NEVADA NEEDS A PRIVACY ACT: HOW NEVADANS ARE PARTICULARLY AT RISK FOR IDENTITY THEFT

Amy S. Scarborough*

I. INTRODUCTION

The use of the Social Security Number ("SSN") by both governmental agencies and private entities for various identification purposes is common and widespread.[1] Unfortunately, a "wealth of information"[2] is accessible through a person's Social Security number, which enables thieves to pilfer the identity of the SSN's owner and exploit and ruin his credit, name, and life. Indeed, the FBI declared identity theft "the fastest growing crime in the nation."[3]

Statistics demonstrate that the threat of identity theft is real. The Federal Trade Commission ("FTC") reports that about ten million Americans annually are victims to identity thieves who open accounts and take out loans with the stolen information.[4] The FTC's February 2005 report "rank[s] identity theft as the number one consumer complaint for the fifth straight year."[5]

Nevada is certainly not immune from the nation's identity theft crisis. The FTC lists Nevada as second in the nation for its per capita identity theft report rate.[6] In 2004 alone, there were nearly 3000 identity theft-related complaints filed in the state.[7] Further, Las Vegas is ranked third of all major U.S. metropolitan areas for per capita identity theft-related complaints.[8]

---

* Amy S. Scarborough is a Juris Doctorate candidate (degree expected May, 2007) at the William S. Boyd School of Law, University of Nevada, Las Vegas.

[1] William H. Minor, *Identity Cards and Databases in Health Care: The Need for Federal Privacy Protections*, 28 COLUM. J.L. & SOC. PROBS. 253, 265 (1995).

[2] *Id.* at 266.

[3] Kate Nash, *Help on Way for ID Theft Victims*, ALBUQUERQUE J., Feb. 5, 2005, at A1.

[4] Tom Zeller, Jr., *Identity Crises: For Victims, Repairing ID Theft Can Be Grueling*, N.Y. TIMES, Oct. 1, 2005, at C1; *see also* Ashley Harris, *Singleton Out to Protect Data from Identity Thieves*, RENO GAZETTE-J., Aug. 16, 2005, at 1D (reporting that according to the Identity Theft Resource Center in San Diego, "[a]s of Aug. 2, more than 55.7 million people could have been affected by 87 reported fraud incidents . . . ."); *see also* Identity Theft Resource Center Home Page, http://www.idtheftcenter.org (last visited Apr. 13, 2007).

[5] *Sen. Bowen's Bill to Protect Personal Information in State Agency Databases Signed into Law*, U.S. ST. NEWS, Sept. 22, 2005 [hereinafter *Sen. Bowen's Bill*] ("Nationwide, identity theft complaints jumped 14.6% between 2003 and 2004.").

[6] *Attorney General Sandoval Unveils Identity Theft Passport Program at Senior Fest*, U.S. ST. NEWS, Sept. 13, 2005 [hereinafter *Attorney General Sandoval*].

[7] *Id.*

[8] *Sen. Bowen's Bill*, *supra* note 5 (The top ten metropolitan areas on the list include "1) Phoenix-Mesa-Scottsdale, AZ; 2) Riverside-San Bernardino-Ontario, CA; 3) Las Vegas-Paradise, NV; 4) Dallas-Fort Worth-Arlington, TX; 5) Houston-Baytown-Sugar Land, TX; 6) Los Angeles-Long Beach-Santa Ana, CA; 7) Miami-Fort Lauderdale-Miami Beach, FL; 8)

Most people admit that they are concerned about SSN abuse.[9] Most are afraid that a thief will use their SSN to access their credit cards or other personal information.[10] People's fears of identity theft "may also come about from [the knowledge] of incidents in which [an individual's] privacy was blatantly invaded."[11] One of the goals of this Note is to demand increased efforts to reduce the risks of identity theft in Nevada by sharing horror stories and presenting the insufficiencies of current legislation and judicial decisions.

Despite an overwhelming fear of identity theft, "there is an alarming lack of legal response to privacy concerns."[12] The pressing need for a legal remedy is undeniable given the statistics of past events and risks of future occurrences, especially given the excessive use of the SSN as an identifier. Indeed, the use of SSNs for identification "is fraught with the potential for abuse [because] . . . the Social Security number is the key to a government file containing a vast amount of personal information."[13] Courts generally permit the government to collect, use, and disseminate SSNs as the government deems necessary, without imposing many limits on the activity.[14]

This Note will argue that Nevadans are in dire need of state legislation enacting a Nevada Privacy Act. Nevada residents are without a remedy to recover from or enforce the Social Security Number provisions of Section 7 of the Privacy Act of 1974 ("Act") when violated by state or local governments or private actors. The Ninth Circuit held in *Dittman v. California*[15] – and strongly re-affirmed its position in *Durante v. Nevada*[16] – that the civil enforcement/remedy provision of the Act only applies to federal agencies. And, because it is in a separate section, it does not apply to Section 7 – the only section of the Act expressly including state and local government agencies as well as federal.[17] It also held that although Section 7 of the Act met the three-prong test for a private right of action under 42 U.S.C. § 1983, the presumption that the right was enforceable under § 1983 was rebutted by the fact that Congress purposely included an enforcement and remedy provision to foreclose any § 1983 reme-

---

San Antonio, TX; 9) San Francisco-Oakland-Fremont, CA; 10) San Diego-Carlsbad-San Marcos, CA . . . .").

[9] Minor, *supra* note 1, at 268; *see also* Flavio L. Komuves, *We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers*, 16 J. MARSHALL J. COMPUTER & INFO. L. 529, 532-33 (1998) (noting that "more than eighty percent of Americans are . . . 'concerned' about privacy issues").

[10] Minor, *supra* note 1, at 268.

[11] Komuves, *supra* note 9, at 533.

[12] *Id.* "An analysis of current law reveals that while courts recognize that SSN dissemination may constitute an invasion of privacy, these same courts will rarely authorize a remedy for such invasions." *Id.* at 572.

[13] Alexander C. Papandreou, Comment, 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, 95 (1993) ("Undoubtedly, free and unregulated access to the highly confidential contents of this government file could substantially threaten the statutory and constitutional guarantees and safeguards of individual privacy.").

[14] Komuves, *supra* note 9, at 572.

[15] Dittman v. California, 191 F.3d 1020 (9th Cir. 1999).

[16] Durante v. Nevada, 22 F.App'x 857 (9th Cir. 2001).

[17] *Dittman*, 191 F.3d at 1027, 1029.

dies against state or local government actors.[18] The Ninth Circuit admitted that this, therefore, "*leaves individuals . . . without a means of enforcing § 7(a)(1) [of the Act] against state and local officials.*"[19]

Section II of this Note will outline the history and purpose of Social Security Numbers, the recognition of the right to privacy, and the historical development of the federal Privacy Act of 1974. Section II will also illustrate how the federal Privacy Act and its application are in a state of disarray, with a circuit split over whether Section 7 is codified, whether the Act applies to state and local government agencies, whether the remedy provision in Section 3 applies to state and local government agencies, whether a § 1983 private right of action can be enforced against state and local government agency violators of the Act, and whether states are immune under the Eleventh Amendment of the United States Constitution from prosecution for their violations of the Act. In response, some states – particularly our geographic neighbors and fellow Ninth Circuit members, Arizona and California – have recognized the shortfalls of the federal Privacy Act and have circumvented the problem by enacting their own state Privacy Acts.

Section III of this Note will discuss that, given the prevalence of identity theft in Nevada and the severity of the consequences, Nevada needs to follow in the footsteps of Arizona and California and enact its own Privacy Act. The few protective measures against identity theft that already exist will be discussed along with the reasons why they are not sufficient. A state Privacy Act will not stop identity theft altogether, but it would reduce its prevalence and make it more difficult for potential thieves to gain access to personal information. Such an Act would force those who collect information to take measures to protect and secure it, only disseminate it when absolutely necessary, and face penalties stiff enough to serve as an incentive to comply. Indeed, the Privacy Acts of Arizona and California should serve as guidance for how Nevada should address the problem legislatively.

II. Historical Background and Development

A. *History of the Social Security Number*

In response to the Great Depression, President Franklin D. Roosevelt's administration unveiled the Social Security Act of 1935 as a retirement plan for Americans.[20] Despite the fact that American colonists rejected the English and European concept of an internal passport because "[i]t represented the type of uninvited intrusion by government . . . that the Bill of Rights was intended to curtail,"[21] the Social Security Act, while not expressly sanctioning SSN creation, did permit the implementation of "'reasonable devices or methods neces-

---

[18] *Id.* at 1029.

