DRIVER LICENSING UNDER THE REAL ID ACT: CAN CURRENT TECHNOLOGY BALANCE SECURITY AND PRIVACY?

Manoj Govindaiah*

I. INTRODUCTION

In an effort to better protect against future terrorist attacks, the U.S. government has passed or amended several pieces of legislation since September 11, 2001.[1] While these laws generate numerous arguments both in support of and in opposition to their purposes, each raises the major issue of the impact on privacy rights in the United States. Many of these laws allow government agencies to collect and store personal information about every individual residing in the United States, including non-citizens.[2] The question that arises is how the government will protect this information in such a manner that only the government's intended users have access.

On May 11, 2005, President Bush signed the REAL ID Act of 2005 ("the Act")[3] into law.[4] The Act modified several aspects of the immigration system and created comprehensive technical specifications for drivers' licenses and identification cards ("DLs/IDs").[5] Although the Act raises numerous concerns,[6] this Recent Development focuses on the

* J.D., University of Illinois College of Law, 2006; A.B., Public Policy Studies, University of Chicago, 2001.

1. *See, e.g.*, USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001); Enhanced Border and Visa Entry Reform Act of 2002, Pub. L. No. 107-73, 116 Stat. 543 (2002); Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2001); Illegal Immigration Reform and Immigrant Responsibility Act, Pub. L. No. 104-208, Division C 110 Stat. 3009, 546-724 (1996).

2. *See generally*, USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

3. REAL ID Act of 2005, Pub. L. No. 109-13, 119 Stat. 302 (2005) (to be codified at 49 U.S.C. § 30301).

4. Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, Pub. L. No. 109-13, 119 Stat. 231 (2005).

5. *See generally* CONGRESSIONAL RESEARCH SERVICE, THE LIBRARY OF CONGRESS, IMMIGRATION: ANALYSIS OF THE MAJOR PROVISIONS OF THE REAL ID ACT OF 2005 (2005) [hereinafter IMMIGRATION], *available at* http://www.fas.org/sgp/crs/homesec/RL32754.pdf.

6. Apart from the numerous immigration issues and civil rights concerns, constitutional issues include whether the Act violates the federalism and enumerated powers doctrines under the Tenth Amendment. *See, e.g.*, Serge Egelman & Lorrie Faith Cranor, *The REAL ID Act: Fixing Identity Documents with Duct Tape*, 2 I/S J.L. & POL'Y INFO. SOC'Y 149, 150 (2006), *available at* http://www.is-journal.org/V02I01/2ISJLP149.pdf. There are also other issues, such as logistical and psychological

current technologies being considered to fulfill the Act's new DL/ID requirements and the privacy concerns those technologies raise. Specifically, Part II provides an overview of the REAL ID Act's history and purpose, as well as highlights specific problematic provisions and privacy issues of the Act. Part III analyzes the technological options that currently exist and how effectively they guarantee privacy of the information gathered under the Act. It will also recommend which technological option the new DLs/IDs should employ.

II. BACKGROUND

A. History, Purpose, and Requirements of the Act

In addition to making broad changes to the immigration system, the REAL ID Act also codified specific requirements with which states' DLs/IDs must comply.[7] The REAL ID Act was introduced into the U.S. House of Representatives in January 2005, and received approval of the House in February 2005.[8] In order to assure passage by the Senate, the House of Representatives added the Act to the Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief of 2005 ("Emergency Supplemental Appropriations Act"), which passed the House in March 2005.[9] By adding the REAL ID Act's controversial provisions to the Emergency Supplemental Appropriations Act, which provided funding for the wars in Iraq and Afghanistan and for Asian tsunami relief,[10] the House of Representatives virtually guaranteed passage of the REAL ID Act by the Senate, because few Senators would oppose the "must pass" piece of legislation to which it was attached.[11]

---

concerns. *See REAL ID: Big Brother Could Cost Big Money*, THROUGH THE LOOKING GLASS (Citizens Against Government Waste, Washington, D.C.), Oct. 17, 2005, at 4, http://www.cagw.org/site/DocServer/Real_ID_FINAL_with_cover.pdf?docID=1281 [hereinafter CAGW] (discussing cost issues associated with the REAL ID Act); Elizabeth Bishop, *State Concerned About Implementing REAL ID Act,* NEWS10.NET, Feb. 24, 2006, http://www.news10.net/storyfull2.aspx?storyid=16091 (discussing the feasibility of and the logistical concerns with the REAL ID Act); Declan McCullagh, *National ID Cards on the Way?*, CNET NEWS.COM, Feb. 14, 2005, http://news.com.com/National+ID+cards+on+the+way/2100-1028_3-5573414.html?tag=nl (explaining protectionist, surveillance, and psychological concerns surrounding the REAL ID Act).

