State Government Information Collection: The Shutdown of the MATRIX Program, REAL ID, and DNA Collection

KATIE STENMAN*

ABSTRACT

This article discusses the mechanisms utilized by state governments to collect, record, and distribute personal information gathered on citizens. States are constantly increasing the amount of personal information collected and formulating new ways to utilize that information. During this past year, the Multistate Anti-Terrorism Information Exchange program data collection pilot program reached the end of three years of federal funding. Even with the end of the Multistate Anti-Terrorism Information Exchange program, states are still seeking to increase the distribution of information previously available through the program and make the information available to all state governments. The federal government now seeks to utilize the states to collect even more information. Congress passed the REAL ID Act of 2005, which will require significant effort on the part of states to comply. Finally, both state governments and the federal government are implementing new and farther-reaching DNA collection laws. An increasing amount of the information collected by state agencies is available for distribution on both a state and federal scale. The collection and distribution of this information raises privacy concerns as an ever-increasing amount of personal information is stored in centralized databases, and access is available to government officials.

INTRODUCTION

The states collect personal information in a myriad of ways, some of which are similar to, or duplicative of, the federal government. States often face complications that are not applicable to the federal government when collecting information and attempting to share the information on a national scale. Federal privacy law is governed primarily by the Privacy Act of 1974.[1] However, states have individual laws that may vary vastly in terms of what constitutes

*The author is a J.D. candidate at The Ohio State University Moritz College of Law, class of 2007. She holds a bachelor's degree in political science from Indiana University of Pennsylvania and a master's degree in political science from The State University of New York at Stony Brook.

[1] Privacy Act of 1974, 5 U.S.C. § 552a (2005).

protected information. Ten state constitutions explicitly recognize a right to privacy,[2] and many states have additional laws protecting various types of privacy.[3] Privacy interests receiving statutory protection include Internet, health, education, identity, and financial privacy. State laws protect these different types of privacy to varying degrees.[4]

The discrepancy in privacy laws among the states and the federal government played a key roll in the shutdown of the Multistate Anti-Terrorism Information Exchange ("MATRIX") program. The MATRIX program, which allowed participating states to collect information and store it in a sharable database, concluded when federal funding expired in 2005. The REAL ID Act of 2005, passed as part of the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005,[5] will place additional constraints on the way states collect, share, and store personal data. The portion of the REAL ID Act that will have the greatest impact on the states promulgates rules states must follow in issuing drivers' licenses and identification cards. States and the federal government are also working to collect a different type of information, DNA, by compiling databases of DNA profiles of persons arrested or charged with criminal activity, with an increasing emphasis on obtaining DNA samples of criminal arrestees before conviction. The collection of various types of information creates unique concerns about personal privacy as an ever-increasing amount of personal information is stored in databases, both state and federally maintained.

This article focuses on the challenges that states and the federal government face in the collection and storage of information. It also examines the MATRIX program shutdown and future alternatives to state data-mining and sharing. Exploring differing perspectives on the REAL ID Act of 2005 and the creation of the centralized databases

---

[2] National Conference of State Legislatures, *Privacy Protections in State Constitutions*, http://www.ncsl.org/programs/lis/privacy/stateconstpriv03.htm (gives an overview of State constitutional privacy protections).

[3] *Id.*

[4] NATIONAL CONFERENCE OF STATE LEGISLATURES, PRIVACY, http://www.ncsl.org/programs/lis/cip/priv/privacy.htm (last visited Nov. 19, 2005) (discusses the various statutory state privacy protections).

[5] H.R. 1268, 109th Cong. (2005) (enacted).

required by the REAL ID Act, this article also addresses the cost of implementing the new mandates of the REAL ID Act that the states will absorb. The new DNA collection laws balance a need to stop and detect criminal activity nationwide with the personal privacy interests that persons who are not yet convicted of any offense have in their DNA.

I. MULTISTATE ANTI-TERRORISM INFORMATION EXCHANGE PROGRAM

The MATRIX ("Multistate Anti-Terrorism Information Exchange") program, which lost funding in April 2005, was a federally funded program that allowed State governments to access a combination of private and government-held[6] personal information.[7] The MATRIX program was similar to the federal Total Information Awareness ("TIA") program, which also was capable of aggregating and analyzing large amounts of data from different sources.[8] The MATRIX program used the Factual Analysis Criminal Threat Solution ("FACTS") to search available resources and to gather information.[9] Information included:

- drivers' license records;[10]

---

[6] Privately held information includes information such as credit reports, and consumer information. Government information includes drivers' license records, criminal records, domestic records, and all other public records typically held by the States.

[7] Press Release, American Civil Liberties Union, What is the Matrix? ACLU Seeks Answers on New State Run Surveillance Program (Oct. 30, 2003), http://www.aclu.org/privacy/spying/15722prs20031030.html.

[8] Sayaka Kawakami & Sarah C. McCarty, *Privacy Year in Review: Privacy Impact Assessments, Airline Passenger Pre-Screening, and Government Data Mining*, 1ISJLP 219, 250-251 (2005).

[9] Press Release, Florida Department of Law Enforcement, MATRIX Pilot Project Concludes (Apr. 15, 2005), *available at* http://www.fdle.state.fl.us/press_releases/expired/2005/20050415_matrix_project.html.

