, CONFIDENTIAL INFORMATION SOURCES (1991). For another overview of the law of informational privacy in the face of technological advances, *see* Hon. Ben F. Overton & Katherine E. Giddings, *The Right of Privacy in Florida in the Age of Technology and the Twenty-First Century: A Need for Protection From Private and Commercial Intrusion*, 25 FLA. ST. L. REV. 25 (1997).

7. Testifying before Congress in 1976, Arthur Miller stated:

> I think if one reads Orwell and Huxley carefully, one realizes that '1984' is a state of mind. In the past, dictatorships have always come with hobnailed boots and tanks and machine guns, but a dictatorship of dossiers, a dictatorship of databanks can be just as repressive, just as chilling and just as debilitating on our constitutional protections. I think it is this fear that presents the greatest challenge to Congress right now.

SOURCE BOOK ON PRIVACY 256 (Joint Comm. Print 1976), *quoted in* Judith Beth Prowda, *Privacy and Security of Data*, 64 FORDHAM L. REV. 738, 743 (1995).

8. A person receives a Social Security Number by filing a completed application with the Social Security Administration (Form SS-5). *See* 20 C.F.R. § 422.103(b) (1996). At that time, the Social Security Administration issues a Social Security card and number to the applicant. The card is made of bank note paper and, supposedly, cannot be counterfeited. *See* 42 U.S.C. § 405(c)(1)(D) (1994); Alexander C. Papandreou, *Krebs v. Rutgers: The Potential for Disclosure of Highly Confidential Personal Information Renders Questionable the Use of Social Security Numbers as Student Identification Numbers*, 20 J.C. & U.L. 79, 79 n.2 (1993). The nine-digit Social Security number contains three parts. The first three numbers, called the Area Portion, are where the individual applied for the SSN (before 1972) or resided at time of application (after 1972), in the following table:

attained the status of a quasi-universal personal identification number.[9] As early as 1974, when Congressional committees were considering the adoption of the Privacy Act, they referred to the extensive use of SSNs as a key area of concern:

> [I]n its report supporting the adoption of the [Privacy Act], the Senate Committee stated that the extensive use of SSNs as universal identifiers is "one of the most serious manifestations of privacy concerns in the nation."[10]

Poll results confirm the Committee's findings. On a more general level, more than eighty percent of Americans are either "very concerned" or "somewhat concerned" about privacy issues.[11] It may come, perhaps,

000 unused	035-039 RI	212-220 MD	247-251 SC	318-361 IL
001-003 NH	040-049 CT	221-222 DE	252-260 GA	362-386 MI
004-007 ME	050-134 NY	223-231 VA	261-267 FL	387-399 WI
008-009 VT	135-158 NJ	232-236 WV	268-302 OH	400-407 KY
010-034 MA	159-211 PA	237-246 NC	303-317 IN	408-415 TN
416-424 AL	449-467 TX	503-504 SD	520 WY	530 NV
425-428 MS	468-477 MN	505-508 NE	521-524 CO	531-539 WA
429-432 AR	478-485 IA	509-515 KS	525 NM	540-544 OR
433-439 LA	486-500 MO	516-517 MT	526-527 AZ	545-573 CA
440-448 OK	501-502 ND	518-519 ID	528-529 UT	574 AK
575-576 HI	586 Pac.Isl.*	600-601 AZ		
577-579 DC	587-588 MS	602-626 CA		
580 VI	589-595 FL			
581-584 PR	596-599 PR			
585 NM				

627-699 unassigned, for future use
700-728 Railroad workers through 1963, then discontinued
729-899 unassigned, for future use
900-999 not valid SSNs, but were used for program purposes when state aid to the aged, blind and disabled was converted to a federal program administered by SSA.
* Guam, American Samoa, Northern Mariana Islands, Philippine Islands
The second part of the number, containing two numbers, is called the Group Portion and is a 'check-sum' on the validity of the number. The Social Security Administration routinely publishes a list of the highest group assigned for each SSN Area. The order of assignment for the Groups is: odd numbers under 10, even numbers over 9, even numbers under 9 except for 00 which is never used, and odd numbers over 10. The third part of the number, containing four numbers, is called the Serial Portion is assigned strictly in order, and has no specific meaning. Number 0000 is never assigned.

See also Computer Professionals for Social Responsibility (visited Jan. 6, 1998) <http://psr.org/cpsr.privacy/ssn/ssn.structure.html> (citing Social Security Administration Pub. No. 05-10633).

9. *See* DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 78 (1989). *See also* William H. Minor, *Identity Cards and Databases in Health Care: The Need for Federal Privacy Protections,* 28 COLUMB. J.L. & SOC. PROBS. 253, 261-71 (1995).

10. International Bhd. of Elec. Workers Local Union No. 5 v. United States Dept. of Housing & Urban Dev., 852 F.2d 87, 89 (3d Cir. 1988) (quoting S. Rep. No. 1183, 93rd Cong., *reprinted in* 1974 U.S.C.C.A.N. 6916, 6943).

11. FLAHERTY, *supra* note 9, at 7. The number has grown over time. In 1976, for example, the number of people reporting they were "very concerned" or "somewhat concerned"

from the historically individualistic nature of the American psyche. It may also come about from people learning of incidents in which individuals' privacy was blatantly invaded. In any event, what is clear is that Americans are concerned about their lack of privacy.

Despite the public's apprehension, there is an alarming lack of legal response to privacy concerns. When one considers the privacy issues discussed in this paper—the use and abuse of SSNs—this lack of response seems anomalous indeed. The need for a legal response is pressing, when one takes into account the poll figures, the very real problems that may arise from SSN abuse, and the problems attendant to the modern technology that allows the interlinking of databases.[12] The United States should consider the example of other Western democracies that, although using PINs, have seriously controlled and limited their use and dissemination. The steps taken by France[13] and Canada[14] are good ex-

---

was only forty-seven percent. *Id.* *See also* William J. Fenrich, Note, *Common Law Protection of Individuals' Rights in Personal Information,* 65 FORDHAM L. REV. 951, 955 n.32 (1996) (noting that eighty percent of Americans agree that "consumers have lost all control over how personal information about them is circulated and used by companies"); *Id.* at 961 (stating that over ninety percent favor regulating business' usage of consumer information).

12. As a result of this ever-increasing interconnectedness, a person can easily collect information from several different databases, a process known as "data mining." *See* A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases,* 15 J.L. & COMM. 395, 400 (1996). The easy way in which this information can be obtained has the potential to severely restrict the "economic and possibly even the political freedom of the persons profiled" in these records. *Id.* The process of data mining is made much easier when the records in the multiple databases are retrievable a single identifier, such as a SSN. *See generally id.* at 483-91 (describing the interlinking of databases). In 1974, Justice Douglas examined the interconnectedness problem, as it existed then, and its relationship to the extensive use of SSNs. *See* California Bankers Assn. v. Shultz, 416 U.S. 21, 85 (1974) (Douglas, J., dissenting). Douglas explained the following:

> [T]hat by getting access to a person's bank checks, an investigator gets to know his doctors, lawyers, creditors, political allies, social connections, religious affiliations, educational interests, the papers and magazines he reads, and so on *ad infinitum.* These are all tied to one's social security number; and now that we have the data bank, these other items will enrich the storehouse and make it possible for a bureaucrat—by pushing one button—to get in an instant the names of the 190 million Americans who are subversives or potential and likely candidates.

Id. Justice Douglas also gave another spirited condemnation of SSN use in light of interlinked databases in *Doe v. McMillan,* 412 U.S. 306, 329 (1973) (Douglas, J., concurring). Notably, Justice Douglas has been the only Supreme Court Justice to address SSN use and abuse in judicial opinions.

13. France keeps a National Identification Register ("NIR") which includes a personal identifying number. *See* FLAHERTY, *supra* note 9, at 229. Nevertheless, privacy advocacy in France has led to relatively tight controls on usage. *See id.* at 231. There, a highly independent National Commission on Informatics and Freedoms ("CNIL"), on which no member of the executive branch of government can serve, oversees use of the NIR. *See id.* at 182, 229-31. The CNIL has acted frequently to restrict widespread use of personal identifi-

amples of what might be done in such situations.

Actual problems that have already arisen from the misuse of SSNs provide an independent and sufficient basis for court or legislative action to control the use of these numbers. Cases of "identity theft," i.e. the use of one person's SSN by another have become common. For example, in one case, a woman sued her sister-in-law, alleging that the latter had stolen her social security number and used it to obtain credit at a retail store.[15] As a result of the theft of the number, the sister-in-law was able to obtain a credit card, which balance due she never paid, and the plaintiff suffered "economic hardship and damage to her credit."[16] In other cases, criminals who use another's SSNs for financial gain have caused more than just financial losses for the true holder of that SSN.[17] In addition, public employees with access to government computers have also been sanctioned after illegally accessing SSNs to perpetrate fraud.[18]

---

ers by both government and private actors, in order to avoid the number becoming used in "interconnecting data banks" which would lead to "enclosing the individual in a network of surveillance, leading to a Surveillance Society." *Id.* at 230.

14. In Canada, the "Social Insurance Number" ("SIN") which each citizen is assigned, has become "the most common numerical identifier in [that] country, the equivalent to the [SSN] in the United States." FLAHERTY, *supra* note 9, at 281. Outcry about the use and abuse of SIN led to 1988 legislation which eliminated most uses of the SIN, despite a cost to the government of over sixteen million Canadian dollars. *See id.* at 283. Thus, unless there is specific approval by the Canadian Parliament or Treasury Board, SIN collection is prohibited, individuals must be explicitly told of their right to refuse to provide their SIN, and government services may not be withheld upon a refusal to provide a SIN. *See id.* at 283-84. The government plans to institute similar controls on SIN use in the private sector. *See id.* at 284. To date, however, only Quebec has passed such legislation. *See* Overton & Giddings, *supra* note 6, at 52. In sum, Canada's efforts to protect citizens' privacy "are almost without precedent internationally as an effort to cut back on surveillance of the public." FLAHERTY, *supra* note 9, at 284.

15. Laracuente v. Laracuente, 599 A.2d 968 (N.J. Law Div. 1991).

16. *Id.* at 969.

17. One victim of identity theft gave this account of the consequences in a sentencing proceeding before a federal district court in Texas:

> It has been extremely difficult for me to begin the new school year with the emotional strain of dealing with all aspects of this situation. It has cost me in terms of multiple times off work to appeal in J.P. Courts to explain and defend my position, to research our credit reports and to make literally hundreds of phone calls to explain my situation to the merchants and collection agencies who accepted the fraudulent checks given by Wendy Wells using my name and Social Security number. Each week I have faced the possibility of additional unjust arrest warrants in my name stemming from Wendy Well's [sic] fraudulent use of my name. For my own protection, I am being forced to carry a forgery affidavit with me at all times to prevent an unfair arrest. It is overwhelming that someone can take over one's identity so quickly.

United States v. Wells, 101 F.3d 370, 372 (5th Cir. 1996).

18. *See* United States v. Smaw, 22 F.3d 330 (D.C. Cir. 1994) (FTC employee convicted of accessing personal files with SSNs therein to obtain fraudulent credit cards). *See also infra* note 47 (Medicaid workers criminally punished after their illegal sales of SSNs from their office's computer files).

Indeed, identity theft is not the only type of problem. Good-faith but negligent errors made by companies who use SSNs to maintain credit records also harm citizens. In one case, a credit report erroneously alleged that a Missouri couple filed for bankruptcy. When this information was distributed to other businesses, the couple's available credit was frozen. Eventually, the financial hardship caused by this erroneous information caused the couple to *in fact* file bankruptcy.[19] In a similar vein, a federal court issued an arrest warrant for a named individual, but erroneously placed another person's SSN on the warrant. When the United States Marshals Service executed the warrant, they arrested the person whose SSN, not name, matched the warrant. The person who was erroneously arrested filed suit against the Marshals Service, but the court held that since the Marshals Service relied in good faith on the SSN, there was no cause of action.[20] Thus, the error in the SSN, and the blind reliance on the SSN by the officers, caused the arrest of an innocent person who had no subsequent remedy available.

Even without tangible consequences from SSN misuse, people dislike the notion that "Big Brother is Watching [Them]"[21] through the use of SSNs. A chilling effect on personal freedom is sure to ensue when people's buying and travel habits, family life, or finances, can be tracked so easily and exchanged among various database keepers. All of this tracking, of course, is made immensely easier through the use of personal identifying numbers.[22]

Nonetheless, SSN use is so important to business and government in this country that a person who is assertive about their privacy rights may find herself in a position in which another will refuse to do business with her unless she furnishes her SSN.[23] In light of the fact that SSN use is so favored, only a few and relatively weak statutes limit the use, dissemination, and requesting of the social security number.

---

19. *See* Prowda, *supra* note 7, at 742 n.245.

20. *See* Rodriguez v. United States, 54 F.3d 41, 48 (1st Cir. 1995).

21. GEORGE ORWELL, 1984 (1949).

22. *See* Elaine M. Ramesh, *Time Enough? Consequences of Human Microchip Implantation*, 8 RISK: HEALTH SAFETY & ENVIRONMENT 373, 378-80 (1997). One of the prime concerns associated with a national personal identifying numbers like the SSNs is that "requiring each citizen to carry a government number is another step along the path of treating people as a national resource, which means government property, whereas the liberal democratic view has always been that government is the people's property." *Id.* at 380 (footnotes and internal quotations omitted).

23. *See, e.g.*, Rudy Larini, *Vanishing Privacy—Databanks Know More on Americans Than They Think*, STAR-LEDGER (Newark, N.J.), Jan. 5, 1992, *available in* 1992 WL 11055180 (asserting that one man spent nine months trying to convince a health insurance company to sell him insurance after he refused to furnish the company with his SSN). The company relented after the man furnished them with a unique nine-digit number—the SSN of his late grandfather. *See id.*

To explore this problem more fully and suggest some responses, Part II of this article identifies areas in which both private individuals and the government request, utilize, or disseminate social security numbers. This article shows how different legal frameworks govern each of these acts with respect to SSNs.[24] Part III examines legal limitations on the requesting, use, and dissemination of SSNs from statutory or decisional law. Finally, Part IV recommends the strengthening of certain federal and state laws in order to limit the abuse of SSNs or other personal identifying numbers.

II. USES OF SOCIAL SECURITY NUMBERS

In this Part, different ways in which private persons and government utilize the SSN as an identifier are explored. While some of the uses are required by law, others arise from voluntary choices made by the keeper of the database. In addition, discussion will include specific problems that may arise from each of these categories of use.

A. USE BY PRIMARILY PRIVATE SOURCES

1. *Financial Information*

In an effort to learn and share financial information about Americans, companies trading in financial information are the largest private-sector users of SSNs[25] and it is these companies that are among the strongest opponents of SSN restrictions.[26] For example, credit bureaus maintain over 400 million files, with information on almost ninety percent of the American adult population.[27] These credit bureau records are keyed to the individual SSN.[28] Such information is freely sold and

24. *See* Prowda, *supra* note 7, at 748-50 (distinguishing between information collectors, information users, and information providers).

25. *See* Steven A. Bibas, *A Contractual Approach to Data Privacy*, 17 HARV. J.L. & PUB. POLICY 591, 593-95 (1994).

26. The American Banking Association's response to recent FTC proposals to limit SSN usage is indicative of the importance of SSN usage to the financial community. The trade group warned that further government requirements on SSN confidentiality "threaten[ed] to ensnare banks and other information-sensitive businesses in a tighter regulatory web." *See* Richard L. Field, *The 1996 Survey of the Year's Developments in Electronic Cash Law and the Laws Affecting Electronic Banking in the United States*, 46 AM. U. L. REV. 967, 1006 (1997).

27. *See* Bibas, *supra* note 25, at 593.