[19] *Id.* (emphasis added).

[20] Minor, *supra* note 1, at 261.

[21] *Id.* at 259.

sary or helpful' to collect taxes and to identify taxpayers."[22] Indeed, the IRS commenced the use of the SSN as an identifier of taxpayers in 1962.[23]

The federal government has increased the dependency upon the SSN as an identifier by expanding its use to various identification purposes.[24] There are several exceptions permitting the collection and use of SSNs as identification for government purposes beyond tax and employment purposes,[25] including law enforcement,[26] bankruptcy and tax courts,[27] driver records,[28] child support records and family law,[29] and student loans.[30] As the SSN has become "a quasi-universal personal identification number,"[31] there is growing apprehension about its use "for purposes other than that for which it was created."[32] The express stipulation on the front of a Social Security card that "it is 'not to be used for identification purposes'" has certainly not stopped the SSN from being used as an identifier.[33]

The overuse, excessive dissemination, and use of SSNs as personal identification numbers is the root cause of identity theft. Identity theft is defined as "the use of one person's SSN by another."[34] Of course, only the person to whom each unique SSN is issued is supposed to use it,[35] but the broad use of the SSN makes it more accessible and thus more vulnerable to theft. In recognition of the overuse of the SSN as a personal identifier, a Social Security

---

[22] *Id.* at 261-62; *see also* Papandreou, *supra* note 13, at 79 n.2 (citing 20 C.F.R. § 422.103(b) (1992)) ("A Social Security number is issued after the Social Security Administration receives and processes a completed application (Form SS-5)."). The Papandreou article also references the SOCIAL SECURITY ADMINISTRATION, PROGRAM OPERATIONS MANUAL SYSTEM § RM 00202.001(B) (2005), to explain that "Application Form SS-5 is the basic document used to establish the Social Security number and set up an individual's record."

[23] Minor, *supra* note 1, at 262-63; *see also* Komuves, *supra* note 9, at 540 n.51 ("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.").

[24] Papandreou, *supra* note 13, at 81.

[25] Komuves, *supra* note 9, at 540 ("[A] SSN is the primary identifying number for individuals who file returns."); 26 U.S.C. § 6109(d) (2006).

[26] Komuves, *supra* note 9, at 541 ("The largest criminal justice database in the country, the National Crime Information Center ("NCIC") maintains lists of, among other individuals, convicted criminals and fugitives.").

[27] *Id.* at 543.

[28] *Id.* at 545-46 ("The use of SSNs . . . for identifying and tracking drivers is common in several states and is specifically authorized by federal statute," 42 U.S.C. § 405(c)(2)(C)(i) (2000), although "[w]idespread distribution of the SSN from driver records has been phased out with the 1994 adoption by Congress of [18 U.S.C. § 2725 (2000)] barring disclosure of 'personal information' in drivers' licenses.").

[29] *Id.* ("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."); 42 U.S.C. § 653(h)(1) (2000).

[30] Komuves, *supra* note 9, at 548 ("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."); 20 U.S.C. § 1091(a)(4)(B) (2000).

[31] Komuves, *supra* note 9, at 531-32.

[32] Minor, *supra* note 1, at 263.

[33] Papandreou, *supra* note 13, at 79.

[34] Komuves, *supra* note 9, at 534.

[35] Papandreou, *supra* note 13, at 79 n.1.

Administration task force was created in 1970 to investigate the problem, and it determined that the SSN was overused "to the point where the adult American citizen is beginning to need a number to function effectively . . . ."[36] The findings of the task force provoked Congress to limit governmental use of the SSN when drafting the Privacy Act of 1974.[37] Congressional committees considering the Act concluded that the extensive use of SSNs as universal identifiers was "a key area of concern" and "one of the most serious manifestations of privacy concerns in the nation."[38]

The use of SSNs as personal identifiers has often encompassed both student identification cards and health insurance membership cards, thus increasing the risk of the SSN being acquired by an identity thief. In response to growing problems, many colleges have stopped using SSNs to identify students.[39] The medical and insurance industries have also undertaken protective measures. The American Medical Association discourages the use of SSNs to identify the insureds, patients, or physicians except where required by law.[40] Highmark Blue Cross Blue Shield said it was reissuing new ID cards with "no correlation to Social Security numbers."[41] However, despite these efforts, "[t]he use of the SSN in the context of medical records is likely to continue."[42] Indeed, a doctor from Boston's Beth Israel Hospital has acknowledged, "there is no such thing as a totally secure medical record."[43]

B. Recognition of the Right to Privacy

The recognition of the need for "the protection of the person, and for securing to the individual . . . the right 'to be let alone'" dates back over one hundred years.[44] Indeed, privacy is "central to the values and principles of the United States."[45] In the 1965 case of *Griswold v. Connecticut*, the Supreme Court recognized the right to privacy as a fundamental right implied in the Bill

---

[36] Minor, *supra* note 1, at 263-64.

[37] *Id.* at 264.

[38] Komuves, *supra* note 9, at 532 (quoting S. REP. No. 93-1183 (1974), *as reprinted in* 1974 U.S.C.C.A.N. 6916, 6943.

[39] Cindi Brownfield, *No Safety in These ID Numbers*, DAYTONA NEWS-J., May 31, 2004, at 01C.

[40] *See generally* American Academy of Insurance Medicine, http://www.aaimedicine.org (last visited Apr. 13, 2007).

[41] Jonathan D. Silver, *Woman Victim of ID Theft After Insurance Card Stolen; Arrest Made For $14,000 in Fraudulent Medical Services*, PITTSBURGH POST-GAZETTE, Apr. 25, 2004, at C1.

[42] Komuves, *supra* note 9, at 539; *see also* Minor, *supra* note 1, at 254 ("Even absent government intervention by way of reform legislation, the health care industry is in the midst of an era of unprecedented computerization of medical records and data [because u]ntil recent years, most doctors, hospitals, and medical centers maintained patient data only in their local offices [while n]ow, data can be widely shared through computerized linkage of such facilities.").

[43] Minor, *supra* note 1, at 281.

[44] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

[45] Julianne M. Sullivan, *Will The Privacy Act of 1974 Still Hold Up in 2004?*, 39 CAL. W. L. REV. 395, 395 (2003).

of Rights.[46] However, at least one federal court has found that the "mandatory disclosure of one's social security number does not so threaten the sanctity of individual privacy as to require constitutional protection."[47]

An individual "is entitled to be protected in the exclusive use and enjoyment of that which is exclusively his" and the right to decide "whether that which is his shall be given to the public."[48] However, the growth of society in both size and complexity has led to an increase in the quantity of records maintained on individuals.[49] Technology has contributed to the diminishment of privacy rights by facilitating the storage and dissemination of personal information electronically.[50] The increase in recordkeeping increases the risk that personal information and SSNs will land in the wrong hands; therefore, "[a]s technology improves, more privacy protections should be instituted."[51]

C. *The Privacy Act of 1974*

Congress enacted the Privacy Act of 1974 on December 31, 1974; it became effective on September 27, 1975.[52] The Act protects the privacy of personal information and records collected, maintained, and used by federal agencies.[53] It requires "a balancing of interests between the government agencies storing the records and the individuals about whom the records are kept."[54]

Indeed, the Act deals primarily with issues of public disclosure and intrusion.[55] It endorses respect for individuals' privacy by prohibiting unnecessary and excessive dissemination of personal information between government agencies or from an agency to entities outside the government.[56] The Act further enables individuals to determine what personal information agencies have collected and allows them to verify its accuracy.[57] In sum, the Act provides citizens with greater "control over the gathering, dissemination, and accuracy of information . . . contained in government files . . . ."[58]

However, because the Act was hastily passed at the end of the session, its legislative history is rarely of much assistance in ascertaining what the legislature intended.[59] There were discrepancies between the bill passed by the House and that passed by the Senate.[60] No official committee report was ever compiled, and there is a further lack of correlation between early congressional

---

[46] *Id.* at 395 (citing Griswold v. Connecticut, 381 U.S. 479 (1965)).
[47] Komuves, *supra* note 9, at 562 (quoting Doyle v. Wilson, 529 F. Supp. 1343, 1348 (D. Del. 1982)).
[48] Warren & Brandeis, *supra* note 44, at 199, 205.
[49] Sullivan, *supra* note 45, at 396.
[50] *See* Komuves, *supra* note 9, at 531.
[51] *Id.* at 573.
[52] Sullivan, *supra* note 45, at 397.
[53] *See* 5 U.S.C. § 552a (2000).
[54] Sullivan, *supra* note 45, at 410.
[55] *Id.* at 395 n.1.
[56] Jay M. Zitter, Annotation, *What Is Agency Subject to Privacy Act Provisions (5 U.S.C.A. § 552a)*, 150 A.L.R. FED. 521 (1998).
[57] Sullivan, *supra* note 45, at 397.
[58] Zitter, *supra* note 56, at 521.
[59] Sullivan, *supra* note 45, at 398.
[60] *Id.*

reports and the enacted statute.[61] The Senate Committee reviewing the Act did consider the usage of the SSN "one of the most serious privacy concerns in the United States. However, [the committee] received conflicting evidence about the effects of § 7 of the Privacy Act . . . ."[62] This raises particularly problematic issues in attempting to determine the section's scope with regard to applicable restrictions on the use and disclosure of SSNs.