[10] *Facilitating an Enhanced Information Sharing Network that Links Law Enforcement and Homeland Security for Federal, State, and Local Governments: Hearing on Homeland Security Information Sharing Before the H. Comm. on Government Reform: Technology, Info. Policy, Intergovernmental Relations, and the Census Subcomm.*, 108th Cong. 78 (2004) (statement of Mark Zadra, Member Florida Department of Law Enforcement), *available at* http://www.mipt.org/pdf/House108-254.pdf.

- digital images;[11]
- criminal histories;[12]
- data from the Department of Corrections as well as any sexual offender history;[13] and
- commercially available public data, such as telephone numbers, property ownership, and any other publicly available commercial information. [14]

The information contained in FACTS was already available to local law enforcement through other sources but was not shared beyond state databases.[15] The FACTS technology only provided a common point of access that allowed law enforcement to search the data in the same way that one would conduct an Internet query search.[16]

The MATRIX program received a total of $12 million in federal funding from the Department of Homeland Security and the Department of Justice.[17] Additional information on the MATRIX pilot program was previously available online. However, now that the program has concluded, the administrators removed the information, but questions may still be addressed through an e-mail address provided on the web site.[18]

---

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Id* at 80.

[16] *Id.*

[17] WILLIAM J. KROUSE, CRS REPORT FOR CONGRESS: THE MULTI-STATE ANTI-TERRORISM INFORMATION EXCHANGE (MATRIX) PILOT PROJECT (2004), *available at* http://www.fas.org/irp/crs/RL32536.pdf.

[18]Multistate Anti-Terrorism Information Exchange, http://www.matrix-at.org (last visited Sept. 15, 2006) (website discontinued, but e-mail address is provided for questions).

A. END OF THE MATRIX PILOT PROGRAM

When the pilot MATRIX program officially concluded on April 15, 2005, the federal funding for the program had expired. Multiple concerns led to the end of the program including: the unavailability of additional federal funding, differing state privacy laws, and a lack of state participation. When the program began, fifteen states were committed to the program, but as the pilot program progressed, states began to withdraw their support.[19] When federal funding ended, only four states still utilized the program: Connecticut, Florida, Ohio, and Pennsylvania.[20]

The MATRIX program was designed to facilitate information exchange among the states, but did not account for the differences in state privacy laws.[21] The database also drew stiff criticism when it provided "government officials the names of 120,000 people whose personal information supposedly fit the profile of a terrorist."[22] Many law enforcement officials support the MATRIX program as an important tool and argue that the use of the FACTS technology, as aggregated by the MATRIX program, has led to many arrests.[23] Florida and Ohio, still find that the program has value to law enforcement and plan to continue to utilize the information through the FACTS technology, but not under the heading of the MATRIX program.[24]

---

[19] Kawakami & McCarty, *supra* note 8, at 265.

[20] Jon Craig, *ACLU Presses State Not to Use Database, Citing Privacy Issues; Officials say FACTS, MATRIX Programs Help Catch Criminals*, THE COLUMBUS DISPATCH, Apr. 22, 2005, at 05C.

[21] Nicholas Hoover & Eric Chabrow, *Homeland Security –How Far Have We Come?*, INFORMATION WEEK, Sept. 5, 2005, *available at* http://www.informationweek.com/story/showArticle.jhtml?articleID=170700240&tid=5979.

[22] Jeffrey Goldfarb, *Consumer Data Stolen from Reed Elsevier*, March 9, 2005, *available at* http://www.insurancebroadcasting.com/031005-32.htm.

[23] Craig, *supra* note 20.

[24] *Id.*

B. FUTURE OF THE MATRIX PROGRAM

The information that was available through the MATRIX program is still available through Seisint, owned by LexisNexis, although sharing capability among the states has ended.[25] Ohio will use $259,000, annually, in federal Homeland Security funds to continue the program statewide.[26] Florida, where the MATRIX program originated, also continues to use the programs statewide through use of the FACTS technology.[27] In a continuing effort to create a program similar to MATRIX and to make that technology available to the states, on April 12, 2005, the Florida Department of Law Enforcement put out a call for vendors to operate a program similar to the MATRIX program, with the intention of again making it available to the states.[28]

C. OPPONENTS OF THE MATRIX PROGRAM AND CONTINUATION

The American Civil Liberties Union ("ACLU") has raised privacy concerns about the continuation of the program as more than 300,000 people had their information stolen from LexisNexis in 2005.[29] Seisint has also experienced some large data breaches in the past; names, addresses, social security numbers, and drivers' license numbers of approximately 32,000 people were exposed by hackers.[30] The ACLU also cites general concerns with the use of data-mining technology[31] and contends that a significant amount of the information the MATRIX program made available to law enforcement was not

---

[25] *Id.*

[26] *Id.*

[27] Matt Galnor, *FDLE Wants to Cast a Wider Net; Privacy Advocates Concerned, But Police Laud System's Ability to Consolidate Data,* THE FLORIDA TIMES-UNION, May 5, 2005, at A-1.

[28] FLORIDA DEPARTMENT OF LAW ENFORCEMENT, REQUEST FOR INFORMATION: INFORMATION SERVICES TO SUPPORT DOMESTIC SECURITY AND CRIMINAL INVESTIGATIONS 2 (2005), *available at* http://fcn.state.fl.us/owa_vbspdf/owa/46616_RFI0003_0_0.pdf.

[29] Goldfarb, *supra* note 22.

[30] *Id.*

[31] ACLU, Matrix: Myths and Reality (Feb. 10, 2004), http://www.aclu.org/privacy/spying/14999res20040210.html.

previously available.[32] Further, there is no guarantee regarding the accuracy of the information that was contained in the MATRIX program.[33] Concerns about inaccuracy would continue with any revival of the program or use of similar technologies.

