# REAL ID: The Devil You Don't Know

*Geoffrey D. Kravitz**

## I. Introduction

One of the principal recommendations of *The 9/11 Commission Report* suggested that the federal government implement standards for identification cards to combat terrorism.[1] In 2005, Congress responded by passing the REAL ID Act.[2] The Act requires the Department of Homeland Security (DHS) to create federal standards for identification cards that would be acceptable for certain official uses such as entering federal buildings and nuclear facilities and boarding commercial airplanes.[3] However, the proposed solution's reliance on an interconnected national database, an unencrypted barcode on each card and biometric identification increases the risk of identity theft, fraud and dissemination of private information without providing strong counterterrorism protection.

This Article argues that, despite a history of American resistance to a national identification system, the REAL ID Act and DHS regulations mandate issuance of unique identification numbers to individuals, numbers that will be accessible through a nationwide network of DMV databases.[4] In essence, this combination creates a de facto national ID card. This Article demonstrates that the government's failure to adequately secure these new technologies increases the potential for nongovernmental entities, such as hackers and private organizations, to access individuals' personal information.[5] To counteract these emerging privacy threats, this Article proposes a combination of technological and legislative solutions aimed at both securing the REAL ID technologies and providing citizens harmed by REAL ID privacy invasions with a cause of action against the government.[6]

---

* J.D. Candidate, University of Maryland School of Law, 2009, and Technology Editor for the Maryland Law Review. Special thanks to Danielle Keats Citron, Associate Professor of Law, University of Maryland School of Law, for her brilliant guidance and unwavering support. The suggestions and insights of Veronica Berruz, Kerry T. Cooperman, and the editors of the *Harvard Law and Policy Review* proved invaluable in the writing of this piece.

[1] *See* National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report 390 (2004).

[2] REAL ID Act of 2005, Pub. L. No. 109-13, 119 Stat. 231, 302 (codified in scattered sections of 8 U.S.C. and 49 U.S.C.).

[3] REAL ID Act, § 201(3).

[4] *See infra* Part III.A.

[5] *See infra* Parts III.B-D.

[6] *See infra* Part IV.

## II. Background

Prior to the REAL ID Act, Congress and the American public consistently rejected national identification cards. Although some have argued that a Social Security Number (SSN) effectively serves as a national identifier because of its widespread use, the government never intended to use the SSN for identification purposes.[7] Other proposals to create a national identifier have also failed.[8]

### *A. The REAL ID Act of 2005*

Against this longstanding opposition to a national ID system, Congressman Sensenbrenner introduced the REAL ID Act on January 26, 2005.[9] Title II of the REAL ID Act, "Improved Security for Driver's License and Personal Identification Cards," details the minimum standards for federal use of state-issued ID cards. Section 202(b) mandates that the card contain certain identifying information, including the cardholder's full legal name, date of birth, gender, identification number, and digital photograph.[10] Section 202(d) requires state Departments of Motor Vehicles (DMVs) to retain copies of documents used to verify a cardholder's identity, subject all applicants to facial image capture, maintain a statewide database of the identification information, and make the database electronically available to all other states.[11] Section 205 of the REAL ID Act vests the Secretary of Homeland Security with the authority to make regulations and set standards.[12]

---

[7] Jim Kouri, *Social Security Cards: De Facto National Identification*, American Chronicle, Nov. 29, 2005, http://www.americanchronicle.com/articles/3911. In 1971, a SSN task force chose not to expand Social Security Cards into a national ID card. Social Security Administration, Social Security Number Policy Chronology, http://www.socialsecurity.gov/history/ssn/ssnchron.html (last visited Apr. 9, 2009).

[8] *See e.g.*, U.S. Dep't of Health, Educ., and Welfare, Secretary's Advisory Comm. on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens (July 1973), *available at* http://aspe.hhs.gov/datacncl/1973privacy/c7.htm (opposition by the Secretary of Health, Education and Welfare to the use of Social Security numbers as a standard identifier); Tom Ridge, Sec'y, Dep't of Homeland Sec., Remarks at National Press Club (Sep. 7, 2004), *available at* http://www.dhs.gov/xnews/speeches/speech_0203.shtm (noting that DHS's enabling act forbids the creation of a national ID card).

[9] *See* H.R. 418, 109th Cong. (2005). Its provisions were attached as a rider to H.R. 1268, which President Bush signed into law on May 11, 2005. REAL ID Act of 2005, Pub. L. No. 109-13, 119 Stat. 231, 302 (codified in scattered sections of 8 U.S.C. and 49 U.S.C.). All Congressional actions on H.R. 1268, 109th Cong. (2005) are available at http://thomas.loc.gov/cgi-bin/bdquery/z?d109:HR01268:@@@X.

[10] REAL ID Act, § 202(b).

[11] *Id.* § 202(d).

[12] *Id.* § 205.

### *B. DHS Regulations*

On March 1, 2007, DHS proposed regulations for implementing the REAL ID Act.[13] During a 60-day period of public comment, the American Civil Liberties Union (ACLU) gave the regulations a failing grade because they did not adequately address privacy concerns.[14] Likewise, PrivacyActivism.org and several other civil liberties groups submitted comments to DHS recognizing that the technology DHS intended to use jeopardizes cardholders' privacy.[15]

On January 11, 2008, DHS issued its final rule for federally acceptable identification cards[16] and addressed the public comments.[17] The applicability and definition sections of Subpart A identify the scope of the rule.[18] Subpart B sets forth the documentation necessary to obtain a REAL ID, the methods that DMVs must use to verify the applicant's identity, and the physical aspects that a card must meet to comply with REAL ID standards.[19] Subpart C addresses the retention of an applicant's identification documents as well as state DMV databases.[20] Subpart D outlines the minimum security precau-

---

[13] Press Release, Dep't of Homeland Sec., DHS Issues Proposal for States to Enhance Driver's Licenses (Mar. 1, 2007), *available at* http://www.dhs.gov/xnews/releases/pr_1172765989904.shtm.