28. *See* RAYMOND T. NIMMER, THE LAW OF COMPUTER TECHNOLOGY ¶ 16.17[2] (2d ed. 1992). *See also* Trans Union Corp. v. Federal Trade Comm'n, 81 F.3d 228, 229 (D.C. Cir. 1996). The Trans Union Corporation, one of the largest credit reporting agencies in the country, maintains a database known as CRONUS, to facilitate marketing efforts on behalf of credit card issuers. The CRONUS database contains the following:

> [A] variety of information, such as name (and aliases), social security number, addresses, phone numbers, occupation, gender, ethnic background, marital status,

traded, virtually without legal limitations.[29] Moreover, "most banks and lending institutions use the [SSN] as the method of identifying certain persons."[30] Other types of financial information may also be freely collected. One example of this would be some states' requirements, in their codification's of the Uniform Commercial Code, that mandate a person who publicly files a security interest under Article 9 of the Code, to include the debtor's SSN.[31]

2. *Education*

Universities, particularly ones with a large student body, frequently

---

and education. It also contains information on the listed person's credit history on any credit account.

Id. In overturning Federal Trade Commission ("FTC") restrictions on the use of this information, the *Trans Union* court noted that the FTC had, in the past, allowed a competitor of Trans Union, TRW, to "market lists from its credit reporting database based on such 'identifying information' as name, zip code, age, social security number, or substantially similar identifiers." *Id.* at 232.

29. *See* Bibas, *supra* note 25, at 594 (explaining that it is "routine" for credit bureaus to sell financial information to other companies for marketing purposes). *See also* Scott Shorr, Note, *Personal Information Contracts: How to Protect Privacy Without Violating the First Amendment*, 80 CORNELL L. REV. 1756, 1785 (1995) (noting that federal law "permits credit bureaus and their customers to exchange large quantities of information with impunity"). Late in 1997, the major credit bureaus announced a plan of self-regulation to curtail some of the more egregious instances of the availability of personal information. For example, these companies have promised that they will not distribute SSNs to the general public, nor allow the general public to run searches on individuals using SSNs as a search term. *See* National Assn. of Attorneys General: Consumer Protection Report, Jan. 1988, at 17. Frankly, this proposal is laughable. First, a breach of these promises is not punishable by legal or regulatory sanction. Second, by restricting only the "general public" in access to information, they do nothing to curtail the exchange of personal information among businesses or government agencies using their services. Finally, to the extent these companies include "public records and publicly available information" among services they sell, nothing in their promises "limits[s] the potential harm that could stem from access to and exploitation of sensitive information" in such documents. *Id.* at 17.

30. Jeffrey A. Taylor, *Medical Process Patents and Patient Privacy Rights*, 14 J. MARSHALL J. COMPUTER & INFO. L. 131, 141 n.75 (1995). *See also* Bibas, *supra* note 25, at 594 ("[b]anks maintain comprehensive files on their customers' financial transactions.") (footnote omitted).

31. *See, e.g.* ALA. CODE § 7-9-307(4)(d) (1975) (stating that the SSN or Federal taxpayer identification number of a borrower must appear on the financing statement). *See also* Harry C. Sigman, *Putting Uniformity Into—And Improving the Operation of—the Uniform Commercial Code: The New National Financing Statement Form*, 51 BUS. LAW 721 (1996). Sigman points out that although the UCC's version of Article 9 does not require that SSNs appear on filed documents, several states do provide for it. Still, the practice is condemned as "not . . . totally reliable and . . . not a viable alternative to a search by debtor name." *Id.* at 730. *See also* 7 U.S.C. § 1631 (c)(4)(D) (requiring SSNs on certain agricultural financing statements).

use social security numbers as student identifying numbers.[32] By using a number, these schools believe that they can better coordinate internal recordkeeping. Additionally, most, if not all of the agencies that administer standardized tests such as the Scholastic Aptitude Test ("SAT") or the Law School Admissions Test ("LSAT") request a person's social security number upon registration. These agencies, therefore, use the social security numbers for both internal purposes and sending the data to the schools that receive the data. In addition, some schools place SSNs on their student disciplinary records.[33]

3. *Blood Donations*

Recent amendments to federal law have authorized states and private entities that collect blood donations to collect the SSNs of donors as identifying numbers.[34] Moreover, the law also authorizes states to require furnishing the SSN as a condition for donating blood.[35] While this provision may have some value in determining which donors should be excluded from donating blood because of disease, this practice can lead to unforeseen invasions of privacy. *Coleman v. American Red Cross* is illustrative of just such a situation.[36] In *Coleman*, a recipient of donated blood contracted Acquired Immune Deficiency Syndrome ("AIDS") from the donor.[37] During discovery, the court ordered the Red Cross to furnish records about the donor, "with all information that would identify the donor redacted."[38] Nevertheless, the Red Cross inadvertently failed to strike out the donor's SSN on one of the documents produced.[39] Thereafter, the plaintiff's attorney hired a private investigator, who determined the donor's name and address, using only the SSN.[40] After an adverse ruling from the district court, the Sixth Circuit granted permission to the attorney to use this information to file suit against the do-

32. *See* Papandreou, *supra* note 8, at 82. This practice is true not only of private universities and colleges, but public ones as well.

33. *See* Florida State Univ. v. Hatton, 672 So. 2d 576, 577 (Fla. Dist. Ct. App. 1996) (explaining that disciplinary records were kept in each student's university records, and included SSNs). The *Florida State* court ultimately decided that since these individual records contained such personal information, they were protected from disclosure under Florida privacy statutes unless the party seeking disclosure could show a substantial need for them. *See id.* at 580. Accordingly, the court ordered the university to produce only summaries of the records, without identifying information. *See id.*

34. *See* 42 U.S.C. § 405(c)(2)(D) (1994).

35. *See id.*

36. 23 F.3d 1091 (6th Cir. 1994).

37. *See id.* at 1093.

38. *Id.* at 1094.

39. *See id.*

40. *See id.*

nor.[41] In sum, a rather significant breach of privacy—the disclosure of the donor's disease—resulted from a mere inadvertent release of a SSN.[42]

4. *Medical Records*

Through a Massachusetts' organization known as the Medical Information Bureau, the medical records of millions of United States residents, which almost always includes the SSN, are maintained and exchanged.[43] Some states, in addition, maintain their own medical records. For example, Florida maintains a list of residents who seek help for alcohol or substance abuse, indexing the list by the patient's SSN.[44] In contrast, Georgia protects the SSNs within minors' medical records when the minors apply for judicial consent to abortions.[45]

The use of the SSN in the context of medical records is likely to continue. In 1996, Congress passed health insurance legislation that requires standards for developing a "standard unique health identifier" for each individual.[46] In response to privacy concerns, however, Congress also provided for severe penalties for wrongful disclosure of medical information, including the "unique health identifier."[47] While many fear that the "unique health identifier" and the SSN will be the same number,

41. *See Coleman*, 23 F.3d at 1094 (citing *Coleman v. American Red Cross*, 979 F.2d 1135, 1141 (6th Cir. 1992)). The Sixth Circuit ruled that even though the attorney's conduct violated a protective order concerning that information, it was improper to dismiss the case under Rule 41(b) of the Federal Rules of Civil Procedure. *See id.* at 1095 ("Admittedly, the attorney's actions in this case were . . . egregious . . . however this does not mandate that the attorney's conduct be imputed to the [plaintiffs]"). The appeals court, however, authorized the district court to sanction the attorney personally. *See id.* at 1096.

42. *See id.* at 1095 n.2 (setting forth press coverage of the court's earlier ruling).

43. *See* Bibas, *supra* note 25, at 594 (stating that the MIB keeps records on over fifteen million Americans); Taylor, *supra* note 30, at 141 n.77. The MIB shares these medical records with all its member organizations, which include over 700 insurance companies. *See id.* (citation omitted). In addition to these insurance companies, federal and state governments which need to access a patient's medical information also do so through use of the SSN. *See id.* at 141 n.75.

44. *See* Craig S. Palosky & Doug Stanley, *Computer Full of Secrets*, TAMPA TRIB., Feb. 18, 1997, *available in* 1997 WL 703560 and 1997 WL 703565 (reporting the concerns over the confidentiality of medical lists such as this one that are indexed by SSN). Florida requires every hospital to report, *inter alia*, the SSN of "every patient." *Id.* Violating the confidentiality of these lists is a criminal offense under both federal and Florida law, but "arrests and prosecutions are rare" despite known incidents where medical records have been disclosed. *Id.*

45. *See* Ga. Code § 15-11-114(b) (1981 & Supp. 1997).

46. 42 U.S.C.A. § 1320d-2(b) (West Supp. 1997).

47. *Id.* § 1320d-6. The maximum penalty is a $250,000 fine and ten years' imprisonment. *See id.* State laws may also cover the wrongful disclosure of information. For example, the Maryland attorney general indicted twenty-four people for selling or receiving the names and SSNs of Medicaid recipients to health insurance companies. *See* Paul W. Valen-

there are alternatives.[48] For example, a separate and unique number could be assigned for health records.

Of course, the listings above can only scratch the surface of private collection and dissemination of SSNs.[49] Even among private users of SSNs, it is plain that the SSN's status as a personal identifying number is widespread.[50]

B. Use by Primarily Governmental Sources

1. *Taxes and Employment*

The tax records of both federal and state governments are keyed to SSN for individuals and a Federal Tax Identification Number ("FEIN") for businesses and other entities. The Internal Revenue Code stipulates that a SSN is the primary identifying number for individuals who file returns.[51] In addition to individuals filing returns, a taxpayer must also include the SSN of any dependent for whom the taxpayer claims a deduc-

---

tine, *Medicaid Bribery is Alleged; Workers for HMOs and Md. Implicated*, Washington Post, June 14, 1995, *available in* 1995 WL 2098620.

48. *See* Lawrence D. Gostin, *Health Information Privacy*, 80 Cornell L. Rev. 451, 459-61 (1995); *see also* Minor, *supra* note 9, *passim*.

49. One recent example involved political fund-raisers who have been accused of compiling personal information on donors, which included their SSNs. *See* Richard A. Ryan, *White House Workers May Have Broken Privacy Laws: Indictments Could Follow if Evidence is Found in Fund Probe*, Detroit News, Feb. 23, 1997, *available in* 1997 WL 5579188 (stating that members of the Democratic National Committee obtained personal information, including SSNs, from a White House database, in violation of the federal Privacy Act). In another bizarre case of disclosing SSNs in order to obtain political advantage, the Governor of Rhode Island released bank depositors' account information including SSNs to the media, in order to encourage passage of legislation providing compensation to depositors in closed state banks and credit unions. *See* Pontbriand v. Sundlun, 699 A.2d 856 (R.I. 1997).

50. One of the most extensive uses of personal data in the private sector is the exchange of consumer information for marketing processes. It is unclear whether these records generally include SSNs. *See* Fenrich, *supra* note 11, at 955-56. Yet, the frequent exchange of personal information by marketers—free of regulation—remains of the greatest areas of general concern by privacy advocates. *See id.* Thus, "[d]espite the apparent public concern over unauthorized uses of personal information, it remains legal to disseminate [it] without first obtaining the consent of the subject . . . . The direct marketing industry is not subject to any regulation at all." *Id.* at 956. The United States Privacy Protection Commission, established by the Privacy Act of 1974, recommended that businesses let consumers opt-out of mailing lists. But it did not recommend regulations to require this, believing industry would do so voluntarily. *See id.* at 969. In large measure, they have not. *See id.*

51. *See* 26 U.S.C. § 6109(d) (1994). The IRS began to use SSNs in 1961, almost thirty years after SSNs were first assigned to Americans for purposes of the Social Security laws. *See* Hugh R. Jones, *Your Number's Up: Social Security Numbers and the Right to Privacy*, Hawaii Bar J., Nov. 1996, at 40.

tion on a particular tax return.[52] In 1986, this requirement was limited to children over five years in age.[53] However, in 1988, Congress reduced the age at which the number was required to two. In 1990, Congress reduced to one. Again, in 1994, the minimum age was abolished altogether.[54] This requirement further enhances the possibilities for use of the SSN as a "cradle-to-grave" personal identifier.[55]

To further the use of the SSN in tax administration, employers must collect SSNs of their employees for purposes of properly accounting for the withholding of taxes. Information about a taxpayer, including their social security number, may be furnished to state tax officials if necessary for the enforcement and administration of such state tax laws.[56]

In addition, the SSN of a taxpayer is printed on liens filed by the Internal Revenue Service.[57] This practice is especially egregious because these liens are filed in county recording offices where the taxpayer owns real property. Such county recording offices are, of course, open to the public. This IRS practice, therefore, allows for wide access to the SSNs of seriously delinquent taxpayers. In a similar vein, when the United States government files for a writ of garnishment to collect a debt, the application must include the debtor's SSN, further exposing the SSN to public view.[58]

2. *Law Enforcement*

Law enforcement agencies frequently key their records on persons to SSN. The largest criminal justice database in the country, the National Crime Information Center ("NCIC") maintains lists of, among other individuals, convicted criminals and fugitives.[59] When a person's name is entered into the NCIC's interstate identification files, the SSN, if available, is included in the person's data.[60] Perhaps sensitive to the fact that the Privacy Act does not authorize law enforcement agencies to request

52. *See* 26 U.S.C.A. § 151(e).

53. *See* Historical and Statutory Notes to 26 U.S.C.A. § 6109 (West 1996).

54. *See id.* This last amendment was made effective with returns for taxable years after August 20, 1996. *See id.*

55. *See id.* (constituting the "cradle" requirement). For the "grave" requirement, *see* 42 U.S.C. § 666(a)(13) (requiring states to place SSNs on decedents' death certificates).

56. *See* 26 U.S.C. § 6103(c). The current version of the statute allows the disclosure of parts of a return for numerous other reasons. Disclosure of "return information" (which includes the SSN) is more limited, but includes child support enforcement and student loan default collection. *See, e.g.*, §§ 6103(*l*)(6), 6103(m)(4).

57. *See* IRS Form 668 (Revised 9-83).

58. *See* 28 U.S.C. § 3205(b)(1)(A). This statute covers both tax debts and other debts owed to the United States. *See id.*

59. *See* Notices - Department of Justice - Privacy Act of 1974 Modified System of Records, 60 Fed. Reg. 19774 (April 20, 1995).

60. *See id.* at 19777.

SSNs without statutory disclosure, there is a notice in the Federal Register that cautions about "the requirements of the Privacy Act with regard to the solicitation of SSNs hav[ing] been brought to the attention of the members of the NCIC system."[61]

In addition to the federally-maintained NCIC file, state-maintained law enforcement records are also keyed to SSNs.[62] For example, New Jersey law provides that anyone may obtain another person's criminal history by furnishing the person's name and either social security number or date of birth to the State Police and paying the appropriate fee.[63] Most states also choose to use the SSN as a means of identifying sex offenders, under their registration and community notification law, and this number is one of the items that the offender must disclose.[64] Moreover, federal agencies also use SSNs for routine criminal background checks.[65]

The use of SSNs in the law enforcement area is routine. For example, police questioning a suspect will frequently ask for a detainee's SSN along with his name. The routineness of this practice is seen in decisions such as *United States v. Johnson*, where the court held that the request for an SSN by a law enforcement officer is "routine booking information" that police may elicit before giving the *Miranda* warning against self-incrimination.[66] However, SSN requests by law enforcement are not authorized by, and probably forbidden by, Section 7 of the Privacy Act of 1974, to be discussed later in this article.

---

61. *Id.* It is important to note that access to NCIC records is strictly controlled, and is limited only to criminal justice agencies; whereby only personnel who have an appropriate clearance and authorization may access criminal justice records, and computer lines connecting NCIC computers must be secured. *See id.* (discussing "Safeguards").

62. *See, e.g.*, N.J. STAT. ANN. § 53:1-20.6 (West 1986 & Supp. 1996).

63. *See id.* The law allows any member of the public access to criminal records, because unlike the federal NCIC records, law enforcement records maintained by state or local agencies are not subject to the controls applicable to NCIC. *See id.*

64. *See, e.g.* N.J. STAT. ANN. § 2C:7-4(b)(1) (West 1995).

65. *See, e.g.* Cathy Bugman et al., *Sites in Middlesex, Somerset Preparing for Today's Presidential Visit*, STAR-LEDGER (Newark, N.J.), Oct. 16, 1992, *available in* 1992 WL 11086071 (stating that in anticipation of the visit of President George Bush, a school principal was required by the Secret Service to "get names, addresses and [SSNs] of about 160 students in the band."); General Services Administration Form SF-50 (requiring an applicant for an employment-related security clearance or background check to submit the SSN).