D. PROPONENTS OF THE USE OF THE FACTS SYSTEM

Defenders of the FACTS technology, which Ohio and Florida will continue to utilize, advocate its use on several grounds:

- FACTS is not a substitute for the TIA Project but is instead a query/response based system to be used only by trained law enforcement officers,[34]
- FACTS does not contain intelligence information but rather contains only information that is already available to law enforcement officials,[35] and
- FACTS does not perform data-mining operations, but only gathers data that is already in possession of law enforcement.[36]

II. REAL ID

The REAL ID Act of 2005,[37] passed as part of 109 H.R. 1268,[38] was signed into law on May 11, 2005. The REAL ID Act contains several important new provisions. In Title I, Amendments to Federal Laws to Protect Against Terrorist Entry, the Act strengthens the

---

[32] *Id.*

[33] *Id.*

[34] *Facilitating an Enhanced Information Sharing Network that Links Law Enforcement and Homeland Security for Federal, State, and Local Governments, supra* note 10, at 71-72.

[35] *Id.* at 72.

[36] *Id.*

[37] REAL ID Act of 2005, Pub. L. No. 109-13, 119 Stat. 231, 301-311 (2005).

[38] H.R. 1268, 109th Cong. (2005).

provisions that govern when an immigrant may not be admitted into the country because of an association with terrorist activity.[39] Additionally, the Act modifies the review process for orders of removal from the country.[40] Title II, Improved Security for Drivers' Licenses and Personal Identification Cards, creates minimum standards for identification cards and drivers' licenses.[41] Identification that meets the specifications of the Act will be necessary if a federal agency is requiring proof of identification in order for the agency to accept it as valid.[42] There are also additional requirements that must be satisfied for issuance of identification to persons who have not attained citizenship.[43] Persons who are only temporarily in the country are only eligible for a license or identification card that will expire when their residency in the country expires.[44] The Act, additionally, strengthens federal jurisdiction with respect to border regulation in Title III, Border Infrastructure and Technology Integration.[45] Title III increases federal control over border security and creates a pilot program that will result in greater border surveillance.[46] Finally, the Act places additional controls over immigrant workers and immigrant worker status, and changes certain visa provisions for persons from Australia and nurses.[47]

A. DRIVERS' LICENSE AND IDENTIFICATION CARD REQUIREMENTS

Title II of the REAL ID Act of 2005 creates a new set of requirements for drivers' licenses and identification cards in order for

---

[39] REAL ID Act of 2005, Pub. L. No. 109-13, § 103, 119 Stat. 231, 301-311 (2005).

[40] *Id.* at § 101, 119 Stat. at 301-307.

[41] *Id.* at § 202, 119 Stat. at 312-314.

[42] *Id.* at § 202, 119 Stat. at 312.

[43] *Id.* at § 202, 119 Stat. at 313.

[44] *Id.*

[45] *Id.* at § 301-303, 119 Stat. at 316-318.

[46] *Id.*

[47] *Id.* at § 401-407, § 501-502, 119 Stat. at 318-323 (modifies laws governing temporary workers and immigrant visas).

the identification to be accepted as valid by the federal government. Starting in 2008, a federal agency will not accept a state issued drivers' license or identification card that does not meet the minimum-security requirements of the Act.[48] An acceptable identification must contain the following information.

- Full legal name;
- date of birth;
- gender;
- a card identification number;
- a digital photograph of the person;
- the address of principal place of residence;
- signature;
- a physical security feature designed to prevent duplication, tampering, and counterfeiting for any fraudulent purposes; and
- "[a] common machine-readable technology with defined minimum data elements."[49]

The Act also requires that the states only issue a personal identification card or drivers' license with proper documentation of the required information. The following information must be verified with the issuing agency for validity, and completeness.

- Name and birth date - verifiable through a photo identity document, with a non-photo identity document accepted only if it contains both a full

---

[48] *Id.* at § 202, 119 Stat. at 312-313.

[49] *Id.*

legal name and birth date, such as a birth certificate.[50]

- Proof of social security number or verification that the person is not eligible for a social security number:
    - states are also required to check social security account numbers with the Social Security Administration and resolve any conflicts, and
    - should another license have been issued under the same social security number by that state or another state, it is the responsibility of the state issuing the license to resolve the discrepancy and take appropriate action.[51]
- Documentation showing the person's name and principal residence, and proof of lawful status, which can be proven through several types of documentation:
    - valid documentary evidence that the person is a citizen; or
    - documentation that the person is a lawful temporary or permanent resident, conditional permanent resident, has approved asylum, has a valid nonimmigrant visa, has a pending asylum application, approved deferred action status, or proof of a pending application for adjustment.[52]

---

[50] *Id.* at § 202, 119 Stat. at 313.