[14] Press Release, American Civil Liberties Union (ACLU), New Regulations Get an 'F' in Solving Problems With Real ID Act, ACLU Scorecard Shows (Mar. 8, 2007), *available at* http://www.aclu.org/safefree/general/28913prs20070308.html.

[15] PrivacyActivism, Real ID Comments to DHS from PrivacyActivism, CASPIAN, and FCPC (May 8, 2007), *available at* http://stoprealid.privacyactivism.org/docs/Real%20ID%20comments-final.htm.

[16] Press Release, Dep't of Homeland Sec., DHS Releases REAL ID Regulation (Jan. 11, 2008), *available at* http://www.dhs.gov/xnews/releases/pr_1200065427422.shtm.

[17] *See* Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 73 Fed. Reg. 5,290–93 (Jan. 29, 2008) (codified at 6 C.F.R. § 37).

[18] *See* 6 C.F.R. § 37 (2008). Subpart A of the rule states that the function of a REAL ID card is limited to "official purposes." *Id.* § 37.1. The final rule defines "official purposes" as 1) accessing Federal facilities, 2) boarding Federally-regulated aircraft, and 3) gaining entrance to a nuclear facility. *Id.* § 37.3. According to Section 201(3) of the REAL ID Act, however, the DHS Secretary may expand the definition. REAL ID Act of 2005, Pub. L. No. 109-13, § 201(3), 119 Stat. 231, 312.

[19] *See* 6 C.F.R. §§ 37.11–29 (2008). The regulations require all applicants to submit to a photograph and specify the "source documents" an applicant must present to the state DMV in order to obtain a REAL ID card. *Id.* § 37.11. The rule defines "source document(s)" as the "original or certified copies (where applicable) of documents presented by an applicant . . ." for a REAL ID card. *Id.* § 37.3. The rule also requires that before a DMV issues a REAL ID card, it must verify the applicant's documents through an electronic validation system. *Id.* § 37.13. All REAL ID cards must include, among other things, the cardholder's full legal name, date of birth, gender, address, unique identification number, biometrically readable facial photograph, dates of issuance and expiration, and state of issuance. *Id.* § 37.17. All of this information must also be encoded into an unencrypted barcode printed on the REAL ID card. *Id.* § 37.19.

[20] 6 C.F.R. §§ 37.31, 37.33. Subpart C permits each state to determine the format in which to maintain source documents, sets the minimum length of retention for each document format—seven years for paper documents and ten years for microfiche and digital images—and outlines the specifications for digital image retention. *Id.* § 37.31. The rule also requires each state DMV to operate a database that contains a record for each individual. *Id.* § 37.33.

tions DMVs must implement to protect the privacy of REAL ID cardholders.[21]

## III. Analysis of The REAL ID Act and DHS's Final Rule

The REAL ID Act and DHS regulations fail to adequately address significant privacy issues raised by the creation of federal standards for ID cards. The security of the cardholder's personal information, which DHS requires state DMVs to maintain, is questionable. Because the card's security features are meant to prevent fraud, not to protect the privacy of the cardholder's personal information,[22] these features fail to adequately ensure that private information is not disseminated. Additionally, because the Act does not set any finite limits on the use of the card, slight changes in DHS regulations could expand the permissible uses and lead to privacy infringements.[23]

### *A. The REAL ID Act and DHS Regulations Create a National Identification Card and a National Database Connected By a National Identification Number*

To comply with the REAL ID Act and its implementing regulations, state-issued identification cards and driver's licenses must contain personal information. Both the front of the card and the barcode must include the state of issuance and a unique driver's license or identification card number.[24] These rules effectively create a national ID card and a national identifier.

Arguably, the regulations avoid a nationwide identifier by requiring that the identification number be unique only within the issuing jurisdiction.[25] A search based solely on a cardholder's ID number will not necessarily return a single record because two or more REAL ID cardholders in

---

The database record must include all information printed on a REAL ID card or within the barcode, as well as the cardholder's SSN, and his or her driving history. *Id.*

[21] 6 C.F.R. §§ 37.41–45. Subpart D calls for each state DMV to create a security plan that protects cardholders' personal information. The state's plan must include "reasonable" safeguards to shield against the unauthorized access, use, or dissemination of data maintained by the DMV. *Id.* § 37.41(b)(2)(i). The plan must also contain a privacy policy. *Id.* § 37.41(b)(2)(ii). Subpart E controls the certification procedures for state ID cards, and Subpart F regulates noncompliant state IDs. *Id.* §§ 37.51–37.65, 37.71.

[22] REAL ID Act of 2005, Pub. L. No. 109-13, § 202(b)(8), 119 Stat. 231, 312 (requiring "[p]hysical security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purposes.").

[23] The Real ID Act delegates the responsibility of further defining an "official purpose" to the unelected Secretary of DHS. REAL ID Act § 201(3).

[24] 6 C.F.R. §§ 37.17, 37.19 (2008).