66. United States v. Johnson, No. 94-5225, 1995 WL 88947, at *3 (4th Cir. Mar. 6, 1995). *See also* State v. Jordan, 506 S.W.2d 74, 83 (Mo. App. 1974) (also holding that officer's SSN request was routine request, before which *Miranda* warning need not be given). The Supreme Court held, in *Pennsylvania v. Muniz*, 496 U.S. 582, 601 (1990), that an officer's request for certain routine information such as name, address, and birthdate, was merely routine booking information, not a request for incriminatory statements, and therefore, is not subject to *Miranda* safeguards. *Johnson* cited *Muniz* as support for its holding that the SSN is also "routine" information. *Id.*

The persuasiveness of SSN usage in law enforcement is especially troubling because the solicitation and usage of a suspect's SSN appears to be illegal. Its usage by law enforcement also creates ancillary problems. Since SSNs are used for both suspect and victim identification, there is a risk of the number entering public records. For example, *Star-Telegram, Inc. v. Walker* describes how a newspaper obtained a *victim's* SSN when it appeared in a routine police report that was easily accessible to reporters preparing a newspaper "police blotter" column.[67]

3. *SSN Usage by Courts*

The Bankruptcy Rules require the SSN of either the debtor or the preparer in many instances.[68] As demonstrated earlier, the use of the SSN for purposes of finance and credit is widespread. Of course, it is when a person's finances are troubled that a person generally comes to bankruptcy court, and it is not surprising to find such similarity in indexing methods. Unlike private debtor records, however, bankruptcy filings are made part of the public record. In order to file a bankruptcy petition, a person thereby exposes his social security number to public view. Applications to a court for a garnishment order of collection of a federal debt must also include the SSN of the debtor.[69]

Similarly, the Tax Court's rules require a petitioner to place their SSNs on all filings with that court.[70] In addition, the rules of the United States District Court for the District of New Jersey require the attorney of record to place the last four digits of her SSN as part of the caption on all pleadings.[71]

Moreover, it is routine for attorneys engaging in discovery, in civil cases, to request SSNs of persons identified in interrogatories.[72] While the practice of requesting SSNs is common, a refusal to supply the SSN

67. *See* Star Telegram v. Walker, 834 S.W.2d 54 (Tex. 1992).

68. *See, e.g.,* FED. R. BANKR. P. 1005 ("the title of the case shall include the name [and] social security number and employer's tax identification number . . ."); Bankruptcy Form 3 (containing a space for a non-attorney bankruptcy preparer to enter his SSN). These requirements have been upheld against constitutional challenges. *See infra* notes 194 and 241.

69. *See* 28 U.S.C. § 3205(b)(1)(A).

70. *See* TAX COURT R. 34(b)(1) (requiring that the petition filed with the Tax Court include "an identification number e.g., Social Security number or employment identification number"). An individual will disclose a SSN, while a business will disclose a TIN. *See also* TAX COURT R. 175(a)(1)(B) (SSN required for small tax cases); 260(b)(1) (SSN required for overpayment determination cases); 261(b)(1) (SSN required for motion to redetermine interest in deficiency cases); 271(b)(1) (SSN required on motion for administrative costs.)

71. *See* U.S. Dist. Ct., D.N.J. Rule 8(A).

72. *See, e.g., In re* Amendments to Rules of Civil Procedure, 577 So. 2d 580, 581 (Fla. 1991) (adopting standard interrogatories in which the SSN of litigants is requested).

may still be upheld by a court on a motion to compel.[73] However, through federal legislation, courts may collect and use the SSNs of jurors for limited purposes.[74]

One of the more troubling uses of SSNs by courts presents itself in the frequent reference to the SSNs of litigants or others for no apparent or justifiable reasons. In many cases, courts, in the process of writing opinions, have listed the SSN of some litigant or other person.[75] In one instance, a federal appeals court took an extreme view and denounced as "frivolous" a litigant's objection to the use of his SSN in case files and captions.[76] Other courts, however, act more prudently, by explicitly redacting SSNs from their published decisions.[77] Only these few courts seem disciplined in exercising restraint, before placing SSNs into the public record. This more balanced approach is better, especially in light of other precedents in which courts profess to recognize that a person's SSN is a private matter, which a government should not freely disclose.[78]

---

73. *See, e.g.*, Mike v. Dymon, Inc., No. 95-2405-EEO, 1996 WL 674007 (D. Kan. Nov. 14, 1996) (holding, on motion to compel discovery, that SSN request was not reasonably calculated to lead to the discovery of admissible evidence); Murcio v. Perez, No. 97 C3339, 1998 WL 60817 (N.D. Ill. Feb. 6, 1998) (granting protective order against release of police officers and SSNs were obtained in discovery).

74. *See* 42 U.S.C. § 405(c)(2)(E). The statute authorizes both state and federal courts to use SSNs once they have compiled a master jury list, to (1) identify convicted felons; and (2) remove duplicates from any list. *See id.* While the statute is silent on other usage's, and thus, does not permit them, courts nevertheless have used them for other purposes. *See, e.g.*, United States v. Pottorf, 769 F. Supp. 1176, 1188 (D. Kan. 1991) (ordering the disclosure of jurors' SSNs to defense counsel and to the attorney for the United States; no mention of a protective order). *But see* Copley Press, Inc. v. San Diego Superior Court, 278 Cal. Rptr. 443, 445 (Cal. App. 4th, 1991) (ruling that SSNs of jurors in a publicized case may be used by the court but may not be disclosed to the public or to reporters).

75. *See, e.g.*, Falco v. Shalala, 27 F.3d 160 (5th Cir. 1994) (listing SSN of litigant in disability appeal case for no apparent reason); Miller v. Shalala, 8 F.3d 611 (8th Cir. 1993) (same); United States *ex rel.* Wilson v. Resor, 332 F. Supp. 1013 (S.D. Ga. 1971) (listing SSN of habeas petitioner attempting to gain discharge from the army); Armstrong v. Laird, 325 F. Supp. 1042 (D. Mass. 1971), *rev'd on other grounds*, 456 F.2d 521 (1st Cir. 1972) (same); Bowser v. First Nat'l Bank of Oakland, 390 F. Supp. 834, 835 n.1 (D. Md. 1975) (listing SSNs of bank depositors in case involving enforcement of IRS administrative summons); Bowen v. Florida Indus. Comm'n, 117 So. 2d 220 (Fla. App. 1959) (listing SSN of workers' compensation appellant). In addition, a brief review of any volume of the *Military Justice* reporter will show, the SSNs of military personnel appealing court-martial convictions also routinely appear next to their names.

76. Bowersock v. Callahan, No. 97-3486, 1997 WL 685403 (6th Cir. Oct. 29, 1997).

77. United States v. Phillips, 19 F.3d 1565, 1568 (11th Cir. 1994) (specifically redacting SSNs from the published opinion); Pasadena Star News v. Superior Court, 249 Cal. Rptr. 729, 732 n.7 (Cal. App. 2d, 1988) (redacting name from published opinion in sensitive case).

78. *See, e.g.* Swisher v. Dept. of Air Force, 495 F. Supp. 337, 340 (W.D. Mo. 1980), *aff'd*, 660 F.2d 369 (8th Cir. 1981) (holding that social security number disclosure constitutes "more than a minimal invasion" of privacy); Aronson v. Internal Revenue Service, 973 F.2d

4. *Driver Records*

The use of SSNs as a means for identifying and tracking drivers is common in several states[79] and is specifically authorized by federal statute.[80] Until recently, as many as thirty-four states furnished a substantial amount of personal information about drivers upon payment of a fee.[81] Some states have case law precluding this practice, as *Doe v. Registrar of Motor Vehicles* illustrates.[82] *Doe* barred Massachusetts' practice of *distributing* numbers, but it does not bar the practice of *collecting* numbers. In fact, that issue was presented in *Ostric v. Board of Appeal on Motor Vehicle Liability Policies and Bonds*, where the court upheld Massachusetts' power to ask for SSNs for licensing against a series of state and federal statutory and constitutional challenges.[83] Indeed, these two decisions illustrate a common theme; that courts will provide greater protection to challenges against dissemination of SSNs as compared to collection of the numbers.

962, 968 (1st Cir. 1992) ("citizens have [a] 'strong privacy interest' in social security numbers").

79. *See, e.g.* N.J. ADM. CODE tit. 13, § 21-1.3(a) (1997) (stating that the applicant for any New Jersey license or permit "shall disclose his or her [SSN]" although the SSN is not printed on the license). While the practice of collecting the number but not putting it on the license is common, other states, like Illinois, mandate placing the SSN on the license itself. *See* 625 ILL. COMP. STAT. ANN. Act 5, ch. 6, § 110 (West 1993 & Supp. 1997).

80. *See* 42 U.S.C. § 405(c)(2)(C)(i).

81. *See* Joan Zorza, *Recognizing and Protecting the Privacy and Confidentiality Needs of Battered Women*, 29 FAM. L.Q. 273, 287 (1995) (responding, legislatively, to an incident where a murderer had located the victim after searching state motor vehicle records). *See also* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 518 n.105 (1995).

82. 528 N.E.2d 880 (Mass. App. Ct. 1988). In *Doe*, the plaintiffs challenged Massachusetts' practice of disclosing, *inter alia*, the SSN, date of birth, and height of all applicants for driver licenses. *See id.* at 881. Reversing a lower court decision, the court said that individuals had enough of a privacy interest in that data to require the Department of Motor Vehicles to justify its policy of releasing the information. *See id.* at 887 ("plaintiffs have shown an invasion of privacy which requires a showing of some public or governmental purpose in disclosure"). The decision was based entirely on Massachusetts' privacy laws, but it relied heavily on federal Privacy Act precedent. *See id.* at 886.

83. 280 N.E.2d 692, 695 (Mass. 1972). *See also* Schmidt v. Powell, 280 N.E.2d 236 (Ill. App. 1972) (holding there was no violation of federal or state due process or equal protection rights when state collected SSNs for drivers' licenses). The Illinois statute referenced in *Schmidt* contained an exception for religious objectors. For further discussion on religious objections to driver license number assignments, *see infra* note 242. *See also* Tennessee v. Loudon, 857 S.W.2d 878, 882 (Tenn. Crim. App. 1993) (describing the statutory requirement that the SSN appear on a license as supporting a "compelling state interest . . . [in] distinguish[ing] a person from others with the same or similar name."). Sadly, it would be no great leap from this unfortunate statement to one in which a court might approve of a general requirement that people carry government-issued identity cards to further that same allegedly "compelling" state interest.

Widespread distribution of the SSN from driver records has been phased out with the 1994 adoption by Congress of a statute barring disclosure of "personal information" in drivers' licenses.[84] The statute provides for both criminal punishment and a private cause of action for violations of the statute.[85] While this statute will eliminate casual, routine requests for information, it is nevertheless riddled with exceptions that allow the distribution of records to, among others, private investigators, car rental businesses, or car marketing researchers.[86] In sum, the statute does little to curtail the *distribution* of personal information from driver records, and does nothing to limit the *use* of SSN information. Even the few protections now available in this federal statute, however, may be struck down. For example, a federal court in South Carolina recently declared portions of the Driver Privacy Protection Act to be an unconstitutional intrusion on states' powers, in violation of the Tenth Amendment.[87]

5. *Child Support Records and Family Law*

The 1996 federal welfare reforms contained a number of provisions authorizing, or sometimes requiring, the use of SSNs as a means of locating individuals who fail to pay their child support or alimony obligations. Even prior to these 1996 amendments, it was permissible for both states and the federal government to use the SSN in connection with collecting these moneys owed.[88] The 1996 law expands the use of SSNs in child support collection.

The statute requires the creation of a database containing the names and SSNs of all persons who owe or are owed child support.[89] The law also creates mechanisms for comparing names and SSNs in the child support database with other new databases mandated by the legislation.

---

84. *See* 18 U.S.C.A. § 2725 (West Supp. 1997). "Personal information" includes a driver's photograph, SSN, driver license number, name, address, phone number, and "medical or disability information." *Id.* § 2725(3). It does not include the five-digit zip code, or information about the driver's accidents, infractions, or driver status. *See id.*

85. *See id.* §§ 2723, 2724 (West Supp. 1996).

86. *See id.* § 2721(b)(1)-(14) (West Supp. 1996). Other exceptions allow distribution of records to any government official in the performance of their functions, or for product safety recalls, and insurance activities. *See id. See infra* note 270 & accompanying text for discussion of a proposal to close these loopholes.

87. *See* Condon v. Reno, 972 F. Supp. 977 (D.S.C. 1997).

88. *See* 42 U.S.C. § 405(c)(2)(C)(ii) (1994) (outlining that the federal government would use SSNs for child support collection by requiring a person seeking a garnishment order for child support purposes to furnish either a SSN or some other personal identifier before processing). *See* 5 C.F.R. § 581.203(a)(3) (1996) (requiring SSN, employment number, Department of Veterans Affairs claim number, or civil service retirement number).

89. *See* 42 U.S.C.A. § 653(h)(1) (West Supp. 1997) (requiring the SSN "or other uniform identification number" to identify those who owe child support).

These databases are to contain the names of employees in the private sector, state and local governments,[90] and the federal government.[91] Finally, the new rules also compare the databases of applicants for professional licenses with child support or alimony "deadbeats."[92]

It is now commonplace in the collection of alimony and child support payments for the SSN of the debtor, if known, to be placed on records sent to the government agency responsible for collecting overdue child support and alimony.[93] However, other states have been more resistant to the new provisions. Some western states, for example, have expressed opposition to the new federal legislation. In particular, the Colorado and Wyoming legislators have voiced significant concerns to new federal mandates that require states to overhaul child support collection mechanisms and furnish state employees' SSNs to a federal registry.[94] Despite local opposition, these new federal statutes will greatly increase SSN use around the country.

In addition, the use of SSNs has been contemplated in other issues involving family law as well. Along with using SSNs for family debt collection, as discussed above, the Uniform Laws have suggested that the SSNs of both parties should be disclosed on applications for a marriage license.[95] Similarly, some states require that when an unmarried man acknowledges paternity of a child, the SSN must be disclosed.[96]

---

90. Upon hiring a new worker, these employers must furnish the worker's SSN to a "Directory of New Hires." *Id.* § 653a(b)(1)(A) (West Supp. 1997). The state must then proceed to match the information in the Directory of New Hires with the information in the federal database of those who failed to pay their obligations. *See id.* § 653a(f). Any matches are to be reported to the appropriate authorities so the debt collection may resume. In addition, the information received by a state's Directory of New Hires must be forwarded to the federal registry within three days so that federal registries can then be checked and compared. *See id.* § 653a(g)(2)(A).

91. *See id.* § 653(n) (West Supp. 1997) (mandating that a list of all federal employees' names and SSN be compiled every quarter and compared with the national registry).

92. *Id.* § 666(a)(13) (West Supp. 1997).

93. *See, e.g.,* N.J. Court Rule 5:7-4(b).

94. *See* Carl Hilliard, *Republican Caucus Questions Child Support Bill as "Big Brother,"* ASSOCIATED PRESS (Feb. 28, 1997), *available in* 1997 WL 2504481 (stating that many Colorado Republican legislators were willing to forfeit up to $35 million in federal aid for not complying with the mandates, on the grounds that the federal mandates were a "slippery slope toward Big Brotherism."); John Sarche, *Senators Acted Irresponsibly*, ASSOCIATED PRESS (Feb. 21, 1997), *available in* 1997 WL 2503071 (stating that several Wyoming legislators risked forfeiting $6 million in federal funds to that state because of their opposition to this "federal mandate [which] . . . invade[s] personal privacy").

95. *See* UNIFORM MARRIAGE AND DIVORCE ACT § 202(a)(1), 9A U.L.A. 162 (1987) (providing that applicants for a marriage license shall disclose their SSNs on their application form). Nevertheless, no state has accepted this provision of the Uniform Law. *Id.*

96. *See* ALASKA STAT. § 18.50.165(a)(2) (1995) (requiring both parents' SSNs to be on the acknowledgment form). The federal authorization for states to require SSNs on birth certificates is found at 42 U.S.C. § 405(c)(2)(C)(ii).