[51] *Id.*

[52] *Id.*

These rules also extend to temporary licenses and identification cards. Digital images of the documentation utilized to obtain a drivers' license or identification card will be retained in electronic storage pursuant to storage requirements promulgated by the federal government.[53] States are also required to maintain databases containing all drivers' license and identification card information as well as motor vehicle histories and make that information available to other states.[54] The original rationale behind strengthening federal provisions regulating drivers' licenses was in response to the terrorist attacks of Sept. 11, 2001.[55] The stated rationale for increased security measures for the issuance of drivers' licenses and identification cards is to decrease the ease of obtaining fraudulent identification, through the use of forged or inauthentic documents.[56]

B. IMPLICATIONS FOR THE STATES

Some states' rights advocates have argued that the REAL ID Act is beyond the appropriate reach of the federal government because it is an unfunded mandate requiring extensive effort of the states without guaranteeing federal funding.[57] The Act places a significant burden on the states to bring their systems of issuing drivers' licenses and identification cards up to federal standards by May 11, 2008.[58] The Act contains a provision for the appropriation of federal funds to assist the states, but there is no specific grant to each state, only a provision

---

[53] *Id.* at 119 Stat. 314 (Paper copies are to be retained for seven years and electronic copies for ten years).

[54] *Id.* at 119 Stat. 315.

[55] DEMOCRATIC STAFF OF H. COMM. ON THE JUDICIARY, 109TH CONG., REPORT ON THREE STRIKES AGAINST THE SO-CALLED REAL ID ACT (H.R. 418): BAD FOR NATIONAL SECURITY, BAD FOR CIVIL LIBERTIES, BAD FOR VICTIMS OF PERSECUTION 18 (2005), *available at* http://www.house.gov/judiciary_democrats/hr418debate109cong/demhr418views2905.pdf (the REAL ID Act was previously contained in a separate bill before it was passed as part of H.R. 1268).

[56] *Id.*

[57] NATIONAL CONFERENCE OF STATE LEGISLATURES, PREEMPTION MONITOR (2005), http://www.ncsl.org/standcomm/sclaw/preemption0805.htm.

[58] REAL ID Act of 2005, § 202, 119 Stat. 312.

that the secretary "may make grants."[59] Furthermore, states receive funding only if they join the inter-state compact to make information available to all other states.[60]

The current administration claims that it will cost the states about $100 million over five years to comply with the mandates of the REAL ID Act. However, the National Conference of State Legislatures estimates that figure at somewhere between $9-13 billion.[61] According to some estimates, it would cost $85 million to bring Pennsylvania alone up to compliance with the Act.[62] States' rights advocates estimate that these regulations will force State Department of Motor Vehicle employees to spend a significant amount of time verifying sources and exchanging information with various other public agencies.[63] Some advocates speculate that all drivers' licenses will have to be reissued to comply with the Act.[64] The rationale behind this speculation is that even if the information contained on the license or identification card is correct and properly verified at issuance, it is likely that the documents used to obtain the identification were not properly verified, nor were they digitally recorded in the format necessary to be included in the federal database.[65]

California, in a budget signed into law on June 30, 2006, appropriated $18.8 million and allocated 36 positions to help the state comply with the Act.[66] A major concern in California is the possibility of chaos at the Department of Motor Vehicles ("DMV").

---

[59] *Id.* at § 204, 119 Stat. 315.

[60] *Id.*

[61] NATIONAL CONFERENCE OF STATE LEGISLATURE, *supra* note 57.

[62] Electronic Privacy Information Center, National ID Cards and REAL ID Act (2006), http://www.epic.org/privacy/id_cards/.

[63] Rich Ehisen, *SNCJ Spotlight: What Will REAL ID Really Cost?*, ST. NET CAPITOL J, Sept. 5, 2005, http://www.statenet.com/capitol_journal/09-05-2005.

[64] *Id.*

[65] Declan McCullagh, *FAQ: How Real ID will Affect You,* CNET NEWS.COM, May 6, 2005, http://news.com.com/FAQ+How+Real+ID+will+affect+you/2100-1028_3-5697111.html.

[66] Lynda Gledhill, *Long Waits Looming for License Renewals; DMV Officials Fear New Federal ID Rules Will Lengthen Lines,* THE SAN FRANCISCO CHRONICLE, July 24, 2006, at A1.

With DMV facilities already crowded by just maintaining normal business, there is concern that complying with the REAL ID Act will create even larger delays.[67] Virginia's REAL ID Task Force estimates the cost of implementation in Virginia at somewhere between $33 and $169 million.[68] The Governor of Virginia has proposed an additional fee on drivers' license renewal to help cover the cost of the program.[69]

California and other states are still waiting on rules, expected by the end of 2006, issued by the federal government, explaining how the states are to comply with the provisions of the REAL ID Act.[70] States wishing to begin compliance are at a standstill, waiting for federal regulations more than a year after the passage of the Act.[71] Because of the delay in the issuance of federal rules, the National Governor's Association is requesting that the compliance deadline be pushed back from the original May 2008 deadline.[72]

While states are free to reject the requirements of REAL ID, there is speculation that some businesses may require a REAL ID compliant identification to complete transactions, and it will be necessary for both national and international travel. New Hampshire has tried to reject the requirements of the Act.[73] The New Hampshire legislature has debated several bills that would keep the state from participating in the REAL ID program.[74] Further complicating the ban, New Hampshire has been chosen as one of two states that would run a pilot program for REAL ID, obtaining a $3 million federal grant, although privacy advocates in the New Hampshire legislature oppose taking the funding.[75] Additionally, it is possible that by failing to comply with

---

[67] *Id.*

[68] Tim McGlone, *Lack of Information Stymies ID Plans*, THE VIRGINIAN-PILOT, July 15, 2006, at B1.

[69] *Id.*

[70] Gledhill, *supra* note 66.

[71] McGlone, *supra* note 68.

[72] *Id.*

[73] Tom Fahey, *Efforts to Kill REAL ID Program Fall Short*, THE UNION LEADER, May 12, 2006, at A8.

