

# **Stealing the Self: Identity Theft and Restrictions on Using and Disseminating Personal Identifiers**

A Report of the Legal Project

Markle Foundation Task Force on National Security  
In the Information Age

August 21, 2002

Sean Fogarty

Researcher  
The Legal Project

Markle Foundation Task Force on National Security in the Information Age

and

Daniel R. Ortiz

John Allan Love Professor of Law and  
Joseph C. Carter, Jr., Research Professor  
University of Virginia



## Introduction

Identity theft is today the fastest growing financial crime in America. It costs billions of dollars annually<sup>1</sup> and its harms run far beyond the economic. It can destroy one's emotional, psychological, and physical well-being. As Senator Jon Kyl, Chairman of the Senate Judiciary Subcommittee on Technology, Terrorism and Government Information put it, "there are few clearer violations of personal privacy than having your identity stolen and used in the commission of a crime."<sup>2</sup>

This report examines the regulation of identity systems in the United States. Part I discusses the growing identity theft problem and Congress's only comprehensive response to it: the Identity Theft and Assumption Deterrence Act of 1998. Part II analyzes the dissemination of specific personal identification information by public and private actors and various legislative responses. It particularly looks at the use of social security numbers (SSNs) as personal identifiers and at legislation which attempts to reign in their use. It also looks at how Congress has limited the accessibility of driver's license information to the public.

### I. Identity Theft and the Identity Theft and Assumption Act of 1998

Identity theft occurs when an individual steals the name, address, and usually the SSN or other identification information of another person. The identity thief then uses the information to open credit card accounts, apply for bank loans, steal money from the victim's bank accounts, and obtain false driver's licenses or birth certificates. Although the crime is primarily financial, with estimated financial losses in excess of \$ 2 billion annually,<sup>3</sup> identity theft also potentially subjects its estimated 500,000 to 700,000 victims per year to various long-lasting secondary effects.<sup>4</sup>

The story of Terry Rogan well illustrates the non-financial implications of having one's identity stolen.<sup>5</sup> In 1981 McKandes, an escapee from prison, began using Rogan's name after obtaining a copy of his birth certificate. He then used the birth certificate to obtain a valid driver's license in Rogan's name. Over the next two years, McKandes committed a series of crimes using Rogan's identity. As a result, a California court issued an arrest warrant for a Terry Rogan and inserted his name into the National Crime Information Center (NCIC) database, which is accessible to law enforcement officials nationwide. From 1982 to 1984, Rogan was twice pulled over for minor traffic infractions and once on suspicion of trespassing. When the officers entered Rogan's information into the NCIC database, they pulled up the outstanding arrest warrant. Each time, Rogan was summarily searched, handcuffed, taken into custody, and detained.

In order to successfully steal someone's identity, the thief must at least know the target individual's name and address and obtain information about the target that a business believes verifies his identity and that only the target himself would know, like his SSN or driver's license number. The more pedestrian identity thief can normally

obtain the desired information by lifting a person's purse or wallet or searching his trash to discover personal information on bank or credit card statements. In the information age in which we now live, however, this hands-on approach is probably more time-consuming than necessary. The internet puts all the personal information necessary to be successful at an identity thief's finger tips. At countless websites, a person's home address, phone number, and email address can be accessed free of charge, and seconds later an identity thief can visit another site and purchase that same individual's SSN. In addition, other private information about an individual can often be found in public records compiled by the government and stored in easily accessed databases.

Prior to the passage of the Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act), identity theft was not specifically regulated or investigated as a crime. Congress relied instead upon a few federal statutes to protect the information necessary to commit identity theft and upon general anti-fraud provisions to punish and redress any injury. Only when identity theft rose dramatically in the 1990s, did Congress decide to address the issue directly.