1. Restrictions on Use of Social Security Numbers – Section 7 of the Privacy Act

Of particular importance to identity theft prevention, Section 7 of the Privacy Act is "[t]he main source of restrictions on SSN usage."[63] Section 7 provides that "[a]ny federal, state, or local government agency which requests the disclosure of a Social Security number must inform the individual whether the disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it."[64] Section 7 further provides that "[i]t shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number."[65] On its face, Section 7 appears to prohibit several governmental uses of the SSN; however, given the number of exceptions to the rule granted by Congress for SSN collection and use, "the exceptions clearly swallow the general rule."[66]

One of the initial issues involving Section 7 is whether it is codified within the Privacy Act, because it "appears in the annotated code as a historical note to 5 U.S.C.A. § 552a."[67] Some courts, including the Ninth Circuit, have therefore

---

[61] *Id.*

[62] Papandreou, *supra* note 13, at 80 n.4.

[63] Komuves, *supra* note 9, at 549.

[64] 37A AM. JUR. 2D *Freedom of Information Acts* § 9 (2005) (citing 5 U.S.C.A. § 552a note (West 2002) (Disclosure of Social Security Number)). Section 7

> 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 Congress to require submission of a SSN. If neither of those two conditions is satisfied, then the entity may still request that an individual submit his SSN voluntarily. 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.

Komuves, *supra* note 9, at 549-50.

[65] 5 U.S.C.A. § 552a note (Disclosure of Social Security Number).

[66] Komuves, *supra* note 9, at 550; *see also* 37A AM. JUR. 2D *Freedom of Information Acts* § 9 (2005) (noting that the Section 7 restrictions do not apply to SSN disclosures required by federal statutes) (citing 5 U.S.C.A. § 552a note (Disclosure of Social Security Number)).

[67] Papandreou, *supra* note 13, at 83 n.12.

found or noted that Section 7 is uncodified.[68] Few courts have found that Section 7 *is* codified within the Act.[69]

Section 7 is also the only portion of the Act expressly referring to federal *and* state and local government agencies; the rest of the Act expressly applies to federal agencies alone.[70] This express inclusion of state and local government agencies within Section 7 raises questions as to whether it means or implies that other provisions of the Act – specifically, enforcement provisions found in other sections – are also meant to apply to state and local government agencies.

The Privacy Act defines "agency" as it is defined in section 552(e) of Title 5, which corresponds to the Freedom of Information Act ("FOIA").[71] However, the definition of an agency is found within § 552(f) of the FOIA, and *not* § 552(e) as the Privacy Act suggests.[72] This error apparently "resulted when the reference was not updated when subsections [of the FOIA] were relettered;"[73] however, it demonstrates the Act's current state of disarray.

Section 552(f) of the FOIA states that the term "agency" "includes any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency . . . ."[74] Clearly this statutory definition does not expressly consider or refer to a state or local government agency as an "agency" within the Privacy Act.[75] Accordingly, several courts have found that the definition applies only to federal agencies, and not state or local government agencies or private actors.[76] Nor does a state agency become a federal agency because it receives federal funding or is subject to federal statutes.[77]

---

[68] *See, e.g.*, Dittman v. California, 191 F.3d 1020, 1024 (9th Cir. 1999) (mentioning that § 7 was uncodified); Krebs v. Rutgers, 797 F. Supp. 1246, 1253 (D.N.J. 1992) (noting that § 7 was "never codified" and it appears only "as an historical note to 5 U.S.C. § 552a"); *see also* 37A AM. JUR. 2D *Freedom of Information Acts* § 9 (2005); Papandreou, *supra* note 13, at 83 n.12 ("Section 7 of the Privacy Act of 1974 was never incorporated into the United States Code.").

[69] Schmitt v. City of Detroit, 395 F.3d 327, 330 (6th Cir. 2005) (noting that § 7 of the Act was codified, despite its being a note to 5 U.S.C. § 552a).

[70] *See* 5 U.S.C. § 552a (2000).

[71] *Id.* § 552a(a)(1). The Freedom of Information Act is codified at 5 U.S.C. § 552 (2000).

[72] Papandreou, *supra* note 13, at 83 n.12; *see also* 5 U.S.C. § 552(e)-(f)(1).

[73] Papandreou, *supra* note 13, at 83 n.12.

[74] 5 U.S.C. § 552(f)(1).

[75] *See* Zitter, *supra* note 56.

[76] *Id.* at 530; *see* Schmitt v. City of Detroit, 395 F.3d 327, 331 (6th Cir. 2005) (noting that "notwithstanding the codification of § 7(b) – the Privacy Act applies exclusively to federal agencies"); Unt v. Aerospace Corp., 765 F.2d 1440, 1447 (9th Cir. 1985) (recognizing rule that the Privacy Act applies solely to federal agencies); Polchowski v. Gorris, 714 F.2d 749, 752 (7th Cir. 1983) (noting that the Privacy Act applies only to federal agencies); St. Michael's Convalescent Hosp. v. California, 643 F.2d 1369, 1373 (9th Cir. 1981) (holding that the definition of agency "does not encompass state agencies or bodies"); Shields v. Shetler, 682 F. Supp. 1172, 1176 (D. Colo. 1988); Ryans v. New Jersey Comm'n for the Blind and Visually Impaired, 542 F. Supp. 841, 852 (D.N.J. 1982) (noting that "the federal Privacy Act governs federal agencies only").

[77] Krebs v. Rutgers, 797 F. Supp. 1246, 1256 (D.N.J. 1992). Although Rutgers University was "a state-created entity, serving a state purpose, and receiving a large degree of financing

Further, at least one court held that individual directors or employees of agencies cannot be sued for violations of the Privacy Act.[78]

Nevertheless, at least one federal court suggested that the legislative history and statutory materials support the possibility that state agencies might be covered within the Act's definition of "agency."[79] However, in *Schmitt v. City of Detroit*, the Sixth Circuit relied upon legislative history and held to the contrary: a city was not an "agency" under the Privacy Act's definition[80] because a city is not an "agenc[y] that fell under control of federal government."[81] That court concluded that "the Privacy Act applies exclusively to federal agencies."[82]

While beyond the scope of this Note, another issue concerns whether states are immune from prosecution for violations of the Privacy Act under the Eleventh Amendment of the U.S. Constitution.[83] Under *Seminole Tribe of Florida v. Florida*,[84] Eleventh Amendment immunity to state agencies "may be abrogated by Congressional action, provided that . . . Congress made it unmistakably clear in the statute that they were abrogating immunity."[85] Because Congress did not mention any abrogation of immunity within the Privacy Act, it is likely that "an argument that a Section 7 claim against a state agency is barred by the Eleventh Amendment will . . . be successful."[86]

2. *Enforceability and Remedies Under the Privacy Act*

It seems of little value to enact legislation without providing a remedy for its enforcement. Yet Section 7 of the Privacy Act – the only section both specifically addressing SSN disclosure and mentioning state and local government agencies – does not expressly include a remedies provision.

In *Polchowski v. Gorris*,[87] a decision upon which the Ninth Circuit relied in *Dittman v. California*,[88] the Seventh Circuit acknowledged that Congress provided remedies for violations within every section of the Act except for

---

[from the state]," it remained independent and, therefore, was deemed an independent institution and not subject to the provisions of the Privacy Act. Papandreou, *supra* note 13, at 86-87.

[78] Parks v. U.S. Internal Revenue Serv., 618 F.2d 677, 684 (10th Cir. 1980).