[74] *Id.*

[75] *Id.*

the requirements of the REAL ID Act, states will limit their residents' abilities to interact with the federal government.

C. PROPONENTS OF THE REAL ID ACT

Proponents of the REAL ID Act focus on terrorism prevention as the almost sole justification for the new drivers' license and identification card requirements. House Judiciary Committee Chair James Sensenbrenner stated

> [t]he goal of the REAL ID Act is straightforward: it seeks to prevent another 9/11-type attack by disrupting terrorist travel . . . American citizens have the right to know who is in their country, that people are who they say they are, and that the name on a driver's license is the holder's real name, not some alias.[76]

By creating uniform requirements for the issuance of visas to non-residents, proponents of the REAL ID Act hope the Act will lead to better monitoring of foreign visitors. Representative Sensenbrenner cites to the case of terrorist Mohammed Atta who received a six-month visa to stay in the United States yet received a Florida driver's license good for six years.[77]

Proponents also argue that these strict requirements for the issuance of a driver's licenses will deter terrorist activity on their face.[78] Drafters intend the recording of the documentation used to obtain identification to deter the use of fraudulent documentation, in hope that the requirements will deter people who would potentially obtain fraudulent identification by virtue of the requirements of the new law alone.[79]

---

[76] Press Release, United States House of Representatives Committee on the Judiciary, Sensenbrenner Introduces Terrorist Travel Legislation: REAL ID Act Contains Provisions Dropped from 9/11 Legislation (Jan. 26, 2005), *available at* http://judiciary.house.gov/newscenter.aspx?A=430.

[77] *Id.*

[78] *See id.*

[79] *See id.*

D. PRIVACY IMPACT AND CONCERNS ABOUT THE REAL ID ACT

Numerous opponents of the identification provisions of the REAL ID Act exist. One of their main concerns is that the requirements of the REAL ID Act will do nothing to deter or limit terrorist activity but will be burdensome for states and residents.[80] Encompassed in this concern is the increased incentive to create fraudulent documentation to obtain an identification card or drivers' license. Employees in state DMVs will not possess sufficient training to recognize these fraudulent documents, enabling fraudulent licenses to be obtained regardless of these additional protections.[81] Also, there are privacy concerns about making the information available nationally so the states can perform the proper documentation verification.[82] It is questionable how distribution of the necessary verification information will operate and how many state resources will be consumed to create the database.[83] Given the requirements of the Act and the exposure to sensitive information, state employees who have access to this personal information will be subject to background checks, which could result in staffing shortages.[84] There may also be further conflicts with state laws and exceptions, as some states have special provisions that allow the issuance of drivers' licenses without a photo, often because people object to the photograph for religious reasons.[85]

Much of the additional concern surrounding the REAL ID Act focuses on the new requirement that data sharing among the states occur. Sharing and integrating the information may require the use of a data broker.[86] "[P]rivacy advocates and opponents of the 'REAL ID'

---

[80] DEMOCRATIC STAFF OF H. COMM. ON THE JUDICIARY, *supra* note 55, at 18.

[81] *Id.* at 20.

[82] Brian Bergstein, *Frustration Over Driver's License Law: Anti-Terrorism Law Requiring Standardized ID Called A "Nightmare,"* CBS NEWS, Jan. 12, 2006, http://www.cbsnews.com/stories/2006/01/12/tech/main1206578.shtml.

[83] *Id.*

[84] *Id.*

[85] *Id.*

[86] Martin H. Bosworth, *TSA's Privacy Law Violations May Lead to More Abuses*, CONSUMERAFFAIRS.COM, July 28, 2005, http://www.consumeraffairs.com/news04/2005/tsa_privacy.html (a data broker would most likely be a private company responsible for integrating and making the required information and documentation available to all the states).

Act believe that entrusting such a complex enterprise to companies that have already proven incapable of protecting the data they collect may lead to even more instances of identity theft."[87] Further, with the storage of digital images of personal records, there are additional concerns about the capability of reproducing that documentation and using it to obtain fraudulent identification. The ACLU worries that required state compliance with the REAL ID Act could amount to an "irretrievable loss of citizens' privacy."[88]

Federal funding will be necessary for most states to comply with the mandates of the Act. To be eligible for funding, states will be required to add information about their residents to the national database and accept the risks inherent in the centralization of this personal information. With so much personal information digitally recorded and stored in a single database, there will be significant potential for identity theft.

III. DNA COLLECTION

All fifty states have some mechanism for collecting DNA from certain classes of convicted offenders.[89] The federal government also has similar provisions.[90] However, as DNA collection increases and sharing and storage of this information moves from a local scale to a national scale, privacy concerns arise about the safety of the information.[91] Further, the United States Supreme Court never fully examined a number of provisions for DNA collection from felons. Privacy advocates question the propriety of maintaining a database of such personal information. These DNA databases are also widely accessible to employees of various law enforcement agencies.[92] As the collection of DNA information expands to include persons who

---

[87] *Id.*

[88] Ehisen, *supra* note 63.

[89] Martha L. Lawson, Note, *Personal Does Not Always Equal "Private": The Constitutionality of Requiring DNA Samples from Convicted Felons and Arrestees*, 9 WM. & MARY BILL RTS. J. 645, 650 (2001).

[90] *Id.*

[91] *Id.*

[92] *Id.*

were arrested, but not convicted,[93] concerns about privacy in identification through DNA increases.