7. *See generally* IMMIGRATION, *supra* note 5. Specifically, the REAL ID Act modified eligibility criteria for asylum applicants, limited immigrants' chances for cancellation of removal, limited judicial review of some administrative agency holdings, allowed the Department of Homeland Security ("DHS") more authority to construct barriers at the U.S.-Mexico border, expanded the scope of criminal liability for illegal immigrants, and imposed new requirements upon state drivers' licenses and identification cards. *Id.* at Summary.

8. *Id.* at Summary.

9. *Id.* at 2; *see* Egelman & Cranor, *supra* note 6, at 173.

10. *See generally* Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, Pub. L. No. 109-13, 119 Stat. 231 (2005).

11. IMMIGRATION, *supra* note 5, at 1; Egelman & Cranor, *supra* note 6, at 173.

A version of the Emergency Supplemental Appropriations Act, which did not include the REAL ID provisions, passed the U.S. Senate in April, 2005, by a vote of 99-0.[12] A conference report that resolved the differences between the two versions, and which included the REAL ID provisions, passed the House on May 5, 2005, and the Senate on May 10, 2005, with no Senate debate.[13] President George W. Bush signed the Act into law on May 11, 2005.[14]

The Act's DL/ID provisions intend to create nationwide standards for the format and design of DLs/IDs.[15] Prior to the adoption of the Act, state and local governments maintained wide discretion over their individual DLs/IDs.[16] Previous congressional attempts at standardizing DLs/IDs resulted in widespread criticism due to fear that such a move would create a de facto national identification card.[17] After the September 11, 2001 terrorist attacks, however, support for standardized DLs/IDs gained momentum as a means to reduce illegal immigration and improve security, leading to the passage of the REAL ID Act.[18]

The Act provides specific pieces of information that states should display on the front of their DLs/IDs, including an individual's full legal name, date of birth, and gender, among other information.[19] States should also include physical security features to prevent tampering or use of the DL/ID for fraudulent purposes, and a common machine-readable technology element as well.[20] If a state's DL/ID does not conform to the Act's specifications, federal agencies cannot accept the DL/ID as federal identification or for any other official purpose.[21] This restriction effectively requires states to comply with the Act or risk not having their DLs/IDs accepted for a variety of common actions, such as entering a federal building or boarding a commercial airplane.[22]

---

12. IMMIGRATION, *supra* note 5, at 1.

13. *Id*. at 1–2. On December 8, 2006, Senators Daniel Akaka and John Sununu introduced legislation in the Senate that would repeal the DL/ID Provisions of the Real ID Act. "Akaka Introduces Leglislation Repealing the Real ID Act," Press Release, Dec. 11, 2006, http://akaka.senate.gov/public/index.cfm?FuseAction=PressReleases.Home&month=12&year=2006&release_id=1461. In deciding to try to repeal the Act, Senator Akaka based his decision on the significant estimated cost that implementation of the provisions would incur upon states, the fact that the DHS has still not issued regulations though states are expected to implement the Act's provisions by 2008, and the significant civil liberties and privacy issues that the Act's provisions raise. K.C. Jones, *Senators Threaten to Repeal Real ID Act Unless Changes are Made*, TECHWEB.COM, Dec. 14, 2006, http://www.techweb.com/showArticle.jhtml?articleID=196700218&cid=RSSfeed_TechWeb.

14. *See* Egelman & Cranor, *supra* note 6, at 173.

15. IMMIGRATION, *supra* note 5, at 38–40.

16. *Id.* at 38.

17. *Id.* at 38 n.117.

18. *See* McCullagh, *supra* note 6; *see also* Kelley Beaucar Vlahos, *"REAL ID" Bill Caught in Limbo*, FOXNEWS.COM, Apr. 6, 2005, http://www.foxnews.com/story/0,2933,152328,00.html.

19. REAL ID Act of 2005, Pub. L. No. 109-13, § 202(b)(1)–(7), 119 Stat. 302, 312 (2005) (to be codified at 49 U.S.C. § 30301). At a minimum, the following information must also be included on each DL/ID: DL/ID number, digital photograph, address of principal residence, and signature. *Id.*

20. *Id.* § 202(b)(8)–(9).

21. *Id.*

22. *See id.* § 201(3).