[25] *See* 73 Fed. Reg. at 5,290–91 (Jan. 29, 2008) (codified at 6 C.F.R. § 37) ("the final rule does not require that the REAL ID driver's license or identification card number or design be unique nationally, thus possibly limiting the functionality of the REAL ID card or identification number as a national ID card").

different jurisdictions could have identical numbers. Yet this so-called protection could be undermined by the requirement that the face and barcode of REAL ID cards include both the state of issuance and identification number.

As a result of this requirement, states could create a de facto national identifier in at least three ways. First, a state could use the jurisdiction and identification number to form the equivalent of a unique identifier. A search based upon the unique identification number and the issuing jurisdiction would ensure the same amount of accuracy as a database with a unique key, such as an SSN or a national ID number.[26] Second, each state could use a different number of digits for its identification numbers or could use a unique algorithm that identifies the state of issuance, as credit cards do. Third, states could create a unique key by attaching the two-letter abbreviation for the jurisdiction to the end of the identification number.[27]

The DHS regulations also require applicants for REAL ID cards to provide personal information, which a national network of state DMV databases will store and make searchable, posing an additional privacy concern. The regulations require individuals to submit their SSNs, valid passports, birth certificates, or REAL ID cards.[28] State DMVs must retain copies of applicants' photographs for at least five years and source documents for at least seven years.[29] Each DMV must operate a database that is electronically accessible by other DMVs and includes all information contained on the REAL ID card.[30]

Although neither the final rule nor the REAL ID Act expressly requires a centralized national database, DHS has admitted that the regulations compel a central "hub" to facilitate document verification and access across DMVs.[31] DHS identified two interconnected systems that, together, could potentially act as the hub: AAMVAnet and the Commercial Drivers Licensing System (CDLIS).[32] Regardless of which system DHS uses to create the hub, the necessary result will be a decentralized national database that pro-

---

[26] A unique key is a field within a database record which is unique to that record. In a database of people, for example, fields might include "Name," "Birthday" and "SSN." A search for a person's name or birthday would return records for all people with that name or birthday, but a search for a person's SSN would only return the searched-for person's SSN.

[27] Thus, the records for Doe I, who lives in Maryland and has an ID number of 000-00-000 and Doe II, who lives in Massachusetts and has the same ID number, could have the unique keys 000-00-000MD and 000-00-000MA, respectively.

[28] 6 C.F.R. § 37.11(c)(1) (2008).

[29] *See id.* §§ 37.11(a), 37.31.

[30] *Id.* §§ 37.31, 37.33.

[31] *See* REAL ID Act of 2005, Pub. L. No. 109-13, 119 Stat. 231, 302 (2005) (codified in scattered sections of 8 U.S.C. and 49 U.S.C.); 6 C.F.R. § 37.

[32] Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 73 Fed. Reg. at 5,275-76. AAMVAnet is a private network not directly connected to the Internet. Brenda Cruden, *Data Sharing on the DMV Highway*, FEDERAL COMPUTER WEEK, May 31, 1997. The CDLIS database, which runs on the AAMVAnet network, acts as a clearinghouse for state-to-state communications. *See* American Association of Motor Vehicle Administrators, AAMVA: Commercial Driver's License Information System (CDLIS), http://www.aamva.org/TechServices/AppServ/CDLIS/ (last visited Apr. 9, 2009).

vides access to the personal information contained in all of the state DMV databases.

Taken together, the REAL ID Act and the DHS final rule create a national ID card, with a unique identifier for each resident, and a national database to make all of the accompanying information accessible. Even setting aside the clear history of opposition to a national identifier, this system increases the risk of identity theft and decreases security by failing to protect the information on the card's barcode, relies on fallible biometric technology, and creates a national database of questionable security. Further, the Act and regulations fail to protect against expanded usage of the card beyond the original purposes of providing identification when boarding commercial aircraft and accessing federal facilities and nuclear power plants.

### *B. Privacy Concerns and Vulnerabilities of a National Identification Card*

Two features of the REAL ID card's physical requirements endanger cardholders' privacy. The first is the unencrypted barcode, which vendors could use to glean private information simply by swiping the ID card. Because the card gives the vendor enough information to identify and distinguish among cardholders, it incentivizes vendors to maintain a database of customers for marketing purposes.[33] The second feature, the biometric photograph, creates a privacy risk because biometric verification systems routinely misidentify people and can be manipulated through the reverse engineering of biometric templates.[34]

#### 1. *Use and Abuse of the Barcode by Third Parties*

DHS is not the only entity interested in identifying individuals. Many other organizations, such as data brokers, political parties, and companies that maintain customer databases, also seek to correctly identify individuals.[35]

Targeted, or "database," marketing tailors marketing efforts to individuals with shared characteristics.[36] Also known as direct marketing, this practice is efficient because it increases the likelihood of success through personalized advertising and eliminates the waste of marketing to people outside the target group.[37] Direct marketing, however, relies on an organization's ability to accurately identify whether a particular person falls into the target group. A unique identifier is an integral part of direct marketing because it allows an entity to authenticate the identity of potential consumers and to differentiate between consumers with similar identifying information.

---

[33] *See infra* Part III.B.i.
[34] *See infra* Part III.B.ii.
[35] *See* DANIEL J. SOLOVE, THE DIGITAL PERSON 19–21 (2004).
[36] *Id.* at 19.
[37] *See id.* at 18.