[79] *Krebs*, 797 F. Supp. at 1253; *see also* Zitter, *supra* note 56, at 521.

[80] *Schmitt*, 395 F.3d at 330-31; *No Suit Against City for Disclosure of Social Security Number*, 2 No. 5 ANDREWS PRIVACY LITIG. REP. 8 (January 25, 2005) ("Although Senate Report 93-1183 indicates that Congress considered applying the Privacy Act beyond federal agencies, it held off doing so pending further study . . . .").

[81] Zitter, *supra* note 56, at 46 (Supp. 2006).

[82] *Schmitt*, 395 F.3d at 331.

[83] *See, e.g.*, B.J.R.L. v. Utah, 655 F. Supp. 692, 695 (D. Utah 1987) (holding that certain state agency and state government officials cannot be prosecuted for violations of a federal statute because of immunity pursuant to the Eleventh Amendment); Komuves, *supra* note 9, at 553-54 ("Under the Eleventh Amendment doctrine in light of *Seminole 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.").

[84] Seminole Tribe of Florida v. Florida, 517 U.S. 44 (1996).

[85] Komuves, *supra* note 9, at 554 n.138.

[86] *Id.*

[87] Polchowski v. Gorris, 714 F.2d 749 (7th Cir. 1983).

[88] Dittman v. California, 191 F.3d 1020, 1028-29 (9th Cir. 1999).

Section 7; however, those sections expressly apply only to federal agencies.[89] The Seventh Circuit further recognized that the original bill did contain a remedy for violations by state actors, but it "[was] deleted because of the uncertain effect . . . and because Congress felt that it lacked the necessary information for devising a remedial scheme in this context."[90] Hence, there is no enforcement or remedy provision within any section of the Act that expressly applies to state or local agencies, although Section 7's restrictions *do* expressly refer to state and local government agencies.

Because there is no enforcement scheme within Section 7 of the Act, it warrants considering whether a plaintiff could bring a private right of action under 42 U.S.C. § 1983 for a Section 7 violation.[91] "Section 1983 provides a private right of action whenever an individual has been deprived of any constitutional or statutory federal right under color of state law."[92] But, a § 1983 claim, although presumptively available, cannot be made for every federal statutory violation.[93]

To bring a § 1983 claim, a plaintiff must meet a three-prong test to demonstrate a violation of a federal right.[94] However, even if all prongs are met, it merely creates a rebuttable presumption.[95] No § 1983 claim can stand if it is determined that "Congress has specifically foreclosed a remedy under § 1983" either through express foreclosure within the statute itself or by impliedly foreclosing a § 1983 "remedy by creating a comprehensive enforcement scheme that is incompatible with individual enforcement under § 1983."[96]

The Ninth Circuit, in *Dittman v. California*, held that the Privacy Act met the three-prong test, but it concluded that Congress specifically foreclosed a private cause of action against state and local governments under Section 7 when enacting the Privacy Act because the Act's civil remedy provision, 5

---

[89] Zitter, *supra* note 56.

[90] *Id.* at 533.

[91] 42 U.S.C. § 1983 (2000) provides that:

> Every person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress, except that in any action brought against a judicial officer for an act or omission taken in such officer's judicial capacity, injunctive relief shall not be granted unless a declaratory decree was violated or declaratory relief was unavailable.

[92] Schwier v. Cox, 340 F.3d 1284, 1290 (11th Cir. 2003).

[93] 15 AM. JUR. 2D *Civil Rights* § 66 (2000).

[94] *Id.* The three-prong test requires that

> (1) Congress must intend that the provision in question benefit the plaintiff, (2) the right assertedly protected by the statute must not be so vague and amorphous that its enforcement would strain judicial competence, and (3) the statute must unambiguously impose a binding obligation on the states, in that the provision giving rise to the asserted right must be couched in mandatory rather than precatory terms.

Id. (citing Blessing v. Freestone, 520 U.S. 329 (1997)).

[95] *Id.* at n.69 ("Congress has implicitly foreclosed a 42 U.S.C.A. § 1983 action to enforce a right, privilege or immunity created by a federal statute if the remedial scheme inherent in the federal statute itself is so comprehensive as to leave no room for additional private remedies under 42 U.S.C.A. § 1983.").

[96] *Id.* § 66.

U.S.C. § 552a(g), was exclusively limited to federal agencies.[97] Congress purposely included an enforcement and remedy provision to foreclose any § 1983 remedies against state or local government actors.[98] It admitted that this "leaves individuals . . . without a means of enforcing § 7(a)(1) [of the Act] against state and local officials" despite that Section 7's prohibitions applied to them.[99]

The Ninth Circuit held steadfast to its holding in *Dittman* in its brief decision in *Durante v. Nevada*, where a student at the Community College of Southern Nevada brought suit against the school and the state of Nevada challenging the use of SSNs for identification of students, particularly on student ID cards.[100] The district court previously denied Natalie Durante's request for an injunction because the Privacy Act remedies provision, found in Section 3 of the Act, applies only to violations by federal agencies. She lost her case at trial and, on appeal, the Ninth Circuit refused to overrule *Dittman v. California*, concluding that there is "no private right of action against any of the defendants directly under the Privacy Act or through § 1983 . . . ."[101]

Although of little help to Nevadans, the Eleventh Circuit strongly disagrees with the Ninth Circuit and has found that an individual *could* enforce his rights under Section 7 of the Privacy Act with a private right of action under 42 U.S.C. § 1983.[102] In *Schwier v. Cox,* the court criticized the Ninth Circuit's holding in *Dittman* because *Dittman* involved Section 7 of the Act, yet the Ninth Circuit relied on two decisions that solely involved Section 3 of the Act.[103] The Eleventh Circuit noted that Section 7 of the Act was valid and still held great statutory weight, despite the fact that it was a note to the Act.[104] The court further disagreed with the Ninth Circuit, finding that Congress did not foreclose a § 1983 private right of action within the Privacy Act because Section 7, which mentions state and local government agencies, is unlike Section 3 of the Act because it does not have any enforcement remedial scheme.[105]

The Eleventh Circuit concluded that Section 7 may be enforced by a § 1983 claim because Congress did not explicitly foreclose one and a § 1983 claim is not incompatible with the statute because there is no remedial scheme in Section 7 with which there could be incompatibility.[106] Unfortunately, this decision does nothing to aid Nevadans. Nevadans are bound by the Ninth Cir-

---

[97] Dittman v. California, 191 F.3d 1020, 1029 (9th Cir. 1999).

[98] *Id.*

[99] *Id.*

[100] Durante v. Nevada, 22 F.App'x 857, 857 (9th Cir. 2001).

[101] *Id.* (noting that "because *Dittman* makes it clear that Durante has no private right of action against any of the defendants directly under the Privacy Act or through § 1983, we must deny the appeal." (citation omitted)).

[102] Schwier v. Cox, 340 F.3d 1292, 1292 (11th Cir. 2003).

[103] *Id.* at 1289 (referencing Unt v. Aerospace Corp., 765 F.2d 1440 (9th Cir. 1999) and Polchowski v. Gorris, 714 F.2d 749 (7th Cir. 1983)). The court distinguished those Section 3 cases because they held that the Privacy Act only applied to federal agencies, which the Eleventh Circuit noted was because Section 3 does, in fact, only expressly apply to federal agencies. *Id.*

[104] *Id.* at 1288.

[105] *Id.* at 1289.

[106] *Id.* at 1292.

cuit's decision in *Dittman*, which precluded a § 1983 claim for violations of Section 7 of the Privacy Act.

III. ANALYSIS

A. *Nevada's Need for a Privacy Act*

1. Inadequacy of Current Law

The federal Privacy Act of 1974 is not of much use in restricting the dissemination and overuse of SSNs, particularly for Nevadans. The intent was for Section 7 of the Act to prevent excessive disclosure of SSNs; however, there are several exceptions requiring disclosure nonetheless. There is confusion over whether Section 7 – the only section to address specifically both SSN privacy and mention state and local government agencies – is even codified. There is disagreement over whether the Act's definition of "agency" applies to state and local government agencies at all, despite that they are expressly mentioned in Section 7. Further, it is undisputed that the Act does not apply to private actors or agencies. Finally, while some jurisdictions permit a § 1983 private right of action in light of the lack of an enforcement or remedies provision in Section 7, Nevada is controlled by the Ninth Circuit, which precludes such a claim. Thus, it seems that there is no way for Nevadans to enforce the SSN restrictions of the Act whatsoever.