The Act also standardizes the procedures that states must follow prior to issuing or renewing a DL/ID.[23] States must require proof of address, a social security number, and a photo identification document or a document containing both date of birth and full legal name, such as a birth certificate.[24] Additionally, states must verify that the applicant is a U.S. citizen or legally present in the country, confirm the validity of the individual's social security number with the Social Security Administration, verify that the individual does not have a DL/ID from another state, and authenticate identification documents with the issuing agency.[25] Finally, states must maintain motor vehicle databases containing at least all of the information listed on the DL/ID, in addition to an individual's driving history.[26] The databases must link with those of all other states, and individual states are prohibited from maintaining separate databases for themselves, effectively creating a national database.[27] States must comply with the Act's provisions by May, 2008.[28]

A majority of the states have already complied with some of the Act's provisions even though the DL/ID provisions have yet to take effect.[29] For example, all states require DLs/IDs to display the information that the Act mandates.[30] Each state, however, employs differing types of security features, common machine-readable technologies, and documents required for DL/ID issuance.[31] Additionally, prior to the Act, there was no national database; rather, each state maintained its own database.[32]

B. Privacy Concerns Raised by the Act

The type of technology that the Act requires states to implement in their DLs/IDs will determine the degree of susceptibility to violation of individuals' privacy rights. The DHS is responsible for issuing regulations specifying which common machine-readable technology will

23. *Id.* § 202(c).

24. *Id.* § 202(c)(1); Egelman & Cranor, *supra* note 6, at 175.

25. REAL ID Act § 202(c)(2)(B), (c)(3)(A), (d)(5)–(6). Although states are not required to print an individual's social security number on the DL/ID itself, they must collect the number, verify it with the Social Security Administration, maintain it in a database, and share the database with the federal government. Egelman & Cranor, *supra* note 6, at 172. Additionally, all identification documents must be digitally stored for at least ten years, or stored in paper form for seven years. REAL ID Act § 202(d)(2).

26. REAL ID Act § 202(d)(13).

27. *Id.* § 202(d)(12); *see also* Egelman & Cranor, *supra* note 6, at 174–75. The national database is expected to be shared with those of Canada and Mexico as well. *REAL ID Act Sent to Senate in "Must Pass" Emergency Appropriations Bill*, IMMIGRANTS' RTS. UPDATE (Nat'l Immigration Law Ctr., Los Angeles, Cal.), Mar. 31, 2005, *available at* http://www.nilc.org/immspbs/DLs/DL022.htm.

28. *See* REAL ID Act § 202(a)(1).

29. *See* Egelman & Cranor, *supra* note 6, at 174.

30. *See id.*

31. *See id.* at 155–69, 174.

32. *See id.* at 174–75.

be used, but has not yet done so.[33] Regulations were expected in late 2006 but have not yet been issued.[34] Thus, uncertainty remains as to the type of technology that will be used for DLs/IDs, what information that technology will contain, and what protections will be in place to protect individuals' privacy.

Although several of the Act's provisions raise privacy issues, this Recent Development focuses on privacy concerns specifically arising from the required common machine-readable technology that the DLs/IDs must contain. The main concern with the REAL ID Act's DL/ID provisions is that a much larger group of entities and individuals than ever before will have access to private information. Because only a relatively small proportion of U.S. citizens have passports,[35] the DL/ID has become the logically preferred choice of identification.[36] For example, government-issued identification is required to board an airplane, obtain Medicare benefits, and receive other government services.[37] Additionally, because the DL/ID contains both an individual's picture and date of birth, it has become the de facto form of identification used for non-governmental transactions as well, such as entering a bar, purchasing cigarettes or alcohol, or writing a check.[38] Because of the ubiquitous use of DLs/IDs, the government must require protection of the common machine-readable technology so that unauthorized entities cannot access the information that the technology contains. Furthermore, even if authorized entities access the information encoded on DLs/IDs, there is no guarantee that these entities would use it in authorized manners.[39] Part III elaborates upon these privacy implications. At present, a sufficiently cost-effective technology does not exist to protect against the risks of identity theft. Part III also examines the feasibility of some of the various machine-readable technological options that the DHS may consider for use with DLs/IDs to fulfill the Act's requirements.

---

33. REAL ID Act §§ 201(4), 205(a); *see also* Ethan Butterfield, *States See Hurdles to Implementing REAL ID*, GOVERNMENT COMPUTER NEWS, Oct. 10, 2005, http://www.gcn.com/print/24_30/37196-1.html.

34. LEGIS. ANALYST'S OFF., AN OVERVIEW: IMPLEMENTATION OF THE FEDERAL REAL ID ACT OF 2005 1 (2006), *available at* http://www.lao.ca.gov/handouts/transportation/2006/Real_ID_02_22_06.pdf. "Real ID Act of 2005," Sourcewatch, July 31, 2006, http://www.sourcewatch.org/index.php?title=REAL_ID_Act_of_2005.