6. *Professional and Other Licenses*

With the new federal child support laws, applicants for professional licenses will be required to disclose their SSNs when the statutes take effect. This is already the practice in some states.[97] Similarly, key officers of banks may have to disclose their SSNs to state regulators.[98] One municipality, in an effort to regulate multi-family dwellings, required the owners of these dwellings to provide several items of information, including each resident's SSN.[99] Also, another town required peddlers operating within the town to furnish a SSN to the municipality.[100]

7. *Student Loans*

For any person to receive a federal education grant or loan, the student must furnish a SSN to the school for which they are applying.[101] This requirement assists the government, school, and student maintain information about student loans, and perhaps, upon default, to track down defaulting borrowers.[102]

8. *Other SSN Use*

Governmental use of SSNs for other purposes can vary widely. For example, claimants for veterans benefits must supply SSNs on the application for such benefits.[103] A failure to provide the number is grounds for denying benefits.[104] SSNs are also used by the government for the

97. *See, e.g.*, ALA. CODE § 8-19A-5 (1975) (telemarketer license).

98. *See, e.g.*, ARIZ. REV. STAT. ANN. § 6-1204(A)(4)(e) (1996) (requiring branch managers and "responsible individuals" to disclose SSNs to state regulators).

99. *See* Makula v. Village of Schiller Park, No. 95 C2400, 1995 WL 755305 at *3 (N.D. Ill. Dec. 14, 1995). The other information requested was the resident's name, work and home telephone numbers, and the make and license number of their vehicles. *See id.* The plaintiffs in the case, owners of the units, challenged this recordkeeping requirement as violative of their rights of privacy, association, due process, and equal protection. *See id.* at *8, *9. The court, however, upheld the requirements, at least as they applied to the owners, and did not discuss the rights of the residents. *See id. But see* Yeager v. Hackensack Water Co., 615 F. Supp. 1087 (D.N.J. 1985) (invalidating an executive order requiring the collection of the SSNs of residents).

100. *See* CODE OF MORRISTOWN (N.J.) §§ 153-11(B)(3); 153-23(A)(1) (1995).

101. *See* 20 U.S.C. § 1091(a)(4)(B) (1994).

102. *See id.* at § 1092(b). The statute requires the Secretary of Education to set up a "National Student Loan Data System." *Id.* at § 1092(a). It promotes the exchange of information among participants in the system, and allows participants access to a great deal of student information, including enrollment status and residency, amount borrowed, deferments, forbearance's, and lender and servicer information. *See id.*

103. *See* 38 U.S.C. § 5101(c)(1) (1994).

104. *See id.* § 5101(c)(2). *See also* 38 C.F.R. § 3.216 (1996) ("benefits will be terminated if a beneficiary fails to furnish the Department . . . with his or her social security

identification of seagoing vessels.[105] In addition, SSNs are the primary numerical identifier used by the Selective Service System for administering draft registration.[106]

Not surprisingly, an applicant for any of the particular benefits administered under the Social Security Act must also furnish their SSN.[107] However, the Social Security Administration liberally permits an applicant to provide alternate information. Specifically, if an individual elects not to supply the SSN, he may supply "sufficient additional information," i.e., birthdate, birthplace, and the mother's and father's names.[108] The Social Security Administration will, in turn, use this information to determine the person's SSN.[109] By providing the designated "sufficient additional information," the individual is deemed to have furnished "satisfactory proof" of the SSN, and the application for benefits may proceed.[110] One may be surprised by this fact. It is indeed ironic, considering all the instances of required SSN disclosure by government, that the one area in which a person can refuse the number, but receive benefits is Social Security itself.

III. RESTRICTIONS ON SSN USE AND ABUSE

In this Part, several potential legal attacks are surveyed that a plaintiff challenging SSN collection, use, or dissemination, might advance. Unfortunately, few of these frameworks have been successful in the courts.

A. SECTION 7 OF THE PRIVACY ACT

The main source of restrictions on SSN usage by government comes from Section 7 of the Privacy Act of 1974. The Privacy Act provides that if an entity is a local, state, or federal government agency, it cannot *require* an individual to submit a SSN, unless (1) the records system for which the SSN is being solicited antedated 1975 and then used SSNs as its identifying number; or (2) it has received specific permission from

number . . . within 60 days from the date the beneficiary is requested to furnish the social security number").

105. *See* 46 U.S.C. §§ 12103, 12501, 12503 (1994) (requiring a person who is registering a vessel to furnish either, (1) if an individual, the individual's SSN; (2) if a corporation, then the corporation's TIN or the SSN of an officer of the corporation).

106. *See* Selective Serv. Sys. v. Minnesota Pub. Interest Research Group, 468 U.S. 841, 862 n.1 (1984) (noting requirement); *see also* 50 U.S.C.A. Appendix § 453(b) (West 1990).

107. *See* 20 C.F.R. § 404.469 (1996).

108. *Id.*

109. *See id.*

110. *Id.*

Congress to require submission of a SSN.[111] If neither of those two conditions is satisfied, then the entity may still *request* that an individual submit his SSN voluntarily.[112] In either case, i.e., a requirement or request for the number, the agency must fully disclose what uses will be made of the number.[113]

Section 7 could be applauded because read in isolation, it seems to prohibit a significant number of governmental uses of information. But when one considers how many exceptions Congress has granted for SSN collection and use, the exceptions clearly swallow the general rule. Moreover, Section 7 does not contain any restrictions on private actors. Absent governmental compulsion to collect a SSN, a private individual or entity is not constrained at all by the terms of the Privacy Act of 1974.[114]

1. *When a State Agency is Subject to the Privacy Act*

Whether an entity is a "state agency" under the Privacy Act is not as easy to determine as it might seem, as illustrated in *Krebs v. Rutgers*.[115] *Krebs* involved a challenge to the collection and use of SSNs by Rutgers, the State University of New Jersey.[116] The terms of Section 7 apply to

---

111. *See* Pub. L. No. 93-579, § 7. This provision of the Privacy Act was never codified, but is instead set out as a historical note to 5 U.S.C.A § 552a (West 1996). The full text states the following:

> (a)(1) It shall be unlawful for any Federal, State, or local government agency to deny any individual any right, benefit or privilege provided by law because of such individual's refusal to disclose his social security account number. (2) the provisions of paragraph (1) of this subsection shall not apply with respect to—(A) any disclosure which is required by Federal statute, or (B) the disclosure of a social security number to any Federal, State, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual. (b) Any Federal, State, or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

Id.

112. *See id.*

113. *See id.*

114. Initially, proponents of what became § 7 of the Privacy Act of 1974 urged that private entities be made subject to its provisions, but its final provisions excluded such entities from coverage.

115. 797 F. Supp. 1246 (D.N.J. 1992). I was one of the plaintiffs in the *Krebs* matter, and participating in the case was the prime source of my interest in the privacy issues dealing with personal identifying numbers.

116. In *Krebs*, several students of Rutgers University brought an action against the school and its president, charging that the school (1) illegally requested social security numbers from students and (2) utilized and disclosed them in an illegal manner. *Id.* at 1250-51. The two-count complaint alleged that the university violated section 7 of the Privacy Act and the Buckley Amendment, 20 U.S.C. § 1232g (also known as the Family Educational Rights and Privacy Act or FERPA). *See id.* The discussion here covers only the

"State . . . government agencies," and therefore, the *Krebs* plaintiffs argued that Rutgers was such an agency given that it had a state charter, received significant state funding, and was denominated an "instrumentality of the state" in the New Jersey statutes.[117] The district court, however, rejected this argument. Judge Sarokin opined that in order to fall within the terms of Section 7, the agency in question had to be subject to direct, day-to-day control by the State.[118] The court concluded that Rutgers, which was governed by a separate board of governors outside of the state department of higher education, was not subject to this day-to-day control.[119] Indeed, governance decisions at Rutgers were made "without recourse or reference to any department or agency of the state."[120] As such, because the university was not subject to day-to-day control, it was not an agency of the state within the meaning of Section 7. Therefore, the students could receive no relief on their Section 7 claims.[121]

Even when an agency is not found to be literally a "state agency" within the meaning of the Privacy Act, there is authority which holds that a private actor, when acting pursuant to government compulsion, is still subject to the restrictions of Section 7. The court found such compulsion in *Yeager v. Hackensack Water Company*.[122] In *Yeager*, then-Governor Thomas Kean declared a drought emergency and ordered water companies within the State to take steps to ensure compliance with the emergency.[123] One method the water companies used to ensure compliance was to collect the SSNs of all residents of a particular home.[124]

Privacy Act issues, and the FERPA issues will be discussed later in this Article. For a more detailed discussion of *Krebs*; see Papandreou's casenote on the litigation, *supra* note 8.

117. *Krebs*, 797 F. Supp. at 1258.

118. *See id.* at 1254. The court rejected the plaintiffs' arguments that it evaluate Rutgers' state-agency status based on seven indicia of federal-agency status proposed by the D.C. Circuit in *Rocap v. Indiek*, 539 F.2d 174 (D.C. Cir. 1976). The seven factors were the following:

> (1) government charter; (2) government appointment of the [d]irectors [of the university]; (3) close governmental supervision over business transactions; (4) government audit and reporting requirements; (5) express designation as an agency; (6) employees are considered public for a number of purposes; (7) regulatory powers to make regulations and carry out its functions.

Krebs, 797 F. Supp. at 1254. Instead, the court blended them into a single factor, "government control over and involvement in Rutgers' operations." *Id.*

119. *See Krebs*, 797 F. Supp. at 1255.

120. *Id.* (citing N.J. STAT. ANN. § 18A:65-28 (1996)).

121. *See id.*

122. 615 F. Supp. 1087 (D.N.J. 1985).

123. *See id.* at 1088.

124. *See id.* at 1089.

Applying Section 7 of the Privacy Act, the district court concluded that such a practice was unlawful. The court first considered whether Hackensack Water Company was a "state . . . government agency" within the meaning of Section 7.[125] It concluded that it was not, but reasoned that since the state compelled or provided the impetus for the water company to request the SSNs, the action of the water company "may fairly be treated as that of the state itself."[126] Thus, due to the emergency declaration, the water company's actions were legally imputed to the state.

The court next considered whether the requirements of Section 7 were satisfied and noted two distinct violations of the law. First, the water company failed to provide the statutory disclosure that disclosure of the numbers was voluntary, and of the uses to which the number would be put.[127] Second, the court explained that the water company could not make providing the numbers mandatory because there was neither a federal authorization for the practice nor a records system antedating 1975. Accordingly, the court enjoined any denial of benefits to customers for failing to provide a SSN.[128] Plainly, the rule of *Yeager* would apply even if it was the state itself that was doing what the water company there had attempted to do, since there was no federal statute authorizing the use of SSNs for that purpose.

In contrast to *Yeager*, where state compulsion was found, is *Freeman v. Koerner Ford of Scranton*.[129] In *Freeman*, the plaintiff complained that an automobile dealership acted unlawfully by denying him credit when he refused to place his SSN on his account application.[130] The court first explained that Section 7 of the Privacy Act did not afford the plaintiff a remedy against private actors.[131] However, the plaintiff argued that the Federal Reserve Board—a government agency—created standard loan application forms which were offered as 'model' applications, and that this was a form of "regulation of creditor activities" mean-

125. *Id.*

126. *Id.* at 1091 (citing Jackson v. Metropolitan Edison Co., 419 U.S. 345 (1974)).

127. *See id.* at 1092.

128. *See id.* The court also enjoined the water companies from disseminating the SSNs collected without disclosure to anyone, by any means. However, the court refused to order the destruction of the collected numbers. *See id.* In contrast, the court ordered the destruction of any household members' names collected other than the primary customer's. *See id.* at 1093. The court based this aspect of the decision on constitutional, rather than statutory grounds. It found that the collection of household members' names impinged on an individual's constitutional privacy rights, and was not justified by a compelling state interest. *See id.* (citing Paul v. Davis, 424 U.S. 693, 713 (1976)). The court did not discuss the constitutional issues arising from the use of SSNs.

129. 536 A.2d 340 (Pa. Super. Ct. 1987).

130. *See id.* at 340-41. The dealership's employees asserted that the number was required in order to assess the plaintiff's credit history. *See id.* at 341.

131. *See id.*

ing that the auto dealership's activities could be imputed to the government.[132] The court rejected that approach and stated that the mere fact that the dealership used a governmentally-created 'model' form did not mean it was ordered or sufficiently encouraged to use the form so as to turn this private dealership into a state actor.[133]

2. *Remedies under Section 7*

Unlike Section 7, Section 1 of the Privacy Act of 1974 deals exclusively with records kept by the federal government. More specifically, the Act deals with the issue of what federal government records are deemed private, and provides for remedies such as injunctions and statutory damages for violations of the Act.[134] Section 7 of the Privacy Act does not explicitly provide remedies for its violation. Nevertheless, every court that has faced the issue has concluded that it would be illusory for Section 7 to declare these rights to have SSNs free from compelled or uninformed collection, and provide no judicial remedy.[135]

Accordingly, courts have issued declaratory and injunctive relief for Section 7 violations, but none appears to have awarded damages.[136] It remains an open question whether litigants may use Section 7 in the future to enjoin violations by states and state agencies, at least in federal court. This is so because case law under the Privacy Act (including Section 7) is clear that an *agency* can be a defendant, but an *individual* may not be.[137] Under the Eleventh Amendment doctrine in light of *Seminole*

---

132. *Id.*

133. *See id.* at 342. The *Freeman* court also rejected the plaintiff's contentions that the dealership's actions violated the Equal Credit Opportunity Act. *Id.* at 341; *see also* 15 U.S.C. § 1691(a) (1994).

134. 5 U.S.C. § 552a.

135. *See* Yeager v. Hackensack Water Co., 615 F. Supp. 1087 (D.N.J. 1985) (granting declaratory relief and permanent injunction); Doe v. Sharp, 491 F. Supp. 346, 350 (D. Mass. 1980) (implying that a prospective order of compliance could be issued by a court); Greater Cleveland Welfare Rts. Org. v. Bauer, 462 F. Supp. 1313, 1320-21 (N.D. Ohio 1978) ("plaintiffs [have] an implied cause of action for prospective relief;" court issued order to defendant requiring compliance).

136. An action for damages against state and local entities (but not the federal government) would probably be based on 42 U.S.C. § 1983 (1994), as interpreted in *Maine v. Thiboutot*, 448 U.S. 1 (1980). *Thiboutot* holds that "the § 1983 remedy broadly encompasses violations of federal statutory as well as constitutional law." *Id.* at 4. Therefore, a state actor "may be made to respond in damages . . . for violations of . . . federal statutory law." *Id.* at 5. Accordingly, since Section 7 is part of federal statutory law, a person could obtain not only damages but declaratory and injunctive relief as well by bootstrapping a Section 7 claim into a § 1983 claim. Once a plaintiff prevails on these grounds, attorneys fees can also be awarded against the losing governmental entity. *See* 42 U.S.C. § 1988.

137. *See, e.g.*, Brown-Bey v. United States, 720 F.2d 467, 469 (7th Cir. 1983) ("[t]he Privacy Act authorizes private civil actions for violations of its provisions only against an agency, not against any individual."). *But see* Krebs v. Rutgers, 797 F. Supp. 1246, 1260

Tribe of Florida v. Florida, it may be that neither a state agency nor a responsible individual can be sued for violations of the Privacy Act.[138] This anomaly could present problems in the future.

3. *Exceptions to Section 7*

Once again, Section 7 permits a state agency to require a SSN only, (1) in some records system antedating 1975; or (2) where Congress has specifically authorized its use. As stated above, the exceptions Congress has made are manifold, and this is one of the primary problems with Section 7.[139] State actors may require SSNs to receive Medicare or Medicaid benefits, or to receive a student loan from a state school, to receive welfare benefits, to collect child support. They may require SSNs before allowing an individual to enter into employment, on their tax returns, or on their driver's licenses. If someone is arrested, the SSN will likely be solicited from them. They are used extensively in debtor-creditor relations. They routinely appear in public court filings. In sum, Congress has carved out so many exceptions, and created so many mandatory uses of the SSN, that the Privacy Act's restrictions on government usage of the SSN are all but swallowed up by the exceptions.[140] In all of these instances, a Congressional exception allows a state to require the submission of an SSN by an individual. It authorizes a state to deny benefits if the individual does not comply. Moreover, one court has declared that federal courts (as distinguished from executive branch agen-

(D.N.J. 1992) (although an individual is not a proper defendant under Section 7, plaintiffs might bootstrap Privacy Act claims into a § 1983 claim against the individual).