A. RECENT COURT DECISIONS ON DNA COLLECTION

1. SUPREME COURT DECISIONS

Recently, the United States Supreme Court denied certiorari to hear whether the collection of DNA from incarcerated felons is constitutional.[94] The Court has also denied certiorari to consider whether collection is proper from parolees.[95] The Georgia statute questioned in *Padgett v. Donald*[96] mandates the collection of DNA samples from all incarcerated felons for analysis and storage in a database maintained by the Georgia Bureau of Corrections. DNA samples can be collected through various means but most often is obtained through scraping the inside of the cheek with a swab. The DNA profiles of these persons are available for release to "federal, state, and local law enforcement officers upon a request made in furtherance of an official investigation of any criminal offense."[97] In the lower court, the United States Court of Appeals for the Eleventh Circuit, the Appellants, incarcerated felons in the Georgia Department of Corrections, argued that this statute violated their constitutional rights because it amounted to an unreasonable search and seizure, is unreasonably vague, deprived them of due process, and violated their privacy rights.[98] The Eleventh Circuit rejected these arguments.[99] The United States Supreme Court has never addressed the issue of whether a person's rights are violated by the collection, categorization, and sharing of DNA; however, with increasingly stringent DNA collection mandates on both the state and federal levels, the Court may be forced to adjudicate this issue.

---

[93] *Id.*

[94] Boulineau v. Donald, 126 S. Ct. 352 (2005).

[95] Kincade v. United States, 125 S. Ct. 1638 (2005).

[96] Padgett v. Donald, 401 F.3d 1273, 1275 (11th Cir. 2005).

[97] GA. CODE ANN. § 24-4-63 (2005) (*see also* GA. CODE ANN. § 24-4-60).

[98] Padgett, 401 F.3d at 1276 (11th Cir. 2005).

[99] *Id.* at 1282.

2. LOWER COURT CHALLENGES TO THE DNA COLLECTION LAWS

The first case that challenged the constitutionality of mandatory DNA sampling from convicted felons was *Jones v. Murray* in the United States Court of Appeals for the Fourth Circuit.[100] The court found that the government interest in preventing crime outweighed the convicted felon's limited privacy interest for two reasons:

- the state interest in deterring recidivism among felony offenders is a more important interest when balanced against the minimal intrusion that occurs from taking a DNA sample from an already convicted offender and the questionable claim of privacy in their identity after conviction, and

- the requirement that persons incarcerated before this law had taken effect give a DNA sample does not constitute a retroactive sentence.[101]

Persons are now challenging, on privacy grounds, federal law that mandates DNA collection from everyone convicted of a federal felony.[102] The DNA Backlog Elimination Act of 2000 is also challenged on grounds that there is no limit on the use of DNA nor is there any statutory mandate concerning how long DNA can be stored and utilized by law enforcement.[103] Additionally, litigants have challenged the Act's requirement that persons convicted of non-violent felonies must submit DNA samples, based on evidence that persons convicted of non-violent crimes are no more likely than the general population to be convicted of a crime.[104]

---

[100] Jones v. Murray, 962 F.2d 302 (4th Cir. 1992).

[101] *Id.* at 310-11.

[102] David Harper, *Judges Hear Arguments Challenging DNA Collection from Federal Felons,* THE TULSA WORLD, Nov. 22, 2005, at A9.

[103] *Id.*

[104] *Id.*

A Massachusetts man, Richard Frank, is going to trial in the Boston Municipal Court for refusing to give a DNA sample.[105] The sample was forcibly taken from him after he was arrested, with four corrections officers forcing him to submit, holding him down, and pricking his finger to draw blood sufficient to obtain a DNA sample.[106] Frank is the first person in Massachusetts to refuse to provide his DNA,[107] a crime punishable by Massachusetts statute.[108] This law provides that "[a]ny person required to provide a DNA sample pursuant to this chapter and who refuses to provide such DNA sample shall be subject to punishment by a fine of not more than $1,000 or imprisonment in a jail or house of correction for not more than six months or both."[109]

B. NEW FEDERAL LEGISLATION

The Senate reauthorized the Violence Against Women Act[110] on October 3, 2005, and President Bush signed it into law on January 5, 2006. This Act allows DNA samples from federal criminal arrestees to be included in the National DNA Index System ("NDIS").[111] DNA is analyzed pursuant to the Combined DNA Index System ("CODIS"), established in 1990.[112] The Federal Bureau of Investigation ("FBI") designed and now maintains CODIS.[113] CODIS is a three-tiered

---

[105] Ric Kahn, *DNA for the Taking: Convictions from His Past Left No Right to Refuse Blood Sampling*, THE BOSTON GLOBE, Aug. 14, 2005, at City Weekly 1.

[106] *Id.*

[107] *Id.*

[108] MASS. ANN. LAWS ch. 22E, § 11(LexisNexis 2005).

[109] *Id.*

[110] Violence Against Women Act Reauthorization, Pub. L. No. 109-162, 119 Stat. 2960 (2006).

[111] Press Release, Senator Jon Kyl Press Office, Senate Reauthorizes Violence Against Women Act: Includes Kyl Amendment to Remove Barriers to Maintaining Data From Criminal Arrests (Oct. 5, 2005), *available at* http://kyl.senate.gov/record.cfm?id=246925.

[112] UNITED STATES DEPARTMENT OF JUSTICE, FEDERAL BUREAU OF INVESTIGATION, THE FBI'S COMBINED DNA INDEX SYSTEM PROGRAM, *available at* http://www.fbi.gov/hq/lab/codis/brochure.pdf.