An organization that uses direct marketing can either maintain its own database of customers or hire one of several "data brokers" that aggregate and sell individuals' information.[38] An organization's private database will contain only information related to the organization's business and will use a unique key, such as an SSN, to distinguish between customers. If the organization's database uses the same unique key as another company, or of a date broker, the organization can easily find shared customers and seamlessly import the other company's information into its database. Because the necessary data is readily available on the REAL ID card, and the card provides a common key, companies will begin to use the REAL ID-based identifier to key their databases.

The likelihood that private entities will use the new national identifier is magnified because the information is available in the card's barcode. The DHS regulations require the barcode data be encoded using the PDF417 standard.[39] This widely used standard encodes information in two dimensions (2D barcode).[40] Currently, forty-five out of fifty-one jurisdictions use a 2D barcode on their state-issued ID cards.[41] Most of these jurisdictions encode the basic information that is readily available on the front of the card.[42] However, because of the increased storage capacity of a 2D barcode, some states include other information such as fingerprints, facial recognition templates, and photographs.[43]

Various businesses already scan ID barcodes and automatically record the information in a database. Today, a business (or individual) can buy a scanner capable of scanning a PDF417 barcode for under $120.[44] Bars and convenience stores swipe IDs to ensure that patrons are of legal age to purchase alcohol.[45] Cigarette companies offer promotional items in ex-

---

[38] *See, e.g.*, ChoicePoint, Authentication Solutions Brochure 6 (2005) (claiming a database of 17 billion public records), *available at* http://www.choicepoint.com/authentication/common/pdfs/CPAS_Brochure.pdf (on file with the Harvard Law School library); Acxiom: About the Acxiom Corporation, http://www.acxiom.com/about_us/Pages/AboutAcxiom.aspx (last visited Apr. 20, 2009) (stating that Acxiom updates 10 billion records each month and has demographic records on 500 million people) (on file with the Harvard Law School library).

[39] 6 C.F.R. § 37.19 (2008).

[40] A 2D barcode can store up to 100 times more data than its one-dimensional counterpart. Gilles Lisimaque, Senior Vice President, GEMPLUS, Presentation to the Carnegie Mellon University Workshop on States Security: Technologies for ID Tokens 20 (Mar. 27, 2002), *available at* http://rack1.ul.cs.cmu.edu/tw/statessecurity/lisimaque.pdf (on file with the Harvard Law School Library).

[41] Only California, Michigan, New Mexico, Ohio, Texas, and Wyoming do not have a 2D barcode on their licenses. AAMVA, Standards – U.S. License Technology, http://www.aamva.org/KnowledgeCenter/Standards/uslicensetechnology.htm (last visited Apr. 20, 2008) (on file with the Harvard Law School Library).

[42] American Association of Motor Vehicle Administrators, Personal Identification — AAMVA International Specification — DL/ID Card Design 50 (2005), http://www.aamva.org/AAMVA/DocumentDisplay.aspx?id={66260AD6-64B9-45E9-A253-B8AA32241BE0}.

[43] Jennifer 8. Lee, *Welcome to the Database Lounge*, N.Y. Times, Mar. 21, 2002, at G1.

[44] *See* Provantage Bar Code Reader, MS9520 Voyager Ocia Kit 9PIN F, http://www.provantage.com/metrologic-mk9520-72b09~7MTRO00R.htm (last visited Apr. 9, 2009).

[45] SWIPE, Data-Collection from Driver's Licenses, http://www.we-swipe.us/research.html#who (last visited Apr. 9, 2009).

change for barcode access.[46] A Boston bar owner, who purchased a scanner in 1999 for $2,500, scanned over 1.3 million customers in only three years.[47]

The Drivers' Privacy Protection Act (DPPA), which protects against dissemination of the information contained on a driver's license,[48] is inadequate. Many businesses, such as liquor stores, will come under the DPPA's legitimate business needs exception.[49] For example, any time a person uses a credit card, a business has a legitimate need to authenticate the identity of the purchaser to ensure against fraudulent purchases.[50] This is especially true for online purchases, where businesses cannot rely on a visual signature match.

DHS's decision to use the PDF417 standard invites business to swipe REAL ID cards. The broad use of PDF417 barcodes, from home-printed postage and package tracking to hospital patient bracelets and medications,[51] makes the scanning technology widely available to third parties.

Additionally, DHS's decision to use the PDF417 standard and to leave the information unencrypted creates a significant risk of fraud and identity theft. Currently, the Internet offers several free software tools to encode and decode PDF417 barcodes.[52] Thus, any person with access to the Internet and a printer could manufacture a false barcode, print it on a sticker, and affix it over the barcode on his or her REAL ID. Such fraud would likely pass the cursory examination of a convenience store clerk or a security guard at a crowded bar.

Although a majority of jurisdictions already use a 2D barcode on their state-issued driver's licenses, the PDF417 barcode creates additional privacy risks. The unencrypted barcode requirement decreases the security for citizens in jurisdictions that now require encryption.[53] Further, the standardization of barcodes ratchets up the risk of nationwide swiping by merging the various scanning and decoding technologies into a single standard; this consolidation eliminates the protection that barcode variation among jurisdictions would otherwise provide.

---

[46] *Id.*

[47] Lee, *supra* note 43.

[48] *See* 18 U.S.C. § 2721 (2006).

[49] *Id.* § 2721(b)(3).

[50] Privacy Rights Clearinghouse, Alert: Can Stores Require an ID When I Pay by Credit Card? Feb. 5, 2008, http://www.privacyrights.org/ar/Alert-FS15.htm (last visited Apr. 9, 2009).