35. *See* YaleGlobal Online, Americans Are Tuning Out the World, http://yaleglobal.yale.edu/display.article?id=6553 (last visited Nov. 24, 2006) (estimating that 21% of U.S. citizens possess passports).

36. Egelman & Cranor, *supra* note 6, at 150.

37. Declan McCullagh, *Your License or Your Life*, WIRED NEWS, Jul. 22, 1999, http://www.wired.com/news/politics/1,20881-1.html.

38. *See* Egelman & Cranor, *supra* note 6, at 150.

39. *See id*. at 178.

III. ANALYSIS

This section considers two possible types of common machine-readable technologies that the DHS may require states to use in order to comply with the REAL ID Act's DL/ID requirements: barcodes and radio frequency identification tags. It then analyzes which technological option can best balance security and privacy interests under the Act.

A. Barcodes

A majority of states currently use barcodes on their DLs/IDs.[40] One of the most commonly used types, the two-dimensional ("2-D") barcode, or PDF417, resembles a crossword puzzle and serves as a small portable data file, which enables the barcode to store a large amount of data.[41] These data could include the information displayed on the front of the DL/ID, a photograph,[42] and possibly a biometric identifier, such as one's fingerprints.

The barcode stores information through the widths and heights of the bars and spaces on the barcode, with the variations representing characters or symbols.[43] Barcode readers are required to access the information stored in the barcode.[44] The reader interprets the widths and heights to decode the stored data; therefore, the only way to retrieve the barcode's stored data is to physically pass the barcode through a scanner.[45] Because of the inability to scan barcodes from a distance, barcodes inherently provide a level of security that protects privacy interests.[46]

Barcodes have become increasingly affordable, and, presently, forty states use 2-D barcodes on their DLs/IDs.[47] As a result, if the DHS chose to implement this technology to fulfill the REAL ID Act's common machine-readable technology requirement, the DHS could do so without posing a substantial burden on the majority of the states in terms of cost or infrastructure upgrades.[48] 2-D barcodes' affordability and popularity, however, have facilitated the purchase of individual printers and

40. *Id.* at 174.

41. IDenticard, Barcode Basics: How the Technology Works, What it Offers, http://www.identicard.com/e-news/july05/barcode.htm (last visited Oct. 4, 2006).

42. *See id.*

43. BarCode1, BarCode1 FAQ Page, http://www.barcode-1.net/pub/russadam/faq.html [hereinafter BarCode1 FAQ] (last visited Oct. 4, 2006); *see also* BarCode1, 2-Dimensional Bar Code Page, http://www.barcode-1.net/pub/russadam/stack.html [hereinafter 2-Dimensional Bar] (last visited Oct. 4, 2006).

44. CAGW, *supra* note 6, at 12.

45. *Id.* at 12–13; BarCode1 FAQ, *supra* note 43; 2-Dimensional Bar, *supra* note 43.

46. *See* CAGW, *supra* note 6, at 12.

47. Egelman & Cranor, *supra* note 6, at 174; *see* CAGW, *supra* note 6, at 16.

48. *See* CAGW, *supra* note 6, at 16.

scanners.[49] Thus, virtually anyone with a barcode reader can scan and decode a barcode, and, in the process, endanger privacy.[50]

Barcodes' ubiquitous use throughout the country heightens privacy concerns. Airports, hospitals, federal buildings, and police officers, among others, now regularly scan DLs/IDs.[51] Additionally, other types of private entities such as bars and convenience stores not only scan barcodes to verify certain pieces of information about customers, such as age, but also gain access to all of an individual's personal information contained on the DL/ID.[52] Business owners insist that the personal information is invaluable because it allows them to create targeted mailings, analyze trends, and determine the popularity of certain events or products.[53] While their claims may be legitimate, there is no reason for these entities to have access to an individual's social security number, physical characteristics, or photograph, for example.[54] Despite these concerns, however, 2-D barcodes remain a viable option for use under the Act.

B. Radio Frequency Identification ("RFID") Tags

Another option that the DHS can use to fulfill the Act's common machine-readable technology requirement is the radio frequency identification tag. RFID tags are a newer form of technology that are quickly gaining widespread use by entities such as government agencies,[55] livestock operations,[56] retail operators,[57] libraries,[58] and schools.[59] The U.S. government is implementing procedures to use RFID tags in passports[60] and for border crossings,[61] and to replace barcodes and magnetic strips for use in government institutions.[62] The DHS has

49. *See* Jennifer 8. Lee, *Welcome to the Database Lounge*, N.Y. TIMES, Mar. 21, 2002, at G1.