138. Seminole Tribe of Florida v. Florida, 116 S. Ct. 1114 (1996). States and state agencies are immune from suit under the Eleventh Amendment. Under *Seminole Tribe*, this immunity may be abrogated by Congressional action, provided that, (1) Congress' power to pass the law in question came from its powers under the Fourteenth Amendment, and not from Article I; and (2) Congress made it unmistakably clear in the statute that they were abrogating immunity. *See id.* at 1123, 1130-32. It is not clear what authority Congress used in passing the Privacy Act of 1974. Moreover, Congress mentioned nothing in the statute about abrogating states' Eleventh Amendment immunity. Thus, an argument that a Section 7 claim against a state agency is barred by the Eleventh Amendment will likely be successful.

As a means of escaping the harshness of the Eleventh Amendment, the court developed the doctrine of *Ex parte Young*, 209 U.S. 123 (1908). This doctrine allows a suit against an individual state officer to enjoin violations of the Amendment. Yet, Privacy Act case law suggests that no action lies against an individual. This may leave plaintiffs suing a state defendant in federal court with a situation in which substantive law grants a remedy only against the agency, but the Eleventh Amendment bars that remedy.

139. *See generally* 42 U.S.C. § 405(c)(2), listing most of the exceptions; *supra* notes 25 to 111 and accompanying text.

140. *See* Prowda, *supra* note 7, at 746 (criticizing Congress' actions in the area of SSN privacy because it "not only . . . authoriz[es] [the SSN's] use, but mandat[es] it").

cies) are not bound by Section 7's restrictions.[141]

However, this is not to say that Section 7 is to be scorned as irrelevant. Significant areas remain where a Section 7 action could be used to invalidate a state requirement of furnishing an SSN. The statute could also be used to force a government entity to furnish the mandatory disclosure when soliciting a SSN, namely, that the individual be told what uses will be made of the information (which must be done in all cases).[142] In addition, in cases where furnishing the SSN is not mandatory, an individual has a right to refuse to furnish the number and no benefits may be denied as a consequence of the refusal. Unfortunately, compliance with this latter requirement is rather lax.[143]

B. Exemption Six of the Freedom of Information Act

Another federal statute controlling SSN dissemination is the Freedom of Information Act ("FOIA").[144] The law requires federal agencies to generally make their records available to the public, unless a specific exemption applies. The key exemption at issue here, "Exemption Six," allows an agency to withhold records that would "disclose information of a personal nature where disclosure would constitute a clearly unwar-

141. *See In re* Adair, 212 B.R. 171, 173 (N.D. Ga. 1997).

142. For example, the SSN requirement imposed in the *Yeager* case, fell as a result of Section 7, while, the requirement of placing SSNs on non-agricultural Article 9 financing statements, discussed *supra* note 31, would probably also fall to a Section 7 challenge. *See supra* note 32 and accompanying text. Also the requirement of SSN disclosure to get a peddlers' license would also fall as a result of Section 7. *See supra* note 100 and accompanying text. Courts have also invalidated SSN requirements in election law. *See* Libertarian Party of Kentucky v. Ehrler, 776 F. Supp. 1200, 1209 (E.D. Ky. 1991); Greidinger v. Davis, 988 F.2d 1348 (4th Cir. 1993).

143. *But see* N.J. Adm. Code tit. 5, § 3-1.2(c); tit. 11, § 17-2.17 (1996). These sections are rare in that they acknowledge a state's duty to notify persons of their rights under Section 7. Privacy activist Kenneth Mayer said that his complaints to the State of New Jersey yielded these regulations. Before that, he added, the state had denied him a license as a construction code official and also refused to appoint him a notary public because of his refusal to furnish his SSN. Under applicable law at each of those times, Congress had not authorized a state to require an SSN in those circumstances. Accordingly, Mayer (1) should have been furnished with a notice of his right to refuse; and (2) given the licenses anyway after he refused. Neither occurred, and when the state agencies declined, Mayer commenced suit. The state conceded Mayer's point shortly thereafter. *See* Mayer v. Essex Co. College, Docket No. 91-5700 (D.N.J 1991); Mayer v. Secretary of State, Docket No. 91-5638 (D.N.J. 1991); Mayer v. Dep't of Community Affairs, Docket No. 92-1805 (D.N.J. 1992). Similarly, he stated that it was not until his intervention that New Jersey's Division of Motor Vehicles started putting information disclosures on its forms. *See* N.J. Adm. Code tit. 13, § 21-1.4. Thus, the DMV's disclosure states, (1) furnishing the SSN is mandatory; and (2) the uses which will be made of SSN. Mayer adds that New Jersey is rare among states in complying with the disclosure provisions of Privacy Act. Telephone Interview with Kenneth Mayer, P.E., October 1, 1997.

144. 5 U.S.C. § 552(a) (1994).

ranted invasion of personal privacy."[145] Courts have consistently held that SSNs are to be withheld from public requesters of agency documents and therefore will not be released or will be redacted from released documents.[146] These decisions reflect judicial awareness of the sensitivity of SSN dissemination. Still, the FOIA protects only those federal records sought by citizen requesters, and is therefore quite limited in scope. It does not address the collection of SSNs by these agencies, nor does it address SSN usage, nor intra-agency dissemination. It is ironic that despite the strong language about SSN usage that courts employ in FOIA decisions, they still give little protection to SSN dissemination outside of the FOIA context.

C. Criminal Penalties for Illegal Use

The widespread use of SSNs and the potential for their misuse has led Congress to impose criminal penalties for such illegal use. For example, misrepresenting a SSN, fraudulent actions to obtain a SSN, or alteration of a SSN are declared felonies with a five-year maximum prison sentence.[147] Construing this statute strictly, one court has held that the mere possession of a false social security number is not criminally pun-

145. 5 U.S.C. § 552(b).

146. *See, e.g.,* Sheet Metal Workers Int'l Assn. v. United States Air Force, 63 F.3d 994 (10th Cir. 1995) (denying union access to employees' SSNs); Painting Ind. of Hawaii Market Recovery Fund v. United States Dep't of Air Force, 26 F.3d 1479 (9th Cir. 1994) (same); International Bhd. of Elec. Workers Local Union No. 5 v. Dep't of Housing & Urban Dev., 852 F.2d 87, 89 (3d Cir. 1988) (same). To the contrary is NLRB v. Illinois Am. Water Co., 933 F.2d 1368 (7th Cir. 1991). Other notable FOIA cases which have protected SSNs include Aronson v. Internal Revenue Service, 973 F.2d 962, 968 (1st Cir. 1992) (denying SSNs from income tax records) and Heights Comm. Congress v. Virginia, 732 F.2d 526 (6th Cir. 1984) (names and SSNs of federal loan recipients redacted).

147. *See* 42 U.S.C. § 408(a)(7). Specifically, a criminal penalty may be imposed when any individual, with the purpose of causing or increasing a payment under the Social Security Act, or obtaining any benefit, or obtaining anything of value, or for any purpose:

> (A) willfully, knowingly, and with intent to deceive, uses a social security account number, assigned by the Commissioner of Social Security (in the exercise of the Commissioner's authority under [42 U.S.C. § 405(c)(2)] to establish and maintain records) on the basis of false information furnished to the Commissioner of Social Security by him or by any other person; or
>
> (B) with intent to deceive, falsely represents a number to be the social security account number assigned by the Commissioner of Social Security to him or to another person, when in fact such number is not the social security account number assigned by the Commissioner of Social Security to him or to such other person; or
>
> (C) knowingly alters a social security card issued by the Commissioner of Social Security, buys or sells a card that is, or purports to be, a card so issued, counterfeits a social security card, or possesses a social security card or counterfeit social security card with intent to sell or alter it.

Id.

ishable, whereas the actual usage of the SSN is punishable.[148] The disclosure, use, or compelled disclosure of an SSN, in violation of federal law, is also a felony punished in a like manner.[149] In addition, in Congress' other recent efforts to curtail privacy violations in driving records and in medical records, a criminal penalty is part of the remedial scheme.[150] These statutes do not penalize collecting the SSN, but rather, distributing it illegally. In sum, there is no criminal remedy for the illegal request of an SSN.

D. CONTROL OF SSNS IN EDUCATION: FERPA

Another federal restriction on the use of social security numbers—at least in the context of education—is found in the Family Educational Rights and Privacy Act ("FERPA"), also known as the "Buckley Amendment."[151] That Act bars educational institutions receiving federal funds from releasing education records or "personally identifiable information" about students there to unauthorized persons.[152] Educational records have been construed to include the SSN of students, whether denominated as such or as "student ID numbers."[153] However, FERPA does not protect the rights of faculty or other employees of the institution.[154]

In *Krebs v. Rutgers*, the plaintiffs, after losing their claims under the Privacy Act, were unable to control the *collection* of SSNs by Rutgers. Nevertheless, the plaintiffs established a likelihood of success on the merits of the FERPA claims, resulting in an injunction against certain illegal *distribution* of SSNs by Rutgers.[155] The court explained that nonconsensual distribution of education records to fellow students, by a school receiving federal funds, violated FERPA.[156] Thus, since the *Krebs* plaintiffs showed that the school used SSNs on attendance rosters and

148. *See* United States v. McKnight, 17 F.3d 1139, 1144 (8th Cir. 1994). The case also presents an interesting discussion of the legislative history of the criminal SSN abuse statute. *Id.* at 1144-45 & n.6.

149. *See* 42 U.S.C. § 408(a)(8) (1994).

150. *See* 18 U.S.C.A. § 2725 (West Supp. 1996); 42 U.S.C.A. § 1320d-6 (West Supp. 1997).

151. 20 U.S.C. § 1232g (1994).

152. *Id.* § 1232g(b)(1). Moreover, although there is no explicit private cause of action under FERPA, courts are unanimous in holding that an action charging a substantive violation of FERPA can be maintained through a § 1983 lawsuit. *See, e.g.*, Fay v. South Colonie Sch. Dist., 802 F.2d 21, 33 (2d Cir. 1986); Krebs v. Rutgers, 797 F. Supp. 1246, 1257-58 (D.N.J. 1992).

153. *Krebs*, 797 F. Supp. at 1258.

154. *See* Klein Ind. Sch. Dist. v. Mattox, 830 F.2d 576 (5th Cir. 1987).

155. *See Krebs*, 797 F. Supp. at 1256-59. Finding that the university's professors had a pattern or practice of releasing SSNs to unauthorized persons—namely, other students—the court enjoined the use of SSNs on any sheet used by a professor for class attendance. *Id.* at 1258.

156. *Id.* at 1258.

grade listings, available to any students in the class, the court enjoined this practice.[157] FERPA therefore remains one of the few promising sources for protection from SSN distribution; unfortunately, it does little to prevent the practice of collecting SSNs.

E. Other Federal Statutes

Other federal statutes now in effect offer some protection to the abuse of SSNs or other personal identifiers. Unfortunately, their protections are often limited. One example is the Right to Financial Privacy Act.[158] This 1978 enactment covers "any record held by a financial institution pertaining to a customer's relationship with the financial institution."[159] The act applies only to the federal government, and it prohibits the Government from acquiring bank records, unless the procedures set forth in the Act are followed.[160] Yet, the exceptions in the act are numerous. While it might prevent a federal agent from swooping down on a bank to get records, or from further disseminating improperly obtained records, it does not address actions of the bank itself dealing with customer records,[161] nor does it address state law enforcement conduct.

Another federal statute criminalizes the release of information concerning the individual videotapes that a person may rent for viewing.[162] Still another limits the type of information that cable television companies may collect.[163] Although it is unclear whether SSNs are routinely kept with either such records, these statutes because they are typical in American law dealing with privacy protection. They are "relatively strict but objectively tame."[164] They allow Congress to state that they have

157. *Id.* at 1262.

158. 12 U.S.C. §§ 3401-422 (1994).

159. *Id.* § 3401(2).

160. *See id.* § 3403(a). Generally, unless there is a customer authorization, administrative subpoena, search warrant, or judicial subpoena, bank records may not be released to the Government. *See id.* §§ 3403-07. Unless exigent circumstances exist, a customer must be told promptly of the disclosure of records. *See id.* at § 3409.

161. For example, a bank employee may volunteer information to the Government. *See id.* § 3403(c). Moreover, the Act does not apply to disclosures to bank regulators, nor to any acquisition of information by the Internal Revenue Service under Title 26. *See* 12 U.S.C. § 3413(a)(c).

162. *See* 18 U.S.C. §§ 2710-11. The statute allows releasing information about the *categories* of videotapes that a person rents, e.g. "adult," "horror," "romantic comedy," etc., unless the customer specifically objects. In addition, the statute does not address the collection of this information, but only its distribution. *See id.*

163. *See* 47 U.S.C. § 551 (1994). The statute declares that subscriber information generally may not be disclosed to other entities, but then makes exceptions if the customer assents or if it is for the cable company's "legitimate business activities." *Id.* § 551(c)(2). The Act also provides for annual notifications to consumers of their rights and provides an opportunity for a customer to "opt out" of certain disclosures. *Id.*

164. Fenrich, *supra* note 11, at 966.

addressed privacy concerns, but the statutes are riddled with exceptions, making them ineffective.[165] Indeed, the Fair Credit Reporting Act ("FCRA"),[166] which addresses credit bureaus and the records they keep—records which indisputably include SSNs—has been derided as too weak.[167] The *absence* of federal legislation regulating other areas is perhaps even more important that this listing of what federal law does protect. In sum, "[t]he law imposes almost no restrictions on the sale of . . . information about employment, criminal records, tenants . . . [or] insurance files."[168]

F. State Laws Governing SSN Use

Commentators have criticized state laws governing information privacy as "fail[ing] to provide comprehensive privacy protection."[169] The failings of state law may come about in one of two ways. First, state government agencies, given the option of using the SSN or not using the SSN as an identifier, generally prefer the use of the SSN, thus making the policy choice of using the more intrusive option. An example of this comes from the use of SSNs in driver licenses. Second, state laws in regard to privacy of records are typically weak. Despite the absence of meaningful federal privacy protections, the states have generally failed to step in with laws of their own.[170]

State recordkeeping laws may have the effect of limiting SSN use by stating that SSNs are not among the records that may be disclosed to other agencies, or to the public, under a state's "Sunshine Law" or simi-

165. The same is true of the legislation restricting access to drivers' records. *See supra* notes 79 to 86.

166. *See* 15 U.S.C. § 1681 (1994).

167. *See* Shorr, *supra* note 29, at 1785 ("In practice . . . the FCRA permits credit bureaus and their customers to exchange large quantities of information with impunity."). There have been proposals to amend FCRA to give consumers greater access to their credit files and to give them the choice of "opting out" of marketing lists, but these legislative initiatives have not been successful. *See* Prowda, *supra* note 7, at 762; *see infra* text accompanying note 268. In fairness, FCRA forbids totally indiscriminate access of SSNs by members of the public. *See* Prowda, *supra* note 8, at 762. Still, the entities that can receive SSNs legally number in the millions. *See id.*

168. Bibas, *supra* note 25, at 595.

169. Fenrich, *supra* note 11, at 970.

170. Texas is an example of a state with weak privacy laws. *See, e.g.*, Industrial Foundation of the South v. Texas Industrial Accident Bd., 540 S.W.2d 668, 681 (Tex. 1976) (holding an employees' workers' compensation files, which included SSNs, are not within the scope of records protected under privacy laws). *See also* Star-Telegram, Inc. v. Walker, 834 S.W.2d 54 (Tex. 1992) (declaring SSN of rape victim kept in police blotter was subject to public inspection under records laws); Houston Chronicle Pub. Co. v. City of Houston, 531 S.W.2d 177, 180, 188 (Tex. App. 1975) (holding police blotter which includes suspect's SSN is public record, while arrestee's personal history and prior arrest record is protected by the "enforceable right of privacy" that Texas recognizes).

lar statute. *Doe v. Registrar of Motor Vehicles* is illustrative of this practice.[171] The *Doe* plaintiffs challenged Massachusetts' practice of disclosing, *inter alia*, the SSN, date of birth, and height of all applicants for driver licenses.[172] Under Massachusetts privacy laws,[173] the state had to persuade a court that the benefits of disclosure would outweigh the intrusion into privacy, a burden it did not satisfy in *Doe*.[174] Thus, *Doe* is illustrative of a framework in which a court must be convinced of the validity of an executive or legislative determination to disseminate an SSN. It does not curtail requesting SSNs, only their distribution.