[51] Omniplanar, PDF417 2D Bar Code Information, http://www.omniplanar.com/PDF417-2D-Barcode.php (last visited Apr. 9. 2009).

[52] *See e.g.*, SourceForge.net, pdf417 decode, http://sourceforge.net/projects/pdf417decode/default.html (last visited Apr. 9, 2009) (software program that can decode a portable bitmap image file of a PDF417 barcode).

[53] *See* SWIPE, The SWIPE Toolkit: Decode Your Barcode, http://turbulence.org/Works/swipe/barcode.html (last visited Apr. 20, 2008).

2. *Use and Abuse of the Biometric Photograph*

The DHS requirement that all REAL ID applicants consent to a biometric photograph also raises privacy concerns. Because no biometric system is 100% accurate, reliance on the biometric photograph, especially an older photograph, can lead to misidentification. Additionally, computer scientists have proven that they can reverse engineer a photograph from a biometric template that is capable of deceiving the system into false identification.[54]

Two distinct processes comprise a biometric system. The first step is enrollment and facial image capture,[55] which the DHS rule requires whenever an individual applies for a REAL ID card.[56] The second step is matching a new facial image to an existing enrollment template.[57] The matching image must first be transformed into a template, which can then be matched in one of two ways: verification or identification.[58] Verification involves matching an individual with a single enrollment template through a simple one-to-one matching scheme.[59] A bar, for example, might use biometric verification by taking a picture of a patron, creating a matching template, and comparing that template with the enrollment template stored on a REAL ID card. Identification uses a more complex, one-to-many matching scheme by which a matching template is used to search a database of biometric templates.[60]

Several localities have implemented biometric facial recognition systems with limited success. Tampa, Florida created a system to scan the faces of Super Bowl patrons in early 2001,[61] but discontinued it in 2003 because it was ineffective[62] A system installed in Virginia Beach in 2002 did not produce a single match within the first several years.[63] The success rate of an identification system at Logan Airport in Boston, Massachusetts was just above 60%.[64]

---

[54] ANDY ADLER, CAN IMAGES BE REGENERATED FROM BIOMETRIC TEMPLATES? 1 (2003), *available at* http://www.identityblog.com/wp-content/resources/adler-2003-biometrics-conf-regenerate-templates.pdf.

[55] INTERNATIONAL BIOMETRIC GROUP, AAMVA UID9 BIOMETRIC IDENTIFICATION REPORT 108 (2003), http://www.aamva.org/aamva/DocumentDisplay.aspx?id={AE7005C8-9098-496C-82E4-11951ED5EF91}.

[56] 6 C.F.R. § 37.11(a) (2008).

[57] *See* INTERNATIONAL BIOMETRIC GROUP, *supra* note 55, at 104.

[58] Ishwar K. Sethi, *Biometrics: Overview and Application*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY 117, 120 (Katherine Strandburg & Daniela Stan Raicu eds., 2006).

[59] INTERNATIONAL BIOMETRIC GROUP, *supra* note 55, at 104.

[60] *Id.*

[61] Ross Kerber, *Viisage, Visionics, and Others Shop Their Face-Scanning Systems*, BOSTON GLOBE, Dec. 31, 2001, at C1.

[62] Lisa M. Bowman, *Tampa Drops Face-Recognition System*, CNET NEWS, Aug. 21, 2003, http://www.news.com/Tampa-drops-face-recognition-system/2100-1029_3-5066795.html.

[63] Joshua Ortega, Op. Ed., *Frown, You're on Face-Rec Camera*, SEATTLE TIMES, Apr. 28, 2003, at B5.

[64] Richard Willing, *Airport Anti-Terror Systems Flub Tests*, USA TODAY, Sep. 2, 2003, at 3A.

In 2003, AAMVA hired the International Biometric Group (IBG) to study the feasibility of implementing a biometric system capable of searching a template database of 300 million records.[65] Ultimately, IBG concluded that "facial recognition will *not* be capable of successfully" identifying a person from a database containing 300 million biometric templates.[66] Thus, a facial recognition system designed to search the national network of DMV databases would fail to perform accurate identification.

A person can also trick biometric facial recognition systems into making a false positive identification. One academic has created an algorithm capable of reverse engineering a sample template to create a facial image.[67] His report concluded that "a fairly high quality image of a person can be automatically regenerated" from a biometric template.[68]

### *C. Privacy Concerns and Vulnerabilities of a National Database*

A system that can access the information stored in state DMV and federal databases carries the risk of serious privacy invasions. The system is vulnerable for two reasons: technological weaknesses and exploitation, including bribery, cons and unintentional dissemination of data.

#### 1. *Technological Weaknesses*

The system envisioned by DHS is susceptible to two primary technological risks. First, hackers can invade the system from a remote location. Second, the software applications could contain glitches and provide inaccurate information about REAL ID applicants and cardholders.

Hacking attempts against government computer systems have occurred with alarming frequency in recent years. In 2005, a hacker circumvented "a number of security safeguards" and stole a file containing personal information of Department of Energy employees.[69] In 2006, computer hackers accessed the State Department's network.[70] In 2007, a successful hacking attempt forced the Pentagon to take a segment of its system offline.[71]

---

[65] INTERNATIONAL BIOMETRIC GROUP, *supra* note 55, at 1. The U.S. population hit the 300 million mark 3 years after the IBG study. Press Release, U.S. Census Bureau, Nation's Population to Reach 300 Million on Oct. 17 (Oct. 12, 2006), *available at* http://www.census.gov/Press-Release/www/releases/archives/population/007616.html.