The Identity Theft Act has two primary purposes: to make the unlawful transfer and use of identity information a federal criminal offense and to establish a right to restitution.<sup>6</sup> Its central provision states that “[w]hoever knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid and abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable State or local law” shall be punished.<sup>7</sup> The Act elsewhere defines “means of identification” as

any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any--

(A) name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(C) unique electronic identification number, address, or routing code; or

(D) telecommunication identifying information or access device ....<sup>8</sup>

In addition, the Act creates criminal penalties;<sup>9</sup> instructs the Federal Trade Commission to receive complaints of identity theft, provide information to targets, and refer complaints to consumer reporting agencies and appropriate law enforcement agencies;<sup>10</sup>

and makes “victims” eligible for restitution under existing law.<sup>11</sup> It also enables the United States Secret Service, the FBI and other law enforcement agencies to combat this crime directly.<sup>12</sup>

The enforcement scheme has several weaknesses. First, of course, a target of identity theft cannot prosecute directly. He must convince a law enforcement agency to investigate and the Department of Justice to prosecute. Second, a target is not usually considered a “victim” under the Victim and Witness Protection Act of 1982 for purposes of restitution.<sup>13</sup> The class of victims extends primarily to those “directly and proximately harmed,”<sup>14</sup> like banks, merchants, and credit card companies who suffer a direct economic loss, and often not to the targets themselves who suffer only indirect economic losses, like attorney’s fees and the costs associated with correcting credit reports.<sup>15</sup> Third, even proper “victims,” like merchants, cannot obtain restitution from a judgment-proof thief.

Despite the Identity Theft Act and laws passed by the majority of states making identity theft a crime,<sup>16</sup> identity theft continues to grow quickly.<sup>17</sup> Commentators have criticized these laws, particularly the Identity Theft Act, for making little difference,<sup>18</sup> for failing to address all the parties responsible for the increase in identity theft,<sup>19</sup> and for being reactionary rather than anticipatory.<sup>20</sup> In response to these and other criticisms, Congress has considered numerous pieces of new legislation addressing identity theft. Nearly 20 bills have been introduced in Congress since the passage of the Identity Theft and Assumption Deterrence Act of 1998. None of these bills, however, has moved beyond the reporting stage.

## **II. Restricting the Use and Dissemination of Personal Identifiers**

### ***Social Security Numbers***

Social Security numbers are the single most useful piece of identification information to identity thieves. Since the implementation of SSNs in 1936, “there have been almost 40 congressionally authorized uses for [them] as an identification number.”<sup>21</sup> As a result, the SSN is the principal identifier used by private persons and government officials, and the identification of choice for identity thieves. Companies trading in financial information are the largest private sector users of SSNs, with credit bureaus maintaining over 400 million files keyed to individual SSNs.<sup>22</sup> Most large universities use SSNs to identify their students. Public and private entities collecting blood donations are required by law to furnish the SSN of the donors. Additionally, the Internal Revenue Code dictates that the SSN be the primary identifying number for all individuals who file tax returns. The largest criminal database in the country maintained by the NCIC includes SSNs in its list of identifying characteristics. Courts, DMVs, federal agencies, professional licensing groups, and student loan administrators all utilize SSNs in the administration of their records. The ubiquitous nature of these once confidential identifiers provide would-be thieves ample opportunity to steal and use them. Despite the

obvious potential for abuse of SSNs, Congress has yet to pass comprehensive legislation restricting their use by private parties. At present private use of SSNs is regulated only by individual laws which apply to particular entities in particular areas.

The primary statutory restriction upon government use of SSNs is found in Section 7 of the Privacy Act of 1974. It states that

- (a) (1) It 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.
- (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.<sup>23</sup>

Although this appears to significantly constrain governmental use of SSNs, Congress has created many exceptions to section 7 that greatly reduce the reach of the Act's central prohibition. For instance, a state may require the disclosure of SSNs for identification purposes "in the administration of any tax, general public assistance, driver's license, or motor vehicle registration law within its jurisdiction . . ."<sup>24</sup> If an individual fails to comply with a state's request for SSNs in these cases, the individual can be denied benefits. The Act, moreover, does not speak to private entities, which can thus require a person to disclose her SSN as a condition for providing a service.