[113] *Id.*

database.[114] The highest level is the NDIS system, which enables law enforcement to share DNA information on a national level.[115] Sub-levels are both local and state databases that allow sharing information on a more limited scale.[116]

Under the proposed law, as soon as a person is charged in a pleading, the government places their information in the NDIS.[117] The database holds the person's information solely because he or she is a federal criminal arrestee. There is no requirement that he or she be a violent offender.[118] Additionally, defendants not convicted of the offense must opt out of the NDIS if they want their information removed.[119] A person may request removal by:

- sending a certified copy of the final court order stating that a conviction has been overturned to the Director of the Federal Bureau of Investigation; or

- by sending the Attorney General either a certified copy of the final court order in which a charge has been dismissed, acquitted or stating that no charge was filed within the appropriate time period.[120]

Current federal law allows states the leeway to take DNA samples on arrest and include those DNA samples in lower level – state and federal – databases. The current law does not allow uploading of DNA information into the federal NDIS database until the person is convicted.[121] Under the proposed law, information can enter the NDIS

---

[114] *Id.*

[115] *Id.*

[116] Senate Reauthorizes Violence Against Women Act, *supra* note 111.

[117] *Id.*

[118] *Id.*

[119] *Id.*

[120] *Id.*

[121] Press Release, Office of Vermont Senator Patrick Leahy, Statement of Senator Patrick Leahy, Senate Consideration of Reauthorization of Violence Against Women Act, S. 1197 (Oct. 5, 2005), *available at* http://leahy.senate.gov/press/200510/100505.html.

before bringing formal charges or even if formal charges are never brought. The arrestee bears the burden of having his information removed from the NDIS.[122]

C. STATE PROVISIONS FOR THE COLLECTION OF DNA

While all fifty states have some mechanism for DNA collection from certain offenders,[123] some states have also begun collecting DNA from persons arrested for certain crimes. Virginia became the first state to create a DNA database in 1989. In 2002, Virginia enacted a provision that allows taking a DNA sample for analysis from every person arrested for the commission or attempted commission of a violent felony.[124] The results of these DNA analyses are made directly available to all local, state, and federal law enforcement officials.[125] Louisiana has enacted a similar statute that allows for the collection of DNA from persons arrested for certain offenses.[126] Starting in 2009, in California, adults arrested for any felony offense will be required to submit to a DNA test and that information will be filed in a DNA database.[127] This California law was passed as part of Proposition 69, and privacy advocates argue that this new law will make it difficult for persons who are not subsequently convicted to have their information removed from the database.[128] The proposition requires that persons who wish to have their information removed from the database take the following three steps.

---

[122] *Id.*

[123] *Id.*

[124] Tracey Maclin, *Is Obtaining an Arrestee's DNA a Valid Special Needs Search Under the Fourth Amendment? What Should (and Will) the Supreme Court Do?*, 33 J.L. MED. & ETHICS 102, 104 (2005).

[125] *Id.*

[126] *Id.*

[127] Privacy Rights Clearinghouse, *Why the Privacy Rights Clearinghouse Opposes California Proposition 69: "DNA Samples. Collection. Database. Funding. Initiative Statute,"* Nov. 5, 2004, http://www.privacyrights.org/ar/Prop69.htm.

[128] *Id.*

- "Send a formal request to the trial court of the county in which" he or she was arrested,
- "[s]end a formal request to the DNA Laboratory of the California Department of Justice," and
- "[s]end a formal request to the prosecuting attorney of the county in which" he or she was "arrested, convicted, or adjudicated, with proof of service on all parties." [129]

Even if the arrestee follows these steps, the judge may still decide not to remove their DNA information from the database, and the decision is not appealable.[130] This type of DNA collection is troubling to privacy advocates, because DNA can be taken and added to a database without conviction and arrest requires a much lower standard of suspicion.

States collect DNA with varying frequency for a variety of offenses at varying stages of criminal prosecution. Utah[131] and Maryland[132] collect DNA from persons convicted of certain misdemeanor offenses as well as felonies. Most states that have DNA collection programs, have DNA collection provisions for misdemeanor violent crimes and misdemeanor sex crimes.[133] A minority of states collect DNA from all adults convicted of any felony, but some limit this collection to persons convicted of a violent felony, while others include juveniles in this collection process.[134] Only California,

---

[129] *Id.*

[130] *Id.*

[131] UTAH CODE ANN. § 53-10-403 (2006).

[132] MD. CODE ANN. Pub. Safety § 2-504 (2006).

[133] Seth Axelrad, Research Assistant ,The American Society of Law, Medicine and Ethics, *Survey of State DNA Database Statutes* (2004), *available at* http://www.aslme.org/dna_04/grid/guide.pdf (*see also DNA Database Statute Grid,* http://www.aslme.org/dna_04/grid/statute_grid_4_5_2006.html for same information).

[134] *Id.*

Louisiana, New York, Texas, and Virginia have mechanisms for sampling upon arrest.[135]

D. RATIONALE FOR ALLOWING DNA COLLECTION FROM ARRESTED FELONS

The rationale for collecting DNA from convicted felons is that convicted felons forfeit their privacy rights when found guilty.[136] This theory falls apart when we consider the implications of taking DNA from persons who are only arrested or charged with a crime.[137] DNA collection has also been justified as a "special needs" search under the Fourth Amendment because there is no probable cause requirement or judicial authorization required for the search.[138] The special needs doctrine allows for searches in contexts where there is no suspicion sufficient to justify getting a warrant for the search.[139] There are inconsistencies in the special needs doctrine and no clear pattern for circumstances that fit within the doctrine, which includes taking DNA samples from those convicted of crimes.[140] Experts question whether taking DNA from arrestees, rather than from persons already convicted, will fall within this exception to the warrant requirement.[141] It is likely that courts will be called upon to decide whether taking DNA samples from arrestees without a warrant is a constitutionally permissible search. As discussed above, cases are currently being litigated in state courts to determine the constitutionality of certain provisions for the collection of DNA and how these provisions balance against a person's right to privacy in his or her own DNA.