[66] INTERNATIONAL BIOMETRIC GROUP, *supra* note 55, at 1 (emphasis added).

[67] ADLER, *supra* note 54.

[68] *Id.* at 2.

[69] H. Josef Herbert, *DOE Computers Hacked; Info on 1,500 Employees Taken*, ASSOCIATED PRESS, Jun. 9, 2006, *available at* http://www.usatoday.com/news/washington/2006-06-09-doe-computers_x.htm.

[70] Larry Greenemeier, *State Department Hack Escalates Federal Data Insecurity*, INFO. WEEK, July 12, 2006, *available at* http://www.informationweek.com/news/showArticle.jhtml?articleID=190302905.

[71] Demetri Sevastopulo, *Chinese Hacked into Pentagon*, FIN. TIMES (Washington), Sep. 3, 2007, *available at* http://www.ft.com/cms/s/0/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac.html; Jennifer Griffin, *Pentagon Source Says China Hacked Defense Department Computers*, Sep. 4, 2007, http://www.foxnews.com/story/0,2933,295640,00.html.

A system based on AAMVAnet and CDLIS would be largely immune from hacking attempts because they bypass the Internet.[72] However, neither the REAL ID Act nor the DHS rule explicitly prohibits a system that connects to the Internet.[73] Further, electronic verification systems like Social Security Number Verification Service (SSNVS) and System Alien Verification for Entitlements (SAVE), which send sensitive information such as an applicant's name, SSN, date of birth, and address over the Internet, are susceptible to remote computer hacking.[74]

Additionally, databases could seriously misrepresent people's personal information. For example, a recent update to the CDLIS Access program notes that a prior version of the software had "[a] bug that caused the Hazmat History information to sometimes display incorrectly on the Accident/Convictions page. . . ."[75] Because employers who hire commercial drivers are permitted to query the CDLIS database to verify applicants' driving histories,[76] this error could have prevented innocent people from obtaining jobs or allowed applicants with hazmat accident histories back on the roads.

Similarly, the SAVE system had a major design failure that came to light in a 2003 Government Accountability Office (GAO) report.[77] According to the GAO report, a SAVE system user could bypass the verification process simply by inventing a SAVE reference number.[78] The user could enter the invented number into the SAVE system rather than perform an actual SAVE verification.[79]

The primary weakness of the interlinked system envisioned by DHS, however, is that access at any specific point allows access to the entire system. Once a hacker has access to the AAMVAnet, he can find information on anyone with a driver's license. Currently, this risk is limited to those with commercial driver's licenses; those with noncommercial licenses have the additional protection provided by the compartmentalization of their informa-

---

[72] *See* American Association of Motor Vehicle Administrators, AAMVA Subscription for Telecommunication Services 4, *available at* http://www.aamva.org/aamva/DocumentDisplay.aspx?id=%7BF8FE718B-B249-499A-922B-303D7CA24A28%7D.

[73] *See* REAL ID Act of 2005, Pub. L. No. 109-13, 119 Stat. 231, 302 (2005) (codified in scattered sections of 8 U.S.C. and 49 U.S.C.); 6 C.F.R. § 37 (2008).

[74] *See* 6 C.F.R. § 37.13(b)(3) (requiring the DMV to query the SAVE system for noncitizen applicants and to verify a citizen-applicant's SSN, birth certificate, or passport).

[75] FED. MOTOR CARRIER SAFETY ADMIN., RELEASE NOTES FOR THE FMCSA IT DEVELOPMENT DIVISION 17 (2008), http://infosys.fmcsa.dot.gov/PublicDocument/softwarereleases/2008%20Release%20Notes/ReleaseNotes%20v1.12.pdf.

[76] For examples of companies offering this service, see http://www.ebiinc.com/services/cdlis_list_report.htm and http://www.background-checks-systems.com/driving-records-dmv.htm.

[77] GOV'T ACCOUNTABILITY OFFICE, SOCIAL SECURITY ADMINISTRATION: ACTIONS TAKEN TO STRENGTHEN PROCEDURES FOR ISSUING SOCIAL SECURITY NUMBERS TO NONCITIZENS BUT SOME WEAKNESSES REMAIN, GAO-04-12 10 (Oct. 2003), *available at* http://www.gao.gov/new.items/d0412.pdf.

[78] *Id.*

[79] *Id.*

tion by jurisdiction. Extending the system to non-commercial drivers would subject almost 190 million additional citizens to this vulnerability.[80]

A DHS-run system may not offer better security. In 2005, when Congress passed the REAL ID Act, DHS received a failing grade for computer security.[81] Admittedly, DHS has made great strides in the last two years, attaining a grade of "B" in 2007.[82] Without comparative data from a standardized security test, it is difficult to determine which system would be less vulnerable to attacks.

2. *The Human Element*

A second way in which one could access the database is by exploiting the system. Although bribery, cons and unintentional dissemination are not unique to REAL ID information, the potential harm they pose in the REAL ID context is much greater. Currently, each citizen's private information is segregated; a breach in one jurisdiction would not affect people in other jurisdictions. However, because of the interconnected nature of the Real ID system, a breach in one location would have national ramifications.