In light of the issues with the Privacy Act, a feasible goal should be to try to reduce the risk of identity theft by taking a preemptive strike and making personal information, specifically Social Security numbers, less accessible. The goal is to try to stop identity theft *before* it happens and to enjoin certain activities that increase the risk and make it easier for thefts to occur. Nevadans are in need of such protection.

There are already criminal remedies in place when someone is caught stealing an identity.[107] Almost every state has enacted state criminal laws related to prosecuting those few identity thieves who are caught.[108] The illegal use of SSNs is punished with federal criminal penalties.[109] Fraudulent actions to obtain a SSN or the misrepresentation or alteration of a SSN are felonies punishable by up to five years in prison.[110]

---

[107] In 1998, the federal government enacted the Identity Theft and Assumption Deterrence Act of 1998, which made identity theft a federal crime. *See* Pub. L. No. 105-318, 112 Stat. 3007 (1998).

[108] *See* Identity Theft Resource Center, *supra* note 4.

[109] Komuves, *supra* note 9, at 556 (citing 42 U.S.C. 408(a)(7)).

[110] *Id.* at 556 n.147.

> Specifically, a criminal penalty may be imposed when any individual, with the purpose of . . . 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 . . . (B) with intent to deceive, falsely represents a number to be the social security account number assigned . . . to him or to another person, when in fact such number is not the social security account number assigned . . . to him or to such other person; or (C) knowingly alters a social security card . . . , 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.

42 U.S.C. 408(a)(7)(A)-(C).

However, it is rare that perpetrators are ever caught and prosecuted.[111] Studies show that identity thieves face a mere "1 in 700 chance of getting caught."[112] When one couple victimized by identity theft hired a private investigator on their own, the investigator was able to find the thief and his address and turned the information over to police.[113] However, when police went to the district attorney with the information, he said "that it would be necessary to obtain a confession from [the thief] or catch him in the possession of fraudulently obtained merchandise or credit cards."[114] This shows just how difficult it is to arrest someone for identity theft and why it needs to be prevented rather than rarely punished.

While statutes criminalizing identity theft and imposing penalties on those few that are caught may serve as a minor deterrent, there is little besides the Privacy Act to prevent the thefts from occurring in the first place. This is why Nevada needs to take measures to enforce strictly the prevention of excessive and unnecessary disclosure and dissemination of personal information such as SSNs by enacting its own Privacy Act.

There is no doubt that the prevalence of identity theft and its serious consequences have been recognized. Some scholars feel that an amendment to the Privacy Act is both in the best interests of the public and required in order to update it, particularly because "the problem will only grow with time."[115] There are, indeed, a number of bills floating through various Senate and House committees involving SSNs and identity theft introduced in response to the problems with stolen personal information.[116] However, the legislature has yet to pass either an amendment to the existing federal Privacy Act or the enactment of a new law that protect SSNs or prevents identity theft.[117]

In particular, the Social Security Protection Act has been seemingly bounced from committee to committee since at least 2000 with a new version renewed and re-introduced every year. For example, in a prior session of Congress, the Social Security Number Privacy and Identity Theft Prevention Act of 2005, H.R. 1745 was pending for passage, and, had it been enacted into law, it would have reduced the use of consumers' Social Security numbers for identification purposes.[118] Both the House and Senate introduced numerous bills similarly addressing identity theft and the misuse and dissemination of Social

---

[111] Zeller, *supra* note 4.

[112] *Id.*

[113] Jane Ann Morrison, *Identity Thieves Thrive on Security Cracks*, LAS VEGAS REV.-J., Sept. 8, 2005, at 1B.

[114] *Id.*

[115] Sullivan, *supra* note 45, at 412.

[116] Robert Dodge, *Congress Looks at Curbing Identity Theft*, DALLAS MORNING NEWS, Apr. 4, 2005.

[117] *See generally* Library of Congress, http://thomas.loc.gov. (last visited Feb. 19, 2006) (Indeed, any bills introduced addressing identity theft or the dissemination of Social Security numbers seem to die in committees and are never passed.).

[118] *Id.*

Security Numbers again in 2007, but it is not clear when any of these bills may get out of committee, much less enacted into law.[119]

Recent Nevada legislation suggests that the legislature has an appreciation for the consequences of identity theft and may be open to a Nevada Privacy Act. The Nevada legislature recently amended Chapter 205 of Nevada Revised Statutes regarding criminal penalties for the misuse of personal information:

> An ACT relating to personal identifying information; prohibiting the establishment or possession of a financial forgery laboratory; enhancing the penalties for crimes involving personal identifying information that are committed against older persons and vulnerable persons; requiring the issuer of a credit card to provide a notice including certain information concerning its policies regarding identity theft and the rights of cardholders when issuing a credit card to a cardholder; requiring data collectors to provide notification concerning any breach of security involving system data; making various other changes concerning personal identifying information; providing penalties; and providing other matters properly relating thereto.[120]

Nevada has also taken steps to assist victims of identity theft by adopting a new program called "The Identity Theft PASSPORT program," which serves to provide identity theft victims with a state-issued ID card that indicates the holder was a victim.[121] The PASSPORT card includes the victim's photo, current address, and thumbprint and can be used to notify creditors and police that the holder was a victim of identity theft.[122] The ID card "can help prevent evictions, bill collections and arrests while the victim cleans up their record."[123] The program commenced January 1, 2006.[124] However, although useful to identity theft *victims*, the PASSPORT program does nothing to prevent the thefts from happening in the first place.

The Ninth Circuit's ruling in *Dittman v. California* is troubling because its decision admittedly leaves Nevadans "without a means of enforcing § 7(a)(1) [of the Act] against state and local officials."[125] If there is no remedy under the Privacy Act and no § 1983 right of action – therefore leaving Nevadans without a way to enforce the state or local governments from putting them at risk of identity theft – then a state Privacy Act must be enacted as a partial solution to the problem. Of course because the federal Privacy Act does not apply to private actors, the prohibitions introduced in a state Privacy Act should apply to them as well. A Nevada Privacy Act could provide restrictions on the collection, use, and dissemination of SSNs and provide a remedy for violations – without having to wait for Congress to finally clarify or enact new federal legislation.

---

[119] *Id.* (That many bills are introduced each year demonstrates an understanding and appreciation for the problem; however, several years of bill-tracking reveals that every attempt to address the issue die in committees.)

[120] Act of June 17, 2005, 2005 Nev. Stat. 2496.

[121] *New ID-Theft Program to Be Unveiled on Tuesday*, RENO GAZETTE J., Sept. 8, 2005, at 4 [hereinafter *New ID-Theft Program*].

[122] *Attorney General Sandoval*, *supra* note 6.

[123] *New ID-Theft Program*, *supra* note 121.

[124] *Attorney General Sandoval*, *supra* note 6. *See also* Nevada Attorney General, Identity Theft Passport Program, http://ag.state.nv.us/menu/passport/introduction.htm (last visited Apr. 13, 2007).

[125] Dittman v. California, 191 F.3d at 1020, 1029 (9th Cir. 1999).

2. Serious Effects and Consequences of Identity Theft to Victims

"[I]dentity theft has become endemic"[126] and is "the fastest growing crime in the nation."[127] Over twenty-seven million people nationwide and over 5000 people in Southern Nevada alone are victims of identity theft.[128] Nevada is listed second in the nation by the FTC for its per capita identity theft report rate.[129] Las Vegas is ranked third of all major U.S. metropolitan areas for per capita identity theft-related complaints.[130] Nevadans undeniably need protection of their SSNs because of the prevalence of identity theft within the state and because most become victims after their personal information is taken from documents or databases holding their SSN.[131]

Examining the severity of the consequences of identity theft helps to appreciate the need for legislation preventing identity theft. One identity theft victim[132] returned home from a Christmas with family to find his mailbox full of brochures for attorneys offering their services because they had seen he was recently arrested. He learned that someone created a driver's license with the victim's personal information but with the thief's picture. The thief used the fraudulent license and SSN to steal the victim's identity for a weekend shopping spree, opening store credit cards at Burdines, Circuit City, Office Depot, JCPenney, and Wal-Mart and maxing-out the limits on every card for over $10,000 worth of clothing, computers, cameras, camcorders, and car stereos. The thief proceeded to open a Blockbuster account, rented video games and DVDs and, of course, did not return them.