California's Information Practices Act[175] and Virginia's Privacy Protection Act of 1976[176] also address recordkeeping by government. They address governmental actions as well as actions taken by private entities performing service for the government under contract.[177] The California statute limits the disclosure of governmental records[178] while the Virginia statute has been interpreted to impose limits only on collection, maintenance, and use of personal data, not its dissemination.[179] Both statutes require that before personal information is solicited from an individual, the information collector must furnish a comprehensive disclosure of the purposes and usage's of the information.[180]

Virginia law goes somewhat further in making it unlawful for any government agency or any private entity under contract with the agency to require a person to submit their SSN as a condition of performing an activity or receiving a service.[181] The only exception to this rule is where federal or state law requires the disclosure.[182] Thus, Virginia law on this subject is unusual in two ways: it specifically addresses the SSN, and its provisions also reach some private actors. In fact, it is one of few statutes that addresses generally the collection or use of SSNs by private

171. 528 N.E.2d 880 (Mass. App. Ct. 1988).

172. *See id.* at 881.

173. *See id.* MASS. GEN. LAWS ANN. Ch. 66A, § 1 (West 1997).

174. *See Doe*, 528 N.E.2d at 886.

175. CAL. CIV. CODE §§ 1798 to 1798.78 (West 1997).

176. VA. CODE ANN. §§ 2:1-377 to 386 (Michie 1997).

177. *See* CAL CIV. CODE § 1798.19; VA. CODE ANN. §2.1-379(6).

178. *See* CAL CIV. CODE § 1798.24.

179. *See* Hinderliter v. Humphries, 297 S.E.2d 684 (Va. 1982). The law requires certain procedural steps to be taken before dissemination, but does not generally impose limitations on dissemination.

180. *See* CAL. CIV. CODE § 1798.17; VA. CODE § 2.1-382.

181. *See* VA. CODE ANN. § 2.1-385.

182. Ironically, however, Virginia requires that an individual's social security number appear on their driver's license and on their voter registration. *See, e.g.*, VA. CODE ANN. § 46.1-375 (driver's license); § 24.1-72.2 (voting). The requirement of SSN disclosure as a condition to voting was held unconstitutional in *Greidinger v. Davis*, 988 F.2d 1344 (4th Cir. 1993), as an undue burden on an individual's right to vote. *See id.*

entities.[183] Still, statutes like these are deficient in that they do not impose meaningful limits on SSN use, collection, or disclosure generally.

G. The Federal Constitutional Right of Privacy

The federal constitutional "right of privacy" has many components, including a right of personal autonomy and bodily integrity.[184] Decisions such as *Roe v. Wade*[185] are illustrative of this branch of federal privacy law. The other branch of the federal right of privacy is a right to "informational privacy."[186] Although recognized to exist, courts have not been ready to find rights of "informational privacy" in most circumstances. For example, in *Whalen v. Roe*, the Supreme Court rejected a challenge to a law requiring physicians to inform the state of the names of patients for whom they prescribed certain "Schedule II" drugs such as cocaine, opium, or methadone.[187] The state would keep these records in a centralized file, and if their names were disclosed, the plaintiffs feared that such disclosure would harm their reputation and stigmatize them as drug users.[188] The Court explained that given the methods being used to keep the information secure, there was no "sufficiently grievous threat" to the constitutional right to "avoid disclosure of personal matters."[189] Since modern medical recordkeeping includes SSNs, opponents of SSN use would find this case to be an obstacle although the case does seem to require some meaningful security against indiscriminate access to SSNs.

---

183. *See id.* While many statutes address the collection and use of records that *include* SSNs, e.g. credit, medical, or insurance records, the Virginia statute is unique in that it addresses the subject of SSN numbers specifically. *Id.*

184. *See* Dan L. Burk & Jennifer A. Hess, *Genetic Privacy: Constitutional Considerations in Forensic DNA Testing*, 5 George Mason Civ. Rts. L.J. 1, 27-33 (1995).

185. 410 U.S. 113 (1973).

186. *See* Burk & Hess, *supra* note 184, at 34-38. This right allows an individual to protect against the disclosure of personal matter and to be free from government surveillance and intrusion. *See also* Nixon v. Administrator of General Services, 433 U.S. 425, 433 (1977) (stating that the right includes a "legitimate expectation of privacy in . . . personal communications."). This right can be defeated if a court determines that the "privacy interests outweigh those interests benefited by disclosure of the" information. State *ex rel.* Beacon Journal Publishing Co. v. Akron, 640 N.E.2d 164, 167 (Ohio 1994). In sum, the federal right to informational privacy seems to involve a low level of scrutiny, not the stricter form reserved for more fundamental rights. *Accord In re* Adams, 214 B.R. 212 (9th Cir. B.A.P. 1997).

187. 429 U.S. 589, 598-604 (1977). *See also Nixon,* 433 U.S. at 433 (rejecting President Nixon's a claim of privacy of his presidential records since the "important public interest" in disclosing the materials outweighed the President's privacy interests, especially in light of his public-figure status).

188. *See* Whalen, 429 U.S. at 595, 600.

189. *Id.* at 599, 602. This *constitutional* right to avoid disclosures is presumably enforceable only upon governmental actors. *See id.*

Challenges to governmental collection and disclosure of financial records have also not fared well. In *United States v. Miller*, the Court considered a Fourth Amendment objection to the required disclosure of financial information by banks.[190] The court rejected the notion of a constitutionally cognizable privacy interest in financial information, holding that there is no "reasonable expectation of privacy" in these records.[191]

An early challenge to SSN collection, on constitutional grounds, was *Meyer v. Putnam*.[192] In *Meyer*, a Colorado statute required a voter to give her SSN to an election clerk before voting. The Colorado Supreme Court gave a narrowing construction to the statute, holding that it only authorized the clerk to request the SSN, and did not authorize the clerk to deny a person's vote upon their refusal to furnish the number. A broad construction would not be given, the court explained, because to construe it broadly and to allow denial of the vote would make the statute unconstitutional.[193] Still, other courts were relatively unresponsive to SSN collection. In *Doyle v. Wilson*, a federal court deciding a constitutional challenge to SSN collection opined that "mandatory disclosure of one's social security number does not so threaten the sanctity of individual privacy as to require constitutional protection."[194]

---

190. 425 U.S. 435, 442 (1976).

191. *Id.* Other Fourth Amendment objections to disclosure of financial information have met with a similar fate. *See* Jack W. Campbell IV, Note, *Revoking the Fishing License: Recent Decisions Place Unwarranted Restrictions on Administrative Agencies' Power to Subpoena Personal Financial Records*, 49 VAND. L. REV. 395, 422-25 (1996). In addition, claims that financial disclosures required by conflict-of-interest statutes were unconstitutional have also been spurned by courts. *See id.* at 422-23. Also, a subpoena of a physician's records was upheld, despite the fact that personal medical information of patients (who were not under investigation) would be reviewed by investigators. *See id.* at 423. In that case, however, the court imposed a protective order on the records, limiting disclosures to certain agents. *See id.*

192. 526 P.2d 139 (Colo. 1974).

193. *See id.* at 140-41.

194. 529 F. Supp 1343, 1348 (D. Del. 1982). *See also* Cantor v. Supreme Court of Pennsylvania, 353 F. Supp. 1307, 1321-22 (E.D. Pa. 1973) ("[I]t is impossible for me to perceive how requiring a [SSN] either threatens the future of Western civilization or deprives lawyers of basic individual dignity and certainly it does not rise to a breach of any federal constitutional rights .... A lawyer has no sacred right to keep inviolate the privacy of his [SSN]"); Conant v. Hill, 326 F. Supp. 25, 26 (E.D. Va. 1971) (not unconstitutional to require SSN on driver's license application), *aff'd*, 487 F.2d 1394 (3d Cir. 1973); Chambers v. Klein, 419 F. Supp. 569 (D.N.J. 1976) (not unconstitutional to require welfare recipients to furnish SSNs), *aff'd*, 564 F.2d 89 (3d Cir. 1977); *In re* Adams, 214 B.R. 212 (B.A.P. 9th Cir., Oct. 10, 1997) (holding that neither the equal protection clause nor the due process clause invalidate the statutory requirement that nonattorney bankruptcy preparers place their SSNs in court filings). These cases are presented here solely for their discussions of the federal constitutional holdings. In fact, these results could very well differ if the practices they challenged were attacked using Section 7 of the Privacy Act instead of the Constitution.

More recent cases, however, have been more protective of privacy than decisions like *Doyle*. The case of *Beacon Journal Publishing Co. v. Akron* is illustrative of increased privacy.[195] The case involved an attempt by a newspaper to obtain payroll records of city employees.[196] The newspaper explicitly asked for SSNs as part of the records to be furnished.[197] The Ohio Supreme Court found that disclosure of the individual employees' SSNs "would violate the federal constitutional right to privacy" and therefore ordered that they not be disclosed.[198]

The *Beacon Journal* court also made reference to another recent case—*Greidinger v. Davis*,[199] a challenge to Virginia's statutory requirement that an SSN appear on a voter's registration form. *Greidinger* does *not* hold that either SSN collection or distribution is itself a violation of a constitutional right of privacy. Nevertheless, the district court held that Virginia had failed to comply with Section 7(b) of the Privacy Act by not listing whether the disclosure was mandatory or not, and listing how the SSN would be utilized.[200] Turning to dissemination, the court held that by making SSNs available on the voter registration cards subject to public inspection, Virginia was "plac[ing] a burdensome condition on the exercise of the fundamental right to vote."[201] Because this burden was substantial, the court reasoned that strict scrutiny was applicable.[202] Virginia's proffered justification for SSN collection and disclosure—pre-

195. State *ex rel.* Beacon Journal Publishing Co. v. Akron, 640 N.E.2d 164 (Ohio 1994).

196. *See id.* at 165-66. *See also* News Group Boston, Inc. v. National R.R. Passenger Corp., 799 F. Supp. 1264, 1272 (D. Mass 1992) (denying newspaper's request for the SSNs of Amtrak employees since it would be a type of "personnel file . . . the disclosure of which would constitute a clearly unwarranted invasion of personal privacy" and hence exempt from disclosure under the Freedom of Information Act, 5 U.S.C. § 552b(b)(6)).

197. *See Beacon Journal*, 640 N.E.2d at 165-66.

198. *Id.* at 166. The court also relied upon the enactment of Section 7 as "creat[ing] an expectation of privacy in the minds of city employees concerning the use and disclosure of their SSNs." *Id.* at 168. Despite all the instances in which SSNs can be collected, it is welcome that this court found a pro-privacy policy in the enactment of section 7. Still, the court's refusal to rely on Section 7 as a separate ground for its decision is entirely proper. That statute only governs requests for the SSN, not dissemination.

199. 988 F.2d 1344, 1348 (4th Cir. 1993) (noting that plaintiff's challenge was not to the state's receipt and internal use of SSNs).

200. *See id.* at 1347. This aspect of the holding was not appealed. *See id.* In another election-law case, *Libertarian Party of Kentucky. v. Ehrler*, 776 F. Supp. 1200 (E.D. Ky. 1991), the court struck down a requirement that a each voter signing a political candidate's nominating petition place their SSN on the petition. The court held that since no federal authorization existed for the use of SSNs in elections, Section 7 of the Privacy Act barred Kentucky from imposing the requirement. *See id.* at 1209. In fact, Kentucky officials conceded their statute's illegality shortly after the suit was brought; they had apparently flagrantly disregarded the federal requirement when they passed the law just two years before. *See id.*

201. *Greidinger*, 988 F.2d at 1348.

202. *See id.* at 1352.

vention of voter fraud—was found to be a compelling state interest.[203] Ultimately, though, the court reasoned that the requirement of keeping SSNs available for public inspection was not "narrowly tailored" to the state interest that was advanced.[204] Accordingly, the court barred further dissemination of voters' SSNs.[205] Thus, *Greidinger*'s specific holding is that the public availability of SSNs is unconstitutional only because it burdens another fundamental right: the right to vote, not because it is *per se* unconstitutional.[206]

H. The Express Right of Privacy in Certain State Constitutions

Ten states explicitly refer to a right of individual privacy in their state constitutions[207] and unlike those in federal constitution, the rights guaranteed by these codes may be enforceable against private actors.[208] Still there is very little law on whether a state constitutional right to informational privacy exists, and if so, what is its scope. The Alaska Supreme Court struck down a statute requiring a physician running for public office to disclose all patients who paid $100 or more to his medical practice, holding this would violate the patients' rights of privacy.[209] In addition, the California Supreme Court has noted that its constitution is intended to prevent "overbroad collection and retention of unneeded personal information."[210] However, Florida's decisions on informational privacy have not been very protective of this right despite an express constitutional provision regarding "privacy" generally.[211] In sum, whether state constitutions recognize a right of informational privacy, and it is still unclear. In addition, none of these cases dealt explicitly

---

203. *See id.* at 1354.

204. *See id.*

205. *See id.*

206. *See id. Accord* Pontbriand v. Sundlun, 699 A.2d 856, 870 (R.I. 1997) (discussing the release of bank depositors' files, which included SSNs, "we are convinced that any *constitutional* right to avoid disclosure of information held in government files based upon the right to privacy must be grounded in a fundamental right clearly tied to a specific constitutional privacy right, the exercise of which would be impeded by the release of such information.").

207. *See* Prowda, *supra* note 7, at 739 & n.223.

208. *See* White v. Davis, 533 P.2d 222, 234 (Cal. 1975) (commenting, in dicta, that the California constitution's right to privacy prohibits "overbroad collection and retention of unnecessary personal information by government and business interests").

209. *See* Marc Silverstein, Note, *Privacy Rights in State Constitutions*, 1989 U. Ill. L. Rev. 215, 230 (citing Falcon v. Alaska Pub. Offices Comm., 570 P.2d 469, 480 (Alaska 1977)).

210. *Id.* at 236 (citing White v. Davis, 533 P.2d 222, 234 (Cal. 1975)).

211. *See* Overton & Giddings, *supra* note 6, at 39-40. For example, it is limited to governmental actions only. *See id.* at 42. Additionally, plaintiffs seeking constitutional protection under a right of informational privacy have not fared particularly well in court proceedings. *See id.* at 39-41 (collecting cases).

with SSNs. Therefore, with the possible exception of the California holdings, there is little precedent to suggest application of a state constitutional right of privacy to bar SSN collection, use, or dissemination, but it should always be considered as a potential means of attack by those challenging such requirements.[212]

I. THE COMMON-LAW PRIVACY TORTS

Virtually all states in the United States recognize a right of privacy, either through statutes or decisions.[213] According to Section 652A of the *Restatement (Second) of Torts*, the common law right of privacy has four distinct parts.[214] In the context of controlling SSN use and abuse, two of these come to mind: the misappropriation tort and the public disclosure of private facts tort.

Two recent decisions show that an action for public disclosure of private facts is becoming useful for controlling SSN abuse. Under this tort, a litigant must show that a person has made public a matter concerning the private life of another, and that the matter publicized would be highly offensive to a reasonable person and not of legitimate concern to the public.[215] This tort has generally only been used for highly embarrassing personal facts such as sexual or medical matters; given this judicial interpretation of the tort, and the widespread dissemination of SSNs, it might be difficult for a plaintiff to show that SSN collection or dissemination would be "highly offensive." Nevertheless, *Pontbriand v. Sundlun* reversed a summary judgment and allowed a jury to consider whether the release to the media of banking records which included name and SSNs was in violation of the tort-based right to prevent "public disclosure of private facts."[216] In *Tacoma Public Library v. Wossner*, a Washington state court considered a citizen's request for the records of public library employees, including, among other things, the employees' "identification numbers."[217] The court allowed the disclosure of names, salaries and benefit information, but treated the request for their SSNs differently. It specifically held that "the disclosure of a public employee's social security number would be *highly offensive to a reasonable person*

212. *See* William J. Brennan, Jr., *State Constitutions and the Protection of Individual Rights*, 90 HARV. L. REV. 489, 491 (1977) (state constitutions can be "a font of individual liberties, their protections often extending beyond those required by . . . federal law.").

213. *See* FREEDMAN, *supra* note 6, at 5.