Though on a smaller scale than the Privacy Act, other statutes restrict the collection and dissemination of SSNs. The Freedom of Information Act (FOIA), which generally requires federal agencies to make their records available to the public, contains an exemption allowing an agency to withhold those records that would “disclose information of a personal nature where disclosure would constitute a clearly unwarranted invasion of personal privacy.”<sup>25</sup> FOIA, however, does not speak to when agencies can require SSNs, how they can use them, and whether they can share them with other agencies. The Family Educational Rights and Privacy Act bars educational institutions receiving federal funds from releasing “personally identifiable information” about students to unauthorized persons.<sup>26</sup> And the Fair Credit Reporting Act directly constrains the dissemination of financial information, which usually contains SSNs.<sup>27</sup> In addition, some states have passed laws addressing informational privacy, but commentators have generally criticized these attempts as “failing to provide comprehensive privacy protection.”<sup>28</sup> Although the law protects SSNs from unauthorized use and dissemination in certain areas by certain actors, these protections are narrow and fail to prevent identity thieves from obtaining this essential piece of information.

### ***Driver’s License Information***

Prior to 1997, in many states the easiest way for an individual to get another person’s identity information was simply to purchase the individual’s driving record from the local DMV. For only a couple dollars, anyone could obtain a driver’s full name, address, birth date and license number, which in many states was the same as the individual’s SSN. Thus, the DMV served as a one-stop shop for the would-be identity thief. This practice changed with the passage of the Driver’s Privacy Protection Act of 1994 (DPPA), which required states to adopt procedures restricting access to motor vehicle records.<sup>29</sup> Adopted for reasons unrelated to identity theft,<sup>30</sup> the Act aimed to make a criminal’s access to other people’s identification information more difficult. Over the last five years, state legislation passed in response to the DPPA has somewhat restricted access to this information, but the Act’s exceptions and opt-out provisions have diminished its effectiveness.

The principal provision of the DPPA, § 2721(a), states that “a State department of motor vehicles . . . shall not knowingly disclose or otherwise make available to any person or entity . . . personal information about any individual obtained by the department in connection with a motor vehicle record.”<sup>31</sup> It proceeds to define “personal information” as “an individual’s photograph, social security number, driver identification number, name, address, telephone number, and medical or disability information.”<sup>32</sup> Although these provisions appear to protect personal information collected by the DMV from disclosure, the fourteen exceptions to the provisions ultimately swallow much of the rule. They allow disclosure for use by any government agency,<sup>33</sup> insurance company,<sup>34</sup> court,<sup>35</sup> or by groups dealing with matters concerning motor vehicle or driver safety.<sup>36</sup> The media is also exempt from the disclosure prohibitions when investigating vehicle or driver safety issues. Unlike these exceptions, which are somewhat limited in their capacity for abuse, § 2721(b)(8) gives much hope to identity thieves. This section permits disclosure

to any licensed private investigator. Consequently, any individual who wants to obtain another person's personal information can hire a private investigator to purchase the information from the DMV for him.

The broadest of all the exceptions to the DPPA are the so-called "opt-out provisions" found in § 2721(b)(11) and (12). These provisions permit a state to disclose personal identification information to any individual or business so long as the state provides license holders written notice that includes a clear opportunity to opt-out.<sup>37</sup> While 19 states enacted statutes with disclosure prohibitions as strict or stricter than the DPPA's default standard, the majority of states have enacted a variety of opt-out laws which allow drivers to choose different levels of confidentiality.<sup>38</sup> Minnesota, for example, enacted a law offering drivers a choice between three different levels of confidentiality: drivers can choose (1) not to allow individual inquiries to be made on their records; (2) not to allow personal information to be given out for solicitation purposes; or (3) both options 1 and 2.

Because the Supreme Court did not uphold the constitutionality of the DPPA until 2000,<sup>39</sup> many states did not begin to comply with the law in earnest until recently. How much the DPPA will help in preventing identity theft remains to be seen. The large revenues many states derive from selling the information in their driver's license databases provide some incentive for them to continue disclosure to the maximum extent the law's exceptions allow.