When attempting to open a Best Buy credit card, the thief was arrested for having a fictitious credit card; however, the thief handed over the false driver's license with the victim's information, leaving the victim to attend court hearings and plead his case of identity theft. Although the credit card charges were waived, the victim still has to explain the incident every time he applies for credit and constantly worries of a future occurrence because his information is still out there.

Victims of identity theft are not treated with much sympathy. When the victim questioned Circuit City for allowing someone to max out a $6000 credit limit in a day, the manager told him to have a good life and hung up on him. Police failed to return his frequent calls, and little was done to investigate the matter. The retail stores were slow in sending affidavits to make fraud claims. JCPenney made the victim go through store surveillance with a manager to assure them that it was not he who opened the accounts. In sum, everyone doubted that he was actually a victim. This victim is convinced that were it not necessary to disclose his personal information so frequently to so many who demand it, this may have been prevented.

---

[126] Dodge, *supra* note 116.

[127] Nash, *supra* note 3.

[128] Omar Sofradzija, *March Break-In: Stolen DMV Materials Found*, LAS VEGAS REV.-J., June 3, 2005, at 1A; *see also* Dodge, *supra* note 116.

[129] *Attorney General Sandoval*, *supra* note 6; *New ID-Theft Program*, *supra* note 121.

[130] *Sen. Bowen's Bill*, *supra* note 5.

[131] Brownfield, *supra* note 39.

[132] The victim, the author's brother, provided an account of his identity theft experience for purposes of this Note.

Identity theft can ruin the financial lives of victims "who risk having bank accounts drained and credit ratings ruined."[133] Consumers who are asked to provide personal information can become identity theft victims to thieves who will exploit their Social Security, driver's license, and credit card numbers.[134] Identity thieves are often employees pilfering clients' information from their employer's files[135] or "dumpster divers" who get information from the victims' trash or from their doctor's offices,[136] insurance companies, credit card companies, or any other business with which the victim has shared personal information.[137] Thieves also frequently obtain SSNs from documents containing the number and stolen from mailboxes.

Identity thieves frequently use the stolen SSNs to apply for credit cards in the victim's name,[138] sometimes by creating fake driver's licenses with the victim's information imprinted on it but including the thief's photograph.[139] Thieves have even been known to file bogus electronic tax returns with stolen information to the IRS claiming huge refunds and then get "refund anticipation loans" from banks or tax preparation services.[140] Methamphetamine rings are known to use the SSNs stolen by addicts in exchange for drugs, to write bad checks or even take out life insurance policies on addicts who they know are likely to die, and then to collect on the policies.[141]

However, the majority of identity theft cases entail opening credit card accounts, subsequent purchasing luxury items, and accumulating fraudulent debts.[142] Such debts have been known to include rental cars that were never returned, delinquent mortgages, jewelry, and cellular phone accounts.[143] For example, in Las Vegas, a Luxor casino employee was caught after stealing the SSNs of two people and using them to obtain a Nevada driver's license, pass-

---

[133] Sofradzija, *supra* note 128.

[134] Dodge, *supra* note 116.

[135] Joseph Menn, *Federal ID Act May Be Flawed*, L.A. TIMES, May 31, 2005, at C1 ("Workers also leak address, Social Security and other information for cash to private detectives, bill collectors and the like, a problem Nevada DMV spokesman Tom Jacobs said probably would increase as information became available from other states' databases.").

[136] *Id.* ("A 2004 survey of the previous year's news accounts . . . found licenses-for-bribes schemes in Nevada [and several other states]. . . ."); *Zeller*, *supra* note 4 (discussing how two thieves had stolen elderly patients' personal information from the eye-care center where they worked).

[137] Komuves, *supra* note 9, at 534 ("In addition, public employees with access to government computers have also been sanctioned after illegally accessing SSNs to perpetrate fraud."); Menn, *supra* note 135 ("More typically, low-level state employees take money to issue [drivers'] licenses improperly."); Morrison, *supra* note 113.

[138] Brownfield, *supra* note 39.

[139] Zeller, *supra* note 4.

[140] *Id.*

[141] *ID Theft Hits Big Time*, PRIVACY J., July 1, 2004, at 6; *see also* John Leland, *Meth Users, Attuned to Detail, Add Another Habit: ID Theft*, N.Y. TIMES, July 11, 2006, at A1 (noting that the majority of identity theft cases involve meth users or dealers and noting the relationship of the states with the highest rates of identity theft, such as Nevada, Arizona, California, Texas, and Colorado, to the levels of illegal immigration and meth use in these states).

[142] Nash, *supra* note 3.

[143] Zeller, *supra* note 4.

port, firearm permits, and numerous credit cards.[144] The thief then mortgaged a house for almost $450,000, financed two luxury cars, and worked under other people's SSN to avoid paying federal income tax.[145]

Indeed, mortgage fraud is a particularly severe issue and should be addressed in a Nevada Privacy Act. An FBI briefing ranked Nevada within the top ten "mortgage fraud hot spots."[146] The particular problem with mortgage fraud is that "loan brokers do not have to comply with the Bank Secrecy Act" and most of the industry does not have to follow any mandatory fraud reporting.[147] Thus, it would be beneficial for a Nevada Privacy Act also to incorporate mandatory fraud reporting to combat mortgage fraud within the state, especially given the increasing number of people moving to Nevada and the growth of the residential real estate market. Given the prevalence of mortgage fraud in Nevada, mortgage brokers should be required to take measures to identify and report any potential fraud before issuing any home loans.

Although Nevada's new PASSPORT program offers some assistance to victims, the consequences of identity theft are so harsh and relentless that the state needs to stop identity theft before it occurs. Victims suffer more than just a damaging credit report.[148] Rectifying the fraudulent debts and charges involves much money, time, headache, and stress.[149] The delinquent credit makes the victim's real creditors lower credit card limits and increase interest rates, thus costing the victim financially for years after the theft.[150] After discovering their identity has been stolen, victims constantly worry that it will happen again because their information is still out there in the hands of thieves.[151] In fact, the average victim spends about 330 hours and $851 in out-of-pocket expenses to clear his name.[152] Additionally, victims are harassed by collectors, face loan rejections and insurance coverage rejections, have their utilities sometimes cut off, and often face criminal investigations as well.[153]

Also posing a risk to Nevada consumers and in need of regulation are those private businesses and government agencies that collect personal information and SSNs. There have been a number of sabotaged databases where data was breached and stolen, including legal research provider LexisNexis where the personal information of 32,000 people was stolen.[154] Bank of America reported that it lost backup computer tapes that included the data on more than one million customers.[155] ChoicePoint, one of the nation's largest

---

144 *Ex-Luxor DJ Sentenced to Three Years*, LAS VEGAS REV.-J., Mar. 23, 2005, at 6B.

145 *Id.*

146 Paul Muolo, *FBI Wants Broker Fraud Cooperation*, NAT'L MORTGAGE NEWS, May 9, 2005, at 1 (States on the list include California, Colorado, Florida, Georgia, Illinois, Michigan, Missouri, South Carolina, Nevada, and Utah.).

147 *Id.*

148 *See* Komuves, *supra* note 9, at 534.

149 Dodge, *supra* note 116.

150 Zeller, *supra* note 4.

151 *Id.*; Morrison, *supra* note 113 (noting that identity theft can happen to the same person more than once).

152 *Sen. Bowen's Bill*, *supra* note 5.

153 Zeller, *supra* note 4.

154 Dodge, *supra* note 116.

155 *Id.*

data-collection companies, disclosed that it discovered that it has sold personal financial data in 145,000 reports to criminals involved in an identity theft scheme.[156] And, more locally, in what was the largest loss of Nevadans' personal information in the Nevada Department of Motor Vehicles' ("DMV") history,[157] someone rammed a truck through a North Las Vegas DMV building and stole a computer and drivers' license-making equipment.[158] Authorities had feared the incident "could have led to massive identity theft" because the personal information of more than 8000 people was on the computer, but when police found it, they determined that the thief never accessed it.[159]

Yet another problem with the Privacy Act is that Section 7 does not apply to private actors.[160] Additionally, there are so many exceptions to the prohibitions provided by the Act that even those to whom the Act is applicable are often exempted because there are so many mandatory uses of the SSN.[161]

In sum, a Nevada Privacy Act must address the collection of personal information of consumers and assess harsh penalties for those businesses and government agencies that do not adequately secure the information they collect. The penalties must be severe enough to serve as a deterrent by encouraging businesses to consider carefully whether the collection of consumer information is absolutely necessary, and, if they do choose to collect it, they must recognize that they need to take extraordinary measures to safeguard it. The Act must further apply to absolutely *anyone* who collects a Nevadan's personal information and SSN, whether a private entity or individual, or whether a state, local, or federal government agency.