---

[135] *Id.*

[136] Editorial, *Use DNA Databases Only for Criminals*, THE ROANOKE TIMES, Oct. 2, 2005, at Horizon Editorial 2.

[137] *Id.*

[138] Maclin, *supra* note 124, at 107.

[139] *Id.*

[140] *Id.* at 115.

[141] *Id.* at 117-18.

E. PRIVACY CONCERNS IMPLICATED IN DNA COLLECTION

Privacy advocates are especially concerned about these new rules. "This clearly opens the door to all kinds of race- or ethnic-based [police] stops," according to privacy protective statements made by James Dempsey of the Center for Democracy and Technology.[142] The concern is that persons suspected of any wrongdoing or persons who police simply suspect, without more, can be stopped, arrested, and their DNA nationally compared and analyzed without sufficient suspicion that they have committed any particular crime. Additionally, pursuant to the amendment contained in the Violence Against Women Reauthorization, information will be uploaded into a national database upon arrest, as opposed to the current rule where information is not uploaded until the person is convicted.[143] A person now has to opt out of the database if he or she is not convicted, which can place a substantial burden on a person who has the misfortune of being arrested for a crime of which he or she was not convicted.[144]

Many state statutes provide penalties for improper usage of DNA information contained in databases designed only for investigatory purposes.[145] States such as Alabama, Kansas, Kentucky, Louisiana, Massachusetts, New York, South Dakota, and Vermont have laws that make tampering with DNA evidence or a DNA sample a criminal felony.[146] In some states, there is no provision at all for improper treatment of DNA samples collected from offenders.[147] States are similarly divided when it comes to protecting DNA databases from improper usage by unauthorized persons. It is a Class B or C felony in some states to improperly use the DNA database. In other states, there

---

[142] Jonathan Krim, *Bill Would Permit DNA Collection From All Those Arrested,* THE WASHINGTON POST, Sept. 24, 2005, at A03 (quoting Jim Dempsey of the Center for Democracy and Technology). *See also*, 151 CONG. REC. 128 (2005).

[143] Statement of Senator Patrick Leahy, *supra* note 121.

[144] *Id.*

[145] Axelrad, *supra* note 133.

[146] *Id.*

[147] *Id.*

is no criminal penalty for unauthorized use and access to the DNA samples and information.[148]

Researchers can use DNA databases, legally, for purposes other than criminal investigations according to certain state statutes.[149] In Alabama, researchers can use information contained in the DNA samples obtained pursuant to convictions for research about the causation, detection, or prevention of disease and disability, and the broad category of assisting human endeavors in educational or medical research if researchers remove identifying information.[150] Some additional statutes are unclear about the acceptability of additional research, while others expressly prohibit any use of DNA samples other than those strictly related to investigatory purposes.[151] Further concerns include the fate of DNA samples after the necessary information has been gathered and entered into the database. Many states still have unclear rules about what happens to the samples after DNA information is obtained and cataloged.[152]

There are additional concerns about having so much data in one place. With respect to large databases, there is an increased risk that those databases will be breached because they create a single target.[153] With the recent theft of approximately 145,000 consumer profiles from ChoicePoint,[154] it is clear that having such a large database of DNA information creates a target for security breaches, which could lead to the release of incredible amounts of DNA information.

CONCLUSION

The types of technologies discussed in this article allow the government to collect an ever-increasing amount of information about its citizens. The MATRIX program allowed for the aggregation of a

---

[148] *Id.*

[149] *Id.*

[150] ALA. CODE § 36-18-31 (2006).

[151] Axelrad, *supra* note 133.

[152] *Id.*

[153] Hoover & Chabrow, *supra* note 21.

[154] Goldfarb, *supra* note 22.

significant amount of government-held and publicly available information into a searchable format. States are still attempting to find ways to use this data, while overcoming the obstacles of differing state participation and enthusiasm for these types of initiatives. States also face the obstacles of overcoming differing state privacy laws and opposition from privacy-oriented interest groups such as the ACLU. The ACLU is also opposed to the REAL ID Act, which among other provisions, mandates that states create a system of drivers' licenses and identification cards that comply with federal standards. The creation of this national system of identification also requires that states store and make available to other states and the federal government a large amount of personal information. Objections to this innovation in storage and the use of searchable technology are most likely similar to those objections to the MATRIX program because the REAL ID database will be a searchable database of personal information and digital images of personal identification documents.

The DNA collection provisions that states and the federal government are enacting provide another way that the states and the federal government can collect and catalog information. New provisions allow information to be collected upon arrest, implicating a number of personal privacy issues that previously constituted a less complex question about the rights of those already convicted of a crime. As these new issues emerge with DNA collection from arrestees, the creation of new systemized identification cards and drivers' licenses, and states investigating the creation of programs similar to the MATRIX program, states will have to balance the interest of protecting personal privacy with the legitimate government objectives that these programs advance, primarily preventing terrorist activities and future crime.