## ENDNOTES

- 1 Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 Tex. L. Rev. 89, 89 (2001).
- 2 *Identity Fraud Protection, Hearings on Identity Theft Before the Subcommittee on Technology, Terrorism, and Government Information*, 105<sup>th</sup> Cong. (May 20, 1998).
- 3 LoPucki, *supra* note 1, at 89.
- 4 *Written Testimony for U.S. Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information*, 106<sup>th</sup> Cong., July 12, 2000, available at [http://www.privacyrights.org/ar/id\\_theft.htm](http://www.privacyrights.org/ar/id_theft.htm), [hereinafter *Testimony*] (statement of Beth Givens).
- 5 See Kurt M. Saunders & Bruce Zucker, *Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act*, 8 Cornell J.L. & Pub. Pol'y 661, 666-67 (1999).
- 6 Martha A. Sabol, *The Identity Theft and Assumption Deterrence Act of 1998 - Do Individual Victims Finally Get Their Day in Court?* 11 Loy. Consumer L. Rev. 165, 169 (1999).
- 7 18 U.S.C. § 1028(a)(7) (1998).
- 8 *Id.* § 1028(d)(4).
- 9 *Id.* § 1028(b).
- 10 Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, § 5, 112 Stat. 3007, 3010 (1998).
- 11 18 U.S.C. § 3663.
- 12 Statement by the President of the United States, 34 Weekly Comp. Pres. Doc. 2203 (Oct 30, 1998).
- 13 18 U.S.C. §§ 3663-64.
- 14 *Id.* §§ 3663(a)(2) & 3663A(a)(2).
- 15 See *United States v. Blake*, 81 F.3d 498, 505-07 (4<sup>th</sup> Cir. 1996).
- 16 For a list of state statutes, see <http://www.consumer.gov/idtheft/statelaw.htm>.
- 17 See, e.g., John Batteiger, *Online Guide; Identity Theft: Web Resources Can Help You Keep Your ID Safe*, San Francisco Chronicle, July 8, 2001, at E3 ("Reports of identity theft have increased 40 percent in each of the past two years, according to one credit-reporting agency ...").
- 18 LoPucki, *supra* note 1, at 89.
- 19 *Testimony*, *supra* note 4.
- 20 Nicole M. Buba, *Waging War Against Identity Theft: Should the United States Borrow from the European Union?*, 23 Suffolk Transnat'l L. Rev. 633, 648 (2000).
- 21 Richard Sobel, *The Degradation of Political Identity Under a National Identification System*, 8 B.U. J. Sci. & Tech. L. 37, 56 (2002).
- 22 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, 536 (1998).
- 23 Privacy Act of 1974, Pub. L. No. 93-579, § 7, 88 Stat. 1896, 1909 (1974).
- 24 42 U.S.C. §405(c)(2)(C)(i) (1988).
- 25 5 U.S.C. § 552(b) (1994); See *Sherman v. United States Dep't of the Army*, 244 F.3d 357 (5<sup>th</sup> Cir. 2001).
- 26 Komuves, *supra* note 22, at 557; see *U.S. v. Miami Univ.*, 294 F.3d 797 (6<sup>th</sup> Cir. 2002).
- 27 15 U.S.C. §1681 (2002).
- 28 See *Yang v. Government Employees Ins. Co.*, 146 F.3d 1320 (11<sup>th</sup> Cir. 1998).
- 29 18 U.S.C. § 2721 (1994 & Supp. II 1997).
- 30 California legislators began the movement for government database reform after the murder of actress Rebecca Schaeffer by a stalker who obtained her name and address from the DMV. Congress then passed this legislation to prevent individuals from using DMV-compiled personal information to commit violent crimes.

31 18 U.S.C. § 2721(a) (1994 & Supp. II 1997).  
32 18 U.S.C. § 2725(3) (1994).  
33 18 U.S.C. § 2721(b)(1) (1994 & Supp. II 1997).  
34 *Id.* § 2721(b)(6).  
35 *Id.* § 2721(b)(4).  
36 *Id.* at § 2721(b)(2).  
37 Angela R. Karras, *The Constitutionality of the Driver's Privacy Protection Act: A Fork in the*  
*Information Access Road*, 52 Fed. Comm. L.J. 125, 131 (1999).  
38 *Id.* at 132-33.  
39 *Reno v. Condon*, 528 U.S. 141 (2000).