The need for regulation of those that collect the personal data of Nevadans is apparent. After the ChoicePoint breach, a number of bills regarding data breaches were introduced and debated.[162] Almost half of the states have enacted their own data breach notification bills, which require companies to notify clients and consumers if the company believes there is a risk of identity theft as a result of the breach.[163] However, some warn that over-notification could degrade the effectiveness of such notice; as a result, people could end up ignoring the notices and wind up becoming a victim of identity theft.[164] Others argue that the "current bills focus too much on notification and not enough on *preventing* data breaches . . . ."[165] Indeed, a Nevada Privacy Act should focus most on prevention and impose stringent safekeeping standards on those who insist upon collecting personal information.

---

156 *Id.*

157 Sofradzija, *supra* note 128.

158 Richard Lake, *DMV Data Never Accessed*, LAS VEGAS REV.-J., June 7, 2005, at 1B.

159 *Id.*

160 Komuves, *supra* note 9, at 550 ("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.").

161 *Id.* at 554 ("[T]he Privacy Act's restrictions on government usage of the SSN are all but swallowed up by the exceptions.").

162 Grant Gross, *Data Breach Bills Unlikely to Pass Before 2006*, IDG NEWS SERVICE, Nov. 14, 2005, *available at* http://www.pcworld.com/article/id,123515-page,1/article.html.

163 *Id.*

164 *Id.*

165 *Id.* (emphasis added).

3. Inadequacy of Self-Protective Measures

There are some protective measures currently available that can help to reduce the risk of identity theft; however, they are just not enough.

Most notably, Nevada recently became one of a growing number of states that will permit its residents to freeze their credit as a means to help prevent identity theft.[166] A security freeze prevents potential thieves from utilizing SSNs to obtain credit fraudulently by not permitting access to the frozen credit report.[167] No accounts can be opened or loans taken while the freeze is in place. The Nevada bill, codified within Chapter 598C of the Nevada Revised Statutes, passed in June 2005 and became effective October 1, 2005.[168]

Individuals can also undertake a number of self-help measures to reduce the risk of identity theft, or catch a theft in the act before it becomes excessively destructive. The foremost way consumers can be proactive is to check their personal financial information consistently and regularly on their credit reports from all three of the major U.S. credit agencies: Experian, TransUnion, and Equifax.[169] Of particular benefit is the Fair and Accurate Credit Transactions Act (FACT Act), under which consumers can now request and obtain a free credit report once every twelve months from each of the three major consumer credit reporting companies.[170] Indeed, it is difficult to detect identity theft without reviewing credit reports for discrepancies.[171] Consumers should look for unfamiliar accounts that may have been opened by a thief and incorrect reporting of late payments.[172] If consumers discover from their credit reports that they are the victims of identity theft, they should immediately "contact the fraud departments of the three credit reporting agencies, . . . close the accounts that have been tampered with [or] fraudulently opened in [their] name, . . . file a police report, . . . [and] file a report with the Federal Trade Commission."[173]

Of course, consumers must take it upon themselves to request their free credit reports and check their credit report for problems and possible thefts.[174] This is problematic because it requires Nevadans to be educated of the measures they must take to protect themselves from identity theft and they must take the time to be proactive on a regular basis. Further, the expensive services

---

[166] Act of June 13, 2005, 2005 Nev. Stat. 1519.

[167] *Id.*

[168] NEV. REV. STAT. §§ 598C.300 – 598C.390 (2006); Act of June 13, 2005, 2005 Nev. Stat. 1519.

[169] Rep. Jo Ann H. Emerson (R-Mo.), *A Credit Check of Your Own*, (Feb. 26, 2005), http://www.house.gov/list/hearing/mo08_emerson/col_050226.html.

[170] 15 U.S.C. § 1601-1615 (2000).

[171] *Id.*

[172] *Id.*

[173] *Id.* But there are those thieves that are aware of the capabilities of the credit reporting agencies and take measures to prevent the victim from learning about the thief's actions. In one instance, a victim called the credit reporting agencies and asked the agencies to call the victim if someone tried to open a credit card, so to combat this effort, the thief cancelled the victim's phone service so he could not be reached. Morrison, *supra* note 113.

[174] To get a free annual credit report, one should go to http://www.annualcreditreport.com (last visited Mar. 7, 2007). The website suggests to "[f]ight identity theft by monitoring and reviewing your credit report."

offered by credit agencies and banks that purport to monitor the customer's credit records and notify them of any identity theft red flags can fail to perform as they claim and, essentially, offer the same services that a consumer can undertake on one's own by accessing their free credit reports periodically.[175]

Regardless, spotting a discrepancy on a credit report means the thief has already acquired the victim's SSN and the theft has already begun. Checking a credit report regularly may limit the damages, but it does nothing to prevent the theft from happening in the first place. A Nevada Privacy Act must limit the disclosure of residents' SSNs and other personal information to only those situations where the party requesting the information demonstrates that it is absolutely necessary.

Another way people can proactively reduce the risk of identity theft is by shredding their documents before putting them in garbage, thus preventing "dumpster divers"[176] from getting personal information from their trash. A Nevada Privacy Act admittedly would not stop people from going through another's trash. However, a Nevada Privacy Act could prohibit publishing SSNs on statements and bills, thereby reducing the dissemination of SSNs and reducing the chance of a SSN appearing on a document found in someone's trash. For example, health insurance companies and medical service providers often print SSNs on statements sent to clients, which unnecessarily opens the patient up to the risk of a dumpster diver, or a potential mail thief who steals the statement before it even reaches the patient. The Nevada Privacy Act should further require private businesses that request SSNs to refrain from using them as identifiers and instead develop alternative numbers for identification.

Nevadans can also take protective self-help measures by limiting disclosures of their SSN and demanding to be informed about how their personal information will be used when they do choose to disclose it.[177] But such measures may only be of limited assistance because Nevadans must be educated about their ability to withhold disclosure and must be aware that they may be denied service as a consequence.[178] A Nevada Privacy Act could prohibit the denial of services to Nevadans who refuse to produce a SSN by both private agencies and any sort of governmental agency, except, of course, where required by federal statute.

There are a few additional methods of protection from identity theft. People can now protect themselves by purchasing an identity theft endorsement on their homeowners' insurance policy.[179] Insurance companies such as Allstate now offer identity theft coverage; however, there is a limit on the coverage for the endorsement, which is not always enough. Further, this option is not avail-

---

[175] Eric Dash, *Protectors, Too, Gather Profits from ID Theft*, N.Y. TIMES, Dec. 12, 2006, at A1 (noting that the fear of identity theft has prompted more than 12 million people to purchase these credit-monitoring services, which equates to a billion-dollar business).

[176] Morrison, *supra* note 113.

[177] Komuves, *supra* note 9, at 574.

[178] *Id.* at 574-75.

[179] Information pertaining to the identity theft endorsement insurance coverage provided by a friend of the author: Stephanie Kellogg, Insurance Agent, of Holden Financial Service, Inc., in Rutland, Vermont.

able in all states. Of course, not everyone owns a home and not everyone who does can afford the extra coverage. Credit cards typically cover unauthorized charges by identity thieves but "the blunt reality [is] that victims must painstakingly prove – often to disbelieving creditors – that debts are not their own."[180] One telephone service provider recommended that those worried about an identity thief making changes on a phone or cellular account should establish a password on their account that prohibits changes to the account without the code.[181] While these measures may be helpful, they still require Nevadans to be both educated of the measures and proactive in their use.

B. Legislative Guidance from the Privacy Acts of Arizona and California

Some states have recognized that there is no current identity theft preventative law protecting SSNs that is applicable to state and local government agencies besides the federal Privacy Act. They have further recognized that there is absolutely no current law that protects SSNs that are collected by private actors.[182]

In response, a small number of states have created their own Privacy Acts,[183] specifically Arizona and California – fellow Ninth Circuit member states. Indeed, the Acts of these states can serve as a guiding template for the Nevada legislature in considering the needs of Nevadans.