214. *See* RESTATEMENT (SECOND) OF TORTS, § 652A (1977). They are: (1) unreasonable intrusion on the seclusion of another or intrusion by physical or mechanical means; (2) misappropriation of a person's name and likeness; (3) putting a person in a false or unfavorable public light; or (4) public disclosure of private facts.

215. *See* RESTATEMENT (SECOND) OF TORTS, § 652D (1977).

216. 69 A.2d 856, 865 (R.I. 1997).

217. *See* Tacoma Public Library v. Wossner, 951 P.2d 357 (Wash. Ct. App. 1998).

and not of legitimate concern to the public."[218] It would be highly offensive, the court ruled, because it would violate the right to not disclose "intimate details of one's personal and private life" and more generally, a "worker's right to be let alone."[219] It was not of legitimate concern to the public, the court continued, because any need for the public to oversee the expenditure of tax dollars through open records, could be performed just as effectively without SSNs.[220]

The Tacoma Library appeal dealt with Washington's open record's statute and was not a tort-based challenge. However, its declaration that indiscriminate, public SSN dissemination is something highly offensive to the reasonable person is an admirable ruling, and an extremely accurate statement in light of the reality of how SSNs can be abused and the public's attitude and awareness of that fact. This case would obviously be a valid precedent in a tort-based challenge to SSN collection because it holds directly that the Restatement's elements of the public disclosure of private facts are satisfied by the dissemination of SSNs.

The misappropriation tort may also show more promise because it has been the one used most frequently in informational privacy litigation and the one "most likely to provide protection against unauthorized dissemination of personal information."[221] According to the Restatement, the tort is committed when one person "appropriates, to his own use or benefit the name or likeness of another."[222] The tort protects the individual's interest in "the exclusive use of his own identity, *in so far as it is represented by his name or likeness.*"[223] Applying the plain terms of the Restatement, it might be easy to conclude that when a commercial enterprise sells a mailing list that includes a given person's name, that enterprise commits the misappropriation tort. Yet, none of the information privacy cases litigated under this tort have been successful.[224] For example, in *Shibley v. Time,* magazine subscribers brought an action

218. *Id.* at 365 (emphasis added) (quoting Progressive Animal Welfare Society of Washington v. Univ. of Washington, 884 P.2d 592 (Wash. 1994).

219. *Id.* at 364-65 (quoting Dawson v. Daly, 845 P.2d 995 (Wash. 1993) and Painting Indus. of Hawaii Mkt. Recovery Fund v. United States Dept. of Air Force, 26 F.3d 1479, 1483 (9th Cir. 1994)).

220. *See id.* at 366.

221. Fenrich, *supra* note 11, at 973 (footnote omitted).

222. RESTATEMENT (SECOND) OF TORTS, § 652C. It does not forbid "incidental" uses of a person's name, such as in a book or a newspaper, but rather the exploitation of the "commercial . . . value associated with the name." *Id.,* cmt. d.

223. *Id.,* cmt. a (emphasis supplied).

224. *See* Fenrich, *supra* note 11, at 989-94 (discussing cases which in which "some form of the [mis]appropriation tort was unsuccessfully used to stop the distribution of personal data"). While none of the cases involved SSNs, their analysis is still instructive because they involved personally identifiable data. *See also* Bibas, *supra* note 25, at 597 ("courts have usually rejected privacy-tort claims based on information privacy") (citing Santiesteban v. Goodyer Tire & Rubber Co., 306 F.2d 9, 1 (5th Cir. 1962)); Overton & Giddings,

against Time for selling mailing lists and personality profiles to other direct-mail advertisers.[225] The court held that the names had to have been displayed to the public in order for the subscribers to claim a tortious invasion of privacy.[226] Other cases have also been unsuccessful.[227] However, even if these cases had been successful, they would not necessarily have been successful in controlling SSN dissemination *per se*. Rather, since the misappropriation tort only protects the identity insofar as it is represented by name or likeness, the SSN is not specifically within the scope of the protection of this tort. Yet, the theory is still valuable for protecting SSNs because if a name cannot be commercially disseminated on a mailing list, neither can a name linked with an SSN be disseminated. The unfortunate[228] rejection of the theory that it is tortious to sell a person's name on a mailing list without affirmative consent or compensation ought to be reconsidered, and if it is, it will plainly benefit advocates of SSN privacy as well. Later in this paper, the idea courts should use this tort more expansively to protect individuals' privacy in their social security numbers will be developed further.

J. Religion-Based Claims

Persons claiming a religious objection to the use of a SSN have been generally unsuccessful in their efforts. The leading case in this regard has been *Bowen v. Roy*.[229] In *Bowen*, the parents of a Native American child were recipients of benefits pursuant to the Aid to Families with Dependent Children ("AFDC") and the Food Stamp programs.[230] The Pennsylvania agency charged with administering the program informed the parents that they had to provide the child's SSN and if they failed to do so, any benefits they received on behalf of the child would be eliminated.[231] The parents stated that according to their Native American religious beliefs, widespread use of an SSN would rob the spirit of the child.[232] After a hearing, the district court granted the plaintiffs much of the relief they were seeking, enjoining the government from cutting off benefits and barring the use or the dissemination of the SSN by the De-

supra note 6, at 44 ("this tort generally provides relief in the area of advertising rather than in the area of data collection and sales.").

225. 341 N.E.2d 337, 339-40 (Ohio Ct. App. 1977).

226. *See id.*

227. *See, e.g.*, Dwyer v. American Express Co., 652 N.E.2d 1351 (Ill. App. Ct. 1995).

228. For a thorough criticism of these decisions, see Fenrich, *supra* note 11, at 988-91.

229. 476 U.S. 693 (1986) (5-4 decision).

230. *See id.* at 695.

231. *See id.* (citing 42 U.S.C. § 602(a)(25) (for AFDC program) and 7 U.S.C. § 2025(e) (for Food Stamp program)).

232. *See id.* at 696.

partment of Health and Human Services.[233] The Supreme Court, however, vacated the injunction. Chief Justice Burger's plurality opinion stated that the court would not apply strict scrutiny—the test normally used for Free Exercise Clause claims—to this case.[234] Rather, the court opined that this law, requiring the furnishing of an SSN, was "wholly neutral in religious terms and uniformly applicable."[235] According to the plurality, individuals may have their religious beliefs infringed by such laws, but that was not enough to invalidate them.[236] Such laws merely require religious adherents to choose between following their beliefs and receiving government benefits and do not *per se* force them to disregard their beliefs. These types of laws need only satisfy rational-basis review,[237] which the court found satisfied in this case.[238] As such, the injunction was inappropriate and was vacated.

Thus, this effort to control SSN use by reference to religious beliefs was unsuccessful. In addition, cases litigated under the Religious Freedom Restoration Act[239] which was declared unconstitutional in 1997,[240] did not yield success in controlling government's use of SSNs.[241] Similar cases in other jurisdictions have also been unsuccessful.[242]

---

233. *See* Roy v. Cohen, 590 F. Supp. 600, 614 (M.D. Pa. 1984), *vacated and remanded sub nom.* Bowen v. Roy, 476 U.S. 693 (1986).

234. *See* Bowen v. Roy, 476 U.S. at 707.

235. *Id.* at 703.

236. *See id.* at 706.

237. Although the court did not specifically articulate rational basis review as the appropriate legal framework, it used traditional rational basis language, analyzing whether "a legitimate and important public interest" was presented, and whether the law was "a reasonable means of promoting that goal." *Id.* at 709.

238. *See id.* at 709-12.

239. 42 U.S.C. §§ 2000bb-1 to 5 (1994). Under RFRA, claims that a government practice impinges on the right to free exercise of religion will prevail if the government practice is not narrowly tailored to achieve a compelling governmental interest. *See* 42 U.S.C. 2000bb-1.

240. *See* City of Boerne v. Flores, 117 S. Ct. 2157 (1997).

241. *See, e.g., In re* Floyd, 193 B.R. 548 (N.D. Cal. 1996). In *Floyd*, a bankruptcy petition preparer, who was required to place his social security number on documents filed with the court, refused to do so. As justification for this, he asserted his belief that a social security number was an identifier—"the mark of the beast" which is discussed in New Testament biblical prophecies. *Id.* at 551. As such, his religious beliefs forbade him to use this number. *See* REVELATIONS 13:16 & 14:9-10 (discussing the "mark of the beast" and its significance in biblical prophecies). The *Floyd* court first rejected the claim that either constitutional privacy rights or free exercise rights were violated by the statutory requirement of placing the SSN on the pleadings. The court also rejected his claims under RFRA, finding that there was no substantial burden on his religious practices. *See Floyd,* 193 B.R. at 554-56.

242. *See* Penner v. King, 695 S.W.2d 887 (Mo. 1985) (holding there is no constitutional bar to state's collection of SSNs for driver licensing notwithstanding plaintiff's religious beliefs). *But see* Leahy v. District of Columbia, 833 F.2d 1046 (D.C. Cir. 1987). *Leahy* held that the requirement that an SSN be obtained and disclosed in order to receive a driver's

IV. PROPOSED LEGAL REMEDIES FOR SSN USE AND MISUSE

A. Problems with Existing Law

The earlier discussion showed that with respect to collecting SSNs from individuals (1) federal law does not bar private actors from requesting SSNs or refusing to do business with someone if they refuse; and (2) state laws, although reaching a few private actors, contain no general prohibitions against SSN use or collection. The analysis also shows that governmental use of SSNs is forbidden by Section 7 of the Privacy Act unless an exception applies, but that over the years Congress has made so many exceptions, that the collection of SSNs in government is quite widespread. This is the case for two reasons: Congress has passed many mandates of SSN use, and where states or private actors are left to decide whether or not to require the SSN, these entities generally choose to use it.

With respect to using and disseminating SSNs, the law is somewhat more unprotective of privacy rights, but is still quite unsatisfying to privacy advocates. While federal statutes like FERPA or some states' informational privacy laws contain restrictions on information dissemination, the fact remains that governmental dissemination of personal identifying numbers is still widespread, and limits on private actors are also virtually nonexistent.

B. Why Allow or Restrict SSN Collection and Use?

There are a number of arguments both for and against a prohibition on the collection and use of personal information generally. Many of these arguments are highly applicable to SSN use as well. It has been pointed out, for example, that when financial and buying habit information about consumers is disseminated, deserving consumers may obtain lower-interest credit because creditors will identify those with good credit habits.[243] For this objective to be achieved, financial information (including SSNs) will have to be regularly shared, as it is now in the case of credit reports. In addition, direct-mail marketers can target likely consumers more accurately. This, in turn, will lower costs and paper usage, resulting not only in cost savings but environmental benefits as well.[244] Achieving this goal also requires extensive collection and sharing of personal information. Similarly, by achieving a high degree of information sharing, the citizen's opportunities to be anonymous also

---

license is a substantial burden on the free exercise of religion for adherents to a theology including "mark of the beast" beliefs. *Id.* at 1049. The case was remanded for further proceedings. *See id.*

243. *See* Prowda, *supra* note 7, at 751.

244. *See* Froomkin, *supra* note 11, at 481 ("[T]he existence of large, interlinked databases is not inevitably bad for the consumer/citizen.").

decrease. According to this argument, anonymity is bad because one can use it to avoid punishment or accountability for illegal or immoral acts.[245]

Information sharing is also an "effective method of preventing fraud."[246] More specifically, SSNs are used to track down alimony and child support deadbeats, student loan defaulters, or people engaging in insurance fraud, more individuals can be apprehended. Since information sharing is arguably made more accurate by use of a number to identify each individual, then it is to be encouraged.[247] However, fraud can be committed easily and frequently by using a false SSN. This problem is exacerbated by the frequent reliance by others on the validity of the SSN presented, which also creates an independent basis for rejecting enhanced use of the SSN as a personal identifier. Consider, for example, the experience of the United States Immigration and Naturalization Service. So many aliens use false SSNs, that in its computer network, the numbers "are not used as a primary means of identification . . . [because] the numbers given are frequently fraudulent."[248]

Moreover, it is plain that business and government use numerical identifiers for all types of matters: taxation, banking and credit, and drivers licensing, to name a few. They do not identify people by reference to name alone. "Account number" usage, then, is pervasive. It is also equally clear that people have a limited amount of memory and cognition, and have a limited capability to remember multiple sequences of numbers. Therefore, it might be wise to have people identify themselves with a single number, rather than having to remember their account number for each and every business or government agency they interact with. Another commentator argues that the public's "right to know" what government is doing would be harmed by decisions that unduly re-

245. *See id.* at 402. *See also* McIntyre v. Ohio Elections Comm'n, 115 S. Ct. 1511, 1537 (1995) (Scalia, J., dissenting) (arguing that anonymity "eliminate[s] accountability" of citizens); Bibas, *supra* note 25, at 599 (stating that effective information sharing about employees or housing renters "rewards good tenants and employees and punishes defaulters and shirkers").

246. James J. Killerlane III, Note, *Finger Imaging: a 21st Century Solution to Welfare Fraud at our Fingertips*, 22 FORDHAM URBAN L.J. 1327, 1351 (1995).

247. This rationale may be the motivation behind a recent proposal in the House of Representatives to require an individual to submit an SSN to register to vote in federal elections. *See* H.R. 224, 105th Cong. § 2 (1997). This proposal would probably be quickly declared unconstitutional by any court following the rationale of *Greidinger v. Davis*, 988 F.2d 1344 (4th Cir. 1993), discussed *supra* at notes 199 to 206 and accompanying text.

248. United States v. Gomez, 38 F.3d 1031, 1033 n.3 (8th Cir. 1994). *See also* Chris Hibbert, *SSN FAQ Addendum* (last modified Oct. 29, 1997) <http://www.cpsr.org/cpsr/privacy/ssn/SSN-addendum.html> (containing an excellent discussion of the flaws of using SSNs as "keys," or access numbers in databases).

strict access to government records.[249] Specifically, it is argued that if courts interpret statutes like the FOIA, which prohibit disclosures of highly personal information like SSNs, too broadly, the public's rights will be harmed.[250]

On the other hand, restricting the collection, use, and dissemination of SSNs in the United States also has advantages. To begin, the notion that any "intrusion [into privacy] is demeaning to individuality, is an affront to human dignity."[251] Prevalent ideals of liberalism and democracy promote treating people as individuals, not as numbers. We associate the treatment of people as numbers with totalitarian regimes[252] and institutions,[253] not with the life of free and democratic people. Indeed, one court wryly noted the similarity between everyday life and the assignment of numerical identifiers to inmates, explaining that "the Court notes that the assignment of personal identification numbers is a part of modern life—prison life in particular."[254] The use of SSNs contradicts these basic ideals, that is, treatment of individuals as humans, not numbers. The pervasive use of SSNs also diminishes the property right in one's identity that every person has. Senator Dianne Feinstein has also explained that as a result of pervasive SSN usage, "people are losing control over their identities . . . [and] [o]ur private lives are becoming commodities with tremendous value."[255]

In addition, as use of personal identifiers increases, a citizen's opportunities for anonymity decrease. Anonymity has been recognized to promote a legitimate value—"protect[ing] unpopular individuals from retaliation—and unpopular ideas from suppression."[256] Thus, in a free political culture such as ours, the sharing of information about individu-

249. *See* Christopher P. Beall, Note, *The Exaltation of Privacy Doctrines Over Public Information Law*, 45 DUKE L.J. 1249 (1996).

250. *See id.* at 1265-66 (condemning decisions like *Sheet Metal Workers Int'l Assn. v. United States Air Force*, 63 F.3d 994 (10th Cir. 1995), which withheld SSNs from disclosure under its exemptions).

251. Krebs v. Rutgers, 797 F. Supp. 1246, 1259 (D.N.J. 1992) (quoting Edward J. Bloustein, *Privacy as an Aspect of Human Dignity*, 39 N.Y.U. L. REV. 962, 973 (1964)).

252. *See, e.g.*, GEORGE ORWELL, 1984, (part one, chapter III) (noting that the main character was known to the governing regime not by his first and last name but as "6079 SMITH W"). *See also* Alan C. Laifer, *Never Again? The "Concentration Camps" in Bosnia-Herzegovina: A Legal Analysis of Human Rights Abuses*, 2 NEW EUROPE L. REV. 159, 159 n.3 (describing how German Nazis would tattoo identification numbers on victims in their concentration camps for identification purposes).