One method of accessing a system by taking advantage of the human element is through bribery. In 2000, a drug runner bribed a U.S. Customs official to access two government databases on his behalf.[83] The Customs official searched both the DHS's Treasury Enforcement Communications System database and the FBI's National Crime Information Center database and passed information back to the drug runner.[84]

One could also con an authorized user into giving an attacker access to the system. A 2003 study in London found that 90% of office workers would trade their computer passwords for a cheap pen.[85] Under another method of social engineering called "pretexting," the attacker could persuade the victim to provide the attacker with information or access to the

---

[80] *See* American Association of Motor Vehicle Administrators, Commercial Driver's License Information System (CDLIS), http://www.aamva.org/TechServices/AppServ/CDLIS/ (last visited Apr. 9, 2009); FEDERAL HIGHWAY ADMINISTRATION, HIGHWAY STATISTICS 2006: SECTION III: DRIVER LICENSING: LICENSED DRIVERS–RATIO OF LICENSED DRIVERS TO POPULATION (2006), *available at* http://www.fhwa.dot.gov/policy/ohim/hs06/driver_licensing.htm.

[81] HOUSE COMM. ON OVERSIGHT AND GOV'T REFORM, SEVENTH REPORT CARD ON COMPUTER SECURITY AT FEDERAL DEPARTMENTS AND AGENCIES 2-3 (Comm. Print 2007), *available at* http://republicans.oversight.house.gov/Media/PDFs/FY06FISMA.pdf.

[82] HOUSE COMM. ON OVERSIGHT AND GOV'T REFORM, SEVENTH REPORT CARD ON COMPUTER SECURITY AT FEDERAL DEPARTMENTS AND AGENCIES 2 (Comm. Print 2008), *available at* http://republicans.oversight.house.gov/media/PDFs/Reports/FY2007FISMAReportCard.pdf.

[83] Jon Stokes, *Analysis: Metcalfe's Law + Real ID = More Crime, Less Safety,* ARS TECHNICA, Jan. 19, 2008, http://arstechnica.com/news.ars/post/20080119-analysis-metcalfes-law-real-id-more-crime-less-safety.html.

[84] *Id.*

[85] John Leyden, *Office Workers Give Away Passwords for a Cheap Pen*, THE REGISTER, Apr. 18, 2003, http://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/.

system.[86] A prime example of pretexting is when an attacker impersonates an information technology department employee and requests a user's password or access to a computer to perform "routine maintenance."[87]

Additionally, the database creates a risk of unintentional dissemination. In 2006, a subcontractor for Veterans Affairs (VA) took home a laptop computer, which was subsequently stolen from his house.[88] The computer contained information on 26.5 million veterans, including their names, dates of birth, and SSNs.[89] The potential for similar dissemination exists with respect to DMV information. A physical breach at a North Carolina DMV resulted in the theft of several computers and workstations containing DMV records on 16,000 drivers.[90]

The final regulations require each DMV to submit a security plan, but provide no strong foundation for protecting people from unauthorized access to their personal information or from human failings.

### *D. Neither the REAL ID Act nor the Final Rule Adequately Protects Against Mission Creep*

Another privacy concern that the REAL ID Act and DHS final rule fail to protect against is mission creep. Mission creep is the expansion of a program's scope beyond its original purpose. The extensive reliance on SSNs as a unique identifier is a salient example of mission creep. In 1936, the SSA began to assign each eligible worker an SSN that represented the individual's unique Social Security benefits account.[91] For nearly 50 years, the card SSA issued to Social Security participants specifically stated that the SSN was "not for identification."[92] Despite the very limited original purpose of SSNs, its use has grown dramatically since its inception. Federal, state, and local agencies rely on SSNs to identify recipients of a variety of benefit programs.[93] Credit reporting agencies, healthcare organizations, banks, schools, and hospitals frequently use the SSN as an identifier.[94] Thus, the "mission" of the SSN has "crept" from its original purpose as a Social Security benefit account number to a public and private sector tool for identification.

---

[86] FTC, Pretexting: Your Personal Information Revealed (Feb. 2006)), http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre10.pdf.

[87] *See* Michael Kaplan, *Three Blind Phreaks*, WIRED, Feb. 2004, *available at* http://www.wired.com/wired/archive/12.02/phreaks.html.

[88] USA.gov, Latest Information on Veterans Affairs Data Security, http://www.usa.gov/veteransinfo.shtml (last visited Apr. 9, 2009); Ellen Ullman, *Identity Stolen? Take a Number,* N.Y. TIMES, July 17, 2006, at A17.

[89] Bob Sullivan, All Veterans at Risk of ID Theft After Data Heist, MSNBC, May 22, 2006, http://www.msnbc.msn.com/id/12916803.

[90] Thomasi McDonald, *Computer, Data Stolen from DMV*, THE NEWS & OBSERVER (Raleigh), Sept. 28, 2006, at B1.

[91] *See* SOLOVE, *supra* note 35, at 115.

[92] *Id.*

[93] *See* Kouri, *supra* note 7.

[94] *See id.*; SOLOVE, *supra* note 35, at 116.

DHS has already considered several expanded uses of REAL ID cards. For example, Stewart Baker, Assistant Secretary for Policy at DHS, commented that pharmacies could require customers to show REAL ID cards to purchase over-the-counter medicine.[95] Baker suggested that requiring a "strong ID," such as a REAL ID, would reduce production of methamphetamine.[96]

## IV. Policy Recommendations

Both the REAL ID Act and DHS final rule fail to sufficiently defend the privacy of individual cardholders. The government creates a national ID card, a national identification number, and a national database without ensuring that cardholder information is secure. Further, the regulations do not strictly limit who may use the information or for what purpose. A combination of technological and legislative solutions can alleviate many of the privacy concerns created by REAL IDs.