California recognizes the personal and fundamental nature of the right to privacy[184] and acknowledges that "[i]n order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits."[185] California's Information Practices Act of 1977 addresses actions by both government agencies and private entities acting under contract with the government.[186] The statute calls for those requesting personal information first to provide the individual with "a comprehensive disclosure of the purposes and usages of the information."[187] Further, California includes protections for SSN confidentiality by prohibiting the display of SSNs on identification cards or in mailings.[188]

Arizona also provides protection through restrictions on the use of SSNs, including prohibitions against printing SSNs on cards, mailings, or any internet site.[189] Further, the act applies to "a person or entity,"[190] thus both private and

---

[180] Zeller, *supra* note 4.

[181] Morrison, *supra* note 113.

[182] There is the federal Gramm-Leach-Bliley Act, where consumers' SSNs and nonpublic information are protected, but this applies only to disclosure by financial institutions. 15 U.S.C. § 6801 (2000). Similarly, federal law also permits civil actions against anyone who discloses or uses personal information from a motor vehicle record. 18 U.S.C. § 2724 (2000).

[183] Komuves, *supra* note 9, at 559 ("Despite the absence of meaningful federal privacy protections, the states have generally failed to step in with laws of their own.").

[184] CAL. CIV. CODE § 1798.1(a) (West 2005).

[185] *Id.* § 1798.1(c).

[186] Komuves, *supra* note 9, at 560.

[187] *Id.*

[188] CAL. CIV. CODE §§ 1798.85-.86 (West 2005).

[189] ARIZ. REV. STAT. ANN. § 44-1373 (2005).

[190] *Id.*

governmental actors. Effective January 1, 2009, Arizona will also prohibit the use of an alternative identifier to the SSN on any identification or membership card or mailing that uses more than five numbers "reasonably identifiable as being part of an individual's social security number."[191] This restriction will also apply to any material mailed to the resident except on applications or documents intended to confirm the accuracy of the SSN, or to open, amend, or close an account, contract, or policy.[192]

These provisions of both California and Arizona law are all beneficial and should be adopted by Nevada. However, Arizona's penalty provision seems inadequate to serve sufficiently as a deterrent. Violations of the prohibition against printing SSNs on ID cards that are committed "knowingly or intentionally" are subject to a mere $100 civil penalty for each violation.[193] The provision mentions nothing of negligent or unintentional violations, and it offers no incentive for businesses and service providers to investigate the restrictions so that they can "knowingly" abide by them. In contrast, California provides that any complainant who brings a successful suit under the section is entitled to an award of a minimum of $2500 in exemplary damages as well as attorney's fees and litigation costs, on top of any damages awarded.[194] Nevada should impose a substantial fine, as much as or more than that of California, to serve as an effective deterrent and give those who feel it necessary to collect SSNs a powerful incentive to treat and safeguard them with care and with respect for the privacy of the owner.

California is extending its privacy protections of its residents with new bills, including one designed to require that "[s]tate agencies . . . follow strict new standards when handling people's sensitive personal information" and requires approval when there is a request for personal data held in a state agency database.[195] California State Senator Debra Bowen noted that the state needs to make sure that collected personal data is not freely shared because that increases the risk of identity theft.[196] She also observed that California has "moved state agencies and businesses away from using Social Security numbers as public identifiers, from printing them on things they mail to people, and . . . given folks the ability to freeze access to their credit reports, but we're obviously not done yet because identity theft continues to rise . . . ."[197]

The new California bill provides a helpful and useful suggestion for Nevada. The state should initiate an approval process that is required before any resident's SSNs is disclosed to anyone else, including other state agencies. Accordingly, reducing the constant dissemination of SSNs would serve to reduce the risks of identity theft.

---

[191] *Id.* § 44-1373.02 (A)(1) and (2).

[192] *Id.* § 44-1373.02 (A)(2).

[193] *Id.* § 44-1373.03 (A). Any fines collected are paid into a general fund. *Id.*

[194] CAL. CIV. CODE § 1798.53 (West 2005).

[195] *Sen. Bowen's Bill*, *supra* note 5.

[196] *Id.* (Sen. Bowen further argued that it is cheaper to prevent identity theft but difficult to do so when the state disseminates SSNs "to people who don't bother to ensure the information is protected . . . .").

[197] *Id.* (The new bill is argued by Sen. Bowen to "take[ ] the state's identity theft prevention efforts one step further by setting strict privacy and security standards that state agencies have to follow before they give anyone access to information in their databases.").

A Nevada Privacy Act should also prohibit the use of SSNs as personal identifiers and prohibit publishing SSNs on identification or membership cards of any type. There are, of course, potential arguments against imposing prohibitions against using SSNs as personal identification numbers. It is true that "people have a limited amount of memory and cognition, and have a limited capability to remember multiple sequences of numbers"; multiple ID numbers for every business or governmental agency may prove more difficult than having to remember one single number.[198] Economically, the functions of many businesses and government agencies are eased by the use of a numerical identifier for matters including taxation, banking and credit, and driver's licensing.[199] However, the advantages of a prohibition against using SSNs for identification outweigh the disadvantages. The intrusion into a Nevadan's privacy "is demeaning to individuality, [and] an affront to human dignity [because] [p]revalent ideals of liberalism and democracy promote treating people as individuals, not as numbers."[200] Certainly the greater the use of SSNs as personal identifiers, the greater the chance of an identity theft occurring.

Nevada citizens are left vulnerable to identity theft with no means to enforce the federal Privacy Act or secure relief for its violation by state or local government agencies or private actors. The Nevada legislature must take action and create its own state privacy act, similar to those of Arizona and California. Now seems a particularly good time to consider a Nevada Privacy Act because the Nevada legislature recently took steps to allow residents to freeze their credit reports and provide identity theft victims with an ID to help them in their recovery. It is possible that, given this recent legislation, the legislature may currently be open to the suggestion of a Nevada Privacy Act.

Given the adamant decision of the Ninth Circuit in *Dittman v. California* not to provide citizens with a remedy for violations of the Privacy Act by state or local government agencies, it seems the best way to preserve the privacy of Nevadans is for the legislature to undertake the issue, rather than relying on the interpretations and judgments of the judiciary.[201] "An ideal legislative solution would control SSN collection, use and dissemination"[202] and "limit the circumstances in which the SSN can be collected."[203] If it is absolutely necessary that SSNs be collected, they must be protected and only be accessible by those few employees to whom it is essential to fulfill their duties. Those businesses or governmental agencies who do require SSNs should need to prove necessity and must be held responsible for any breaches in privacy by their employees, thus encouraging employers to select carefully only the most trustworthy of employees to have access to clients' and patients' personal information. Further, the businesses should be fined heavily regardless if a theft results from their prohibited actions. The penalties must be harsh in order to compel private

---

198 Komuves, *supra* note 9, at 570.

199 *Id.*

200 *Id.* at 571 (quoting Edward J. Bloustein, *Privacy as an Aspect of Human Dignity*, 39 N.Y.U. L. REV. 962, 973 (1964)).

201 Papandreou, *supra* note 13, at 96.

202 Komuves, *supra* note 9, at 575.

203 *Id.* at 576.

and governmental actors to take extreme measures to safeguard personal information.

In particular, due to the computerization of databases, there need to be "[c]ertain minimum standards for handling and processing personal information . . . to preserve the security of . . . data collection and to safeguard the confidentiality of the information . . . ."[204] Businesses should further be required to shred all documents before discarding them. SSNs should not be used as identifiers for health care purposes[205] or as employee or student ID numbers, and they should not be published on health insurance cards, employee ID cards, or student ID cards. The SSN should be disclosed only as required by federal statute and no further.

IV. CONCLUSION

Nevada cannot wait for the federal government to enact a bill to protect against and prevent identity theft and the over-dissemination and misuse of Social Security numbers. The Nevada legislature has already taken commendable steps by enacting The Identity Theft PASSPORT program, amending Chapter 205 of Nevada Revised Statutes regarding criminal penalties for the misuse of personal information, and permitting residents to freeze their credit to prevent thieves from using stolen SSNs to open new accounts in the victim's good name.

The Nevada legislature should continue its efforts and proactively enact a Nevada Privacy Act with provisions applicable to the state and local governments, and to private entities and individuals. The Act must force a reduction in the overuse of SSNs as personal identifiers and strictly regulate the collection and dissemination of SSNs. It would serve as an incentive for both private and governmental agencies to take measures to protect the personal information it collects and to avoid collecting it unnecessarily, or else face strict penalties for noncompliance. A Nevada Privacy Act is, unfortunately, not a solution to the problem of identity theft, but it is a positive step in the right direction by working to preemptively prevent the thefts from occurring at all.

---

[204] Papandreou, *supra* note 13, at 95.

[205] Minor, *supra* note 1, at 295.