253. *See, e.g.*, N.J. ADMIN. CODE tit. 10A, § 18-2.6(c) (1996) (providing that mail addressed to an inmate at a state or county correctional institution will be returned to sender if it lacks the "inmate's name *and number*" (emphasis supplied).

254. Carter v. O'Sullivan, 924 F. Supp. 903, 909-10 (C.D. Ill. 1996).

255. 143 CONG. RECORD S3293 (daily ed. Apr. 16, 1997) (statement of Sen. Feinstein).

256. McIntyre v. Ohio Elections Comm'n, 115 S. Ct. 1511, 1524 (1995).

als threatens some basic values of the culture. In sum, it is a battle between individual dignity and economics.

C. Legal Solutions to the Problem: Court Decisions

An analysis of current law reveals that while courts recognize that SSN dissemination may constitute an invasion of privacy,[257] these same courts will rarely authorize a remedy for such invasions. An exception seems to exist in decisions interpreting the FOIA or similar statutes. Using these statutes and cases decided under them, courts will generally exempt employees' SSNs from public disclosure.[258] Recent case law developing the public disclosure of private facts also shows promise. Still, the general path of the law has been for courts to permit SSN collection, use, and dissemination by government, imposing very few limits.[259]

Some current legal frameworks show an inability to solve the problems presented by the widespread use and dissemination of SSNs. First, constitutional privacy law generally protects expectations of privacy that are reasonable. Can it be said that one has a "reasonable" ex-

257. *See* Swisher v. Dept. of Air Force, 495 F. Supp. 337, 340 (W.D. Mo. 1980), *aff'd*, 660 F.2d 369 (8th Cir. 1981) (holding that social security number disclosure constitutes "more than a minimal invasion" of privacy and that individuals' SSNs are exempt from disclosure under the Privacy Act). *See also* Aronson v. Internal Revenue Service, 973 F.2d 962, 968 (1st Cir. 1992) ("citizens have [a] 'strong privacy interest' in social security numbers, more than in 'home addresses'") (citing International Bhd. of Elec. Workers Local Union No. 5 v. Dep't of Housing & Urban Dev., 852 F.2d 87, 89 (3d Cir. 1988)).

258. Notable court decisions limiting employee SSN disclosure on the rationale of an exemption to FOIA disclosure include *News Group Boston, Inc. v. National R.R. Passenger Corp.*, 799 F. Supp. 1264, 1272 (D. Mass 1992) (denying newspaper's request for the SSNs of Amtrak employees since it would be a type of "personnel file . . . the disclosure of which would constitute a clearly unwarranted invasion of personal privacy and hence exempt from disclosure under [FOIA]"). *See also* State *ex rel.* Beacon Publishing Co. v. Akron, 640 N.E.2d 164 (Ohio 1994) (holding that even though FOIA did not control the case, under the rationale of courts deciding FOIA cases, public disclosure of employees' SSNs to newspaper would be an invasion of privacy); Doe v. Registrar of Motor Vehicles, 528 N.E.2d 880, 888 (Mass. App. Ct. 1988) (relying heavily on federal Privacy Act precedent, Massachusetts law would be interpreted to bar public disclosure of drivers' SSNs).

The SSNs of taxpayers were also held exempt from public disclosure in *Aronson*. *See* 973 F.2d at 968. The plaintiff there was a lawyer who offered to find people who were owed tax refunds by the government. *See id.* at 963. He requested that the IRS furnish him with the names, last known addresses, and tax identification numbers of people who were owed refunds. *See id.* The IRS agreed to furnish the names, but denied his request for the other information, relying on the statutory exemptions to FOIA. *See id.* The First Circuit agreed with the IRS' decision, and refused to allow the release of street addresses. *See id.* at 964-66. The court also rejected Aronson's request for the tax ID numbers, explaining that "the same, or greater, protection attaches to this information as to street addresses." *Id.*

259. For example, Section 7 of The Privacy Act is riddled with exceptions, state constitutional law has not developed sufficiently to find a right of informational privacy, and federal constitutional law on both privacy and religion has been insufficient to protect from SSN abuse.

pectation of privacy in one's SSN? One would be hard-pressed to argue that an expectation of privacy in an SSN is truly reasonable any more.[260] As one civil libertarian explained, "the less privacy [people] have, the more [they are] used to not having privacy."[261] Many agencies, public and private, hold a person's SSN, that it borders on being so well-known as to approach a public record.[262] In addition, there are far too many ways in which one's SSN can in fact enter the public record. And "[a]n individual cannot expect to have a constitutionally protected privacy interest in matters of public record."[263] Thus, courts would be hard-pressed to limit SSN collection, disclosure, or dissemination by using the current framework for evaluating constitutional privacy rights, which are evaluated using a "reasonable-expectation-of-privacy" framework. More specifically, courts that are faced with interpretation of federal and state constitutions, instead of following these outdated frameworks, must recognize a right of informational privacy and protect it with the same vigor that other types of privacy, e.g., bodily-integrity and autonomy privacy, are enforced.

In sum, courts should be more solicitous of individual constitutional rights. Those recent decisions extending Common-Law privacy tort protections to SSNs need to be adopted and expanded in other jurisdictions as well. Perhaps, more importantly, courts should recognize that not only is distribution of SSNs tortious, but it is also tortious to require someone to disclose their SSN as a condition of doing business with them. Moreover, law should eliminate not only indiscriminate SSN dissemination, but also, indiscriminate solicitation of it. The privacy right to withhold SSNs cannot be limited by precedents that were decided before information was so freely disseminated, indeed before so many records could be obtained at the touch of a button. Basically, the doctrine of "reasonable expectation of privacy" presupposes that as technology develops and allows more invasions of privacy, reasonable expectations of privacy diminish. That is precisely the problem: privacy rights diminish with an increase in invasive technology. As technology improves, more privacy protections should be instituted. Further, constitutional privacy law should be re-examined to allow individuals greater control over an integral part of their identity—the SSN—and permit

260. *See* Killerlane, *supra* note 246, at 1349 ("Today, however, [SSNs] have become an integral part of all levels of government and private business . . . . Over time, Americans have come to accept the use of {SSNs] as part of their daily routine.").

261. Larini, *supra* note 23 (quoting Edward Martone, director of the American Civil Liberties Union of New Jersey).

262. *See, e.g.*, 143 CONG. REC. S3292 (daily ed. April 16, 1997) (statement of Sen. Feinstein) ("I found that my own [SSN] was accessible to users of the Internet. My staff retrieved it in less than 3 minutes.").

263. Doe v. City of New York, 15 F.3d 264, 268 (2d Cir. 1994).

some measure of individual dignity to be restored. In sum, the "reasonable expectation of privacy" framework has lost much of its viability and has been unable to meet the need for informational privacy in today's interlinked world.

Along these lines, courts should also take affirmative steps to prohibit SSN and name dissemination through more innovative use of the common law tort of misappropriation as there is sufficient precedent for expanding this tort to cover SSN disclosures. The tort punishes the commercial use of one's name or likeness. Thus, celebrities, alive or dead, retain rights to control others' use of their names or likenesses for commercial purposes. For example, if Elvis Presley's heirs[264] can prevent someone from using his name on a bar or restaurant to make money, why can't the ordinary citizen prevent the commercial use of his name through the sale of the name and SSN on a mailing list? In particular, direct-mail marketing entities may point out that the two types of name usage are dissimilar, but are they really? Both involve the use of one's name and personal characteristics to make money. The courts construing this issue, therefore, have been too cautious in construing the misappropriation tort[265] and should consider its expansion.

D. Legislative and Other Solutions to SSN Usage

If current judge-made law cannot solve the problems associated with SSN usage, other steps should be examined. Individuals who have concerns about the use and dissemination of their SSNs may be able to take a number of self-help measures such as limiting their disclosures or demanding to know how their information will be used.[266] Unfortunately, these self-help measures may be of limited efficacy. First, these individ-

264. *See, e.g.* Elvis Presley Enterprises, Inc. v. Capece, 950 F. Supp. 783, 801-02 (S.D. Tex. 1996). The case found that under certain circumstances heirs have an "inherent right . . . to control the commercial use of his identity." *Id.* at 801. Thus, when a person's name is used "to advertise . . . or for *some commercial purpose*," the tort of misappropriation occurs, and the offender can be held liable. *Id.* (emphasis supplied). The court found that Presley's rights of publicity, which exist in Texas during life as well as after death, were violated when the defendant called his night club "The Velvet Elvis" and derived profit from it. *See id.* at 801.

265. *See supra* notes 222-228 and accompanying text.

266. *See* Ann Cavoukian & Don Tapscott, Who Knows: Safeguarding your Privacy in a Networked World (1996). Among the steps recommended by the authors to limit disclosure of personal information are, (1) asking the requester what use will be made of the information; (2) minimize the amount of personal information given out; (3) demanding to know who will have access to the information furnished; (4) paying bills with cash, to minimize records kept as a consequence of using a credit or debit card; (5) do not furnish an SSN unless required by law. *Id. See also How to Keep Your Personal Information Personal: Tips from the Privacy Rights Clearinghouse*, 14 Cal. Reg. L. Rptr. 1 (1994) (furnishing similar suggestions to consumers on self-help measures they may take to safeguard personal data, including SSNs).

uals must educate themselves about the complex state and federal requirements for when SSNs have to be disclosed to government and when they need not be disclosed. Second, when dealing with non-governmental entities, people will have to be aware of the risk that they will be denied service if they refuse to provide the SSN. Finally, if an individual elects to opt-out of mailing lists, or credit offers, it will require the difficult and burdensome task of contacting the large number of information collectors and purveyors; opting out of one records system will not eliminate a person's file from other records systems.

Short of becoming a hermit and shutting off contact with the outside world, then, there is little prospect for individuals to truly ensure that personal information like the SSN remains private. Current legal frameworks will offer little assistance unless they are boldly expanded, and self-help may just require too much effort for too little gain in privacy. Thus, effective legislative solutions will provide the most effective way of controlling the abuse of personal identifiers such as the SSN.

An ideal legislative solution would control SSN collection, use and dissemination. Despite its shortcomings, recent legislation introduced by Senators Dianne Feinstein (D-Cal.) and Charles Grassley (R-Iowa) shows some promise.[267] A proposed bill in the Senate, Senate Bill 600, introduced on April 16, 1997, contains three main provisions. First, the bill amends the Fair Credit Reporting Act ("FCRA") to designate *any* identifying information about a person, specifically including the SSN, as items which cannot be released unless the customer explicitly consents or there is an inquiry for the credit report from a creditor or employer who has received a specific application from the consumer or prospective employee.[268] This will severely curtail the sale of names and SSNs by credit bureaus, and cure the large defect in the present FCRA statute allowing the practice.[269] Second, the bill closes a significant loophole in the Driver's Privacy Protection Act ("DPPA").[270] The proposal would eliminate SSNs from being used for most of the purposes now allowed under the DPPA. It would also bar the use of SSNs for marketing purposes, which is one of the most glaring exceptions in the DPPA.

The keystone of the proposed Senate Bill 600, however, is Section Three.[271] Section Three prohibits the sale, purchase, or exchange of an

267. *See* S. 600, 105th Cong. (1997). In the House of Representatives, an identical bill was introduced on June 6, 1997. *See* H.R. 1813, 105th Cong. (1997). The bill has 18 cosponsors.

268. *See* S. 600, 105th Cong. (1997), § 2.

269. S. 600 contains an exception: the name (but not the SSN) may be sold if the person has his or her name listed in a local telephone directory. *See id.*

270. *See* 18 U.S.C.A. §§ 2721-25 (West Supp. 1996); *supra* notes 79 to 86 and accompanying text.

271. *See* S. 600, 105th Cong. § 3 (1997):

SSN by any "person"[272] unless one of two exceptions applies. One exception states that if the subject of the information affirmatively consents after being informed of "all purposes for which the number will be used and the persons to whom the number will be known," the use will be permitted. The second exception is that use now authorized by an existing statute may legally be continued.[273] More importantly, the proposal bars any "person" from *using* the SSN or a derivative thereof, as an account number without informed and explicit written consent.[274] Violations of the act may be punishable civilly by either a private action, in which actual damages or $25,000 to $50,000 plus attorney's fees may be recovered; or in a civil enforcement action by the Social Security Administration, with penalties of $25,000 to $500,000 per violation.[275]

The legislation, then, eliminates much of the private dissemination of SSNs existing today. Quite wisely, it takes back a good deal of federal control over the federally-created SSNs. It also changes the current regime in which a person can choose *not* to have the information distributed (an opt-out system),[276] to a regime where a person must make an affirmative choice to have information distributed (an opt-in system). Still, there are shortcomings in the legislation. Indeed, there are more effective ways of controlling SSN abuse, either by amendment to the Feinstein/Grassley bill, or through other legislation.

The legislation does nothing to limit the collection of SSNs, either by government or private individuals. Although the limits on SSN *usage* and *distribution* in the bill may have the collateral effects of lessening SSN *collection*, this is only speculative. Any good SSN control legislation will limit the circumstances in which the SSN can be collected.

> No person may buy, sell, offer for sale, take or give in exchange, or pledge or give in pledge any information for the purpose, in whole or in part, of conveying by means of such information any individual's social security account number or any derivative of such number, without the written consent of such individual.

Id.

272. This would includes private entities, *see* 1 U.S.C. § 1 (1994) ("In determining the meaning of any Act of Congress, unless the context indicates otherwise— . . . the words "person" and "whoever" include corporations, companies, associations, firms, partnerships, societies, and joint stock companies, as well as individuals . . . ."), but it is unclear whether it would include state or local government agencies.

273. *See* S.600, 105th Cong. § 3 (1997). More specifically, if the use is now authorized by Section 7 of the Privacy Act or one of its exceptions found at 42 U.S.C. § 405 or § 6109 of the Internal Revenue Code, the use of such numbers for those enumerated purposes remains unaffected.

274. *See id.*

275. *See id. Cf.* 42 U.S.C. § 408 (criminal penalties for SSN misuse).

276. An example of this would be the current system in which credit bureaus and direct-mail marketers offer a customer the opportunity to have their name 'taken off the mailing list' sold by the bureau.

Closely related to this concern, the Feinstein/Grassley bill does not repeal any of the federal mandates of SSN collection. An example of these mandates was described earlier with reference to the pervasive use of SSNs in child support enforcement. Also, the bill does not repeal any of the federal grants of permission to use the SSNs, as occurs in the case of driver's licenses. Thus, since the legislation allows continuation of the tremendous amount of governmental SSN usage now authorized by statute, the bill is the legal equivalent of closing the barn door after the horse has run away. Both state and federal legislators should also consider reducing the number of instances in which the law mandates SSN usage, or permits its usage, both by government and by private entities.

The proposed legislation allows distribution of SSNs upon receiving the consent of the subject. But the proposal does nothing to limit how this consent can be obtained. More specifically, can the consent contemplated by this statute be obtained by burying such a provision in small print or in an adhesion contract? Or must consent be freely given, without conditions? Any legislation should state, tracking the language of Section 7 of the Privacy Act, that no person can be denied the right to make a contract with another, nor will any right, benefit or privilege be denied because of such an individual's refusal to disclose his SSN.

Furthermore, the legislation does nothing to require the destruction of numbers already collected. Indeed, SSNs collected by one way or another already exist in probably thousands of government and private databases. To ensure that SSNs are not distributed in violation of the law, any privacy legislation should require the destruction of existing SSNs, unless the individual freely consents to it being kept further.

V. CONCLUSION

In sum, these types of provisions should be placed in any privacy protection legislation if it is to have any real teeth. Will these solutions cost money? There is no doubt; restricting SSN usage means incurring monetary costs. But, there is a choice to be made, between economics and human dignity. Canada, for example, has made this choice, and limited the use of their national personal identifier, despite the significant cost to government.[277] Thus, there is precedent for making this choice in the United States. Living in this information society, people can be treated as numbers, or they can be treated as individuals. We have the technology to do the former, but the real question to be answered is whether we have the will to do the latter.

277. *See supra* note 13. *See also EU Data Protection Directive* (Oct. 1995) <http://www2.echo.lu/legal/en/dataprot/directiv/directiv.html> (describing the European Union's Directive protecting individual rights in relation to data collection and limiting the unfettered dissemination of such data).