### *A. Technological Solutions to REAL ID Privacy Concerns*

To reduce the national database's susceptibility to hacking, the system should be isolated from the Internet and should use secure encryption methods. No network or encryption method is completely invulnerable to attack, but if the government upgrades the system as these technologies improve, it will significantly limit hackers' ability to penetrate the database.

To avoid the vulnerability of an unencrypted barcode, the government should create a new 2D barcode standard specifically for REAL IDs. Although this would not solve the problems associated with a nationwide standard, the use of a proprietary barcode, along with proprietary scanning and decoding technology, would reduce the ability of unauthorized users to access barcode data.

Alternatively, the government could protect the barcode data by requiring encryption. Strong encryption would permit only those entities with an encryption key to unlock the data on the card. Encryption would have the additional benefit of allowing different levels of access. For example, one encryption key (appropriate for liquor and tobacco retailers) could allow a swipe only to reveal the cardholder's date of birth. A different encryption key could allow retailers to match the cardholder's name with the name on the credit card. A third encryption key could allow airport security and police full access to all of the information on the card. Such a system would allow access to necessary information without sacrificing the privacy of the cardholder.

---

[95] Posting of Greg Burnett to PolicyBeta, *REAL ID for Sudafed? Call it 'Mission Creep,'* http://blog.cdt.org/2008/02/04/real-id-for-sudafed-call-it-mission-creep/ (Feb. 4, 2008, 9:19 am).

[96] *Id.*

### *B. Legislative Solutions to REAL ID Privacy Concerns*

A simple way to reduce the likelihood of mission creep by the government is to amend Section 201(3) of the REAL ID Act to eliminate the ability of the Secretary of DHS to expand the "official purposes" of the REAL ID card.[97] Congress could still expand the "official purposes" of REAL IDs through legislation. Eliminating the DHS Secretary's ability to enlarge the scope of the REAL IDs would have the additional benefit of legitimizing any potential mission creep as the act of the democratically elected Congress rather than the unilateral decision of an unelected executive officer.

The government should also be held accountable, under a doctrine of sovereign liability, for potential harms resulting from the loss of privacy facing REAL ID cardholders. To subject a sovereign power to liability, Congress must first pass a law creating a cause of action.[98] An amendment to Section (g) of the Privacy Act of 1974, which prescribes civil remedies for privacy violations, is the most straightforward means to create sovereign liability.[99]

Congress should recommend a strict liability standard for database breaches and a negligence standard for data breaches relating to the physical REAL ID card. Holding the government strictly liable for unauthorized access to the national network of DMV databases accords with contemporary tort theory[100] and correctly places the burden of ensuring the security of citizens' personal data on the government. Liability would arise when harm results from someone hacking into the database, faulty database software, or personal information leaks due to bribery or unintentional dissemination. Because a single hacking attempt could result in the theft of millions of citizens' personal information, strict liability would compel the government to use the most secure technology available or face tens of millions of dollars in damages for each database breach.

A less stringent negligence standard is appropriate for privacy invasions resulting from the inadequate protection of information stored on the REAL ID card itself. In this cause of action, the duty of the government is to protect the privacy and security of its citizens through the use of secure technologies. The government breaches that duty by using insecure technologies. For example, if a gas station attendant bought a $120 barcode scanner and stole the identity of a patron by scanning her REAL ID card, the negligence standard would impose liability on the government because the unencrypted 2D barcode is a proximate cause of the patron's harm.

---

[97] *See supra* note 18.

[98] Block v. N. Dakota *ex rel.* Bd. of Univ. & Sch. Lands, 461 U.S. 273, 280 (1983) (stating that "all . . . entities are barred by federal sovereign immunity from suing the United States in the absence of an express waiver of this immunity by Congress") (citations omitted).

[99] 5 U.S.C. § 552a(g)(1) (2007).

[100] *See* Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public And Private Law At The Dawn of The Information Age*, 80 S. CAL. L. REV. 283-294 (2007) (finding support for imposing strict liability on database operators and information brokers in various theories of tort law, including instrumentalism, justice theories and formalism).

The strongest argument against sovereign liability is the potential cost to the government of the resulting litigation. However, this is also the reason sovereign liability is the best mechanism for effective change. Imposing a negligence standard for information stolen directly from the REAL ID card permits the government to decide whether the cost of requiring that the cards carry the most secure technology outweighs the cost of litigation from the use of less secure methods. Unlike the database, where strict liability is preferable because of the immense aggregate harm of a single attack, wrongdoers who steal information from a physical REAL ID card can access the private information of only one individual. Thus, sovereign liability ensures that the government appropriately considers both the cost of implementing more secure technologies and the potential losses to individual cardholders in deciding what level of security would be cost-effective.

## V. Conclusion

A combination of technological and legislative solutions can cure many of the infirmities that plague the REAL ID Act and corresponding DHS regulations. An interconnected database that uses secure encryption and that is walled off from the Internet would minimize the risk of a successful hack. A proprietary barcode would limit the ability of nongovernmental organizations to access REAL ID card data. Amending the Act to remove the DHS Secretary's ability to expand the scope of REAL IDs would reduce the likelihood of mission creep. The imposition of strict liability for database-related violations would provide citizens a cause of action for harm beyond their control. A negligence-based cause of action for violations relating to the physical REAL ID card would provide cardholders with a civil remedy when the government uses insecure methods and would permit flexibility with regard to how the government protects the information contained on the card. Together, these solutions would further the government's counterterrorism goals while ensuring the privacy of cardholders' personal information.