50. *See generally id.*

51. *Id.*

52. *Id.*

53. *Id.*

54. Some bar owners claim that learning the age, weight, height, and gender of their patrons allows them to know what types of drinks should be marketed to certain groups of people. Kim Zetter, *Great Taste, Less Privacy*, WIRED NEWS, Feb. 6, 2004, http://www.wired.com/news/privacy/0,1848,62182,00.html.

55. *See generally* U.S. GOV'T ACCOUNTABILITY OFF., RADIO FREQUENCY IDENTIFICATION TECHNOLOGY IN THE FEDERAL GOVERNMENT (2005) [hereinafter RFID], *available at* http://www.gao.gov/new.items/d05551.pdf. A complete list of government agencies using RFID tags (current as of May 2005) and for what purposes is available. *Id.* at 13.

56. Bob Brewin, *Radio Frequency Identification*, COMPUTERWORLD, Dec. 16, 2002, http://www.computerworld.com/mobiletopics/mobile/technology/story/0,10801,76682,00.html.

57. Kendra Mayfield, *Radio ID Tags: Beyond Bar Codes*, WIRED NEWS, May 20, 2002, http://www.wired.com/news/technology/0,1282,52343,00.html.

58. Julia Scheeres, *Three R's: Reading, Writing, RFID*, WIRED NEWS, Oct. 24, 2003, http://www.wired.com/news/technology/0,1282,60898,00.html.

59. *Id.*

60. RFID, *supra* note 55, at 17.

61. U.S. Department of Homeland Security, Fact Sheet: Radio Frequency Identification Technology, http://www.dhs.gov/dhspublic/display?content=4307 (last visited Sept. 6, 2006).

62. *See generally* RFID, *supra* note 55, at 13–14.

previously stated its preference for RFID tags, indicating a high probability that it will require their use in DLs/IDs under the REAL ID Act.[63]

There are several types of RFID tags, with the passive, read-only, tag being the most cost-effective version.[64] RFID technology requires a tag, a reader, and a database.[65] The tag contains a chip that stores data and an antenna that transmits the data to the reader.[66] Passive, read-only RFID tags store only a minimal amount of information—less data than a 2-D barcode.[67] The reader emits radio transmissions that serve as the tag's power source, causing the tag to transmit data to the reader.[68] Under the right conditions, the reader can read data from ten to twenty feet away.[69] Whether readers are stationary or mobile, their emission of radio waves will cause all tags that are designated to respond to the readers' particular frequency to transmit their data.[70] The data then pass to a database that matches and decodes it.[71]

As is the case with barcodes, rapidly lowering costs have made RFID tag technology easily accessible. Currently, one can purchase a mobile reader for only a few hundred dollars.[72] However, no state presently uses RFID tag technology in its DLs/IDs.[73] Thus, requiring use of this common machine-readable technology would create a significant burden on states, especially given the short timeframe in which states must implement the technology.[74] Moreover, and in contrast to barcodes, RFID tag technology has greater implications for individuals' privacy.[75] Because readers can scan RFID tags from a distance, one can imagine a significant increase in identity theft resulting from thieves easily and discretely scanning others' DLs/IDs in public places.[76] While an individual must generally consent to a scan of his or her DL/ID's

63. *See* Anita Ramasastry, *Why the "REAL ID" Act Is a Real Mess*, FINDLAW, Aug. 12, 2005, http://www.cnn.com/2005/LAW/08/12/ramasastry.ids/index.html.

64. RFID, *supra* note 55, at 6–8. Information about the other types of RFID tags is available. *Id.* at 4–11.

65. *Id.* at 5.

66. *Id.*

67. A passive, read-only RFID tag can only store less than 64 bits of data. *Id.* at 7. A 2-D barcode, however, can store approximately 2000 bytes of data. Swipe, Swipe Research, http://www.we-swipe.us/research.html (last visited Oct. 4, 2006). One byte is equivalent to eight bits. *Byte*, WIKIPEDIA, THE FREE ENCYCLOPEDIA (Oct. 4, 2006), http://en.wikipedia.org/wiki/Byte. Therefore, 2-D barcodes can store 16000 bits of data, versus only 64 bits with passive, read-only RFID tags. Other types of RFID tags can store significantly more data but are much more expensive. RFID, *supra* note 55, at 7–8; *see also* CAGW, *supra* note 6, at 14.

68. RFID, *supra* note 55, at 6.

69. *See id.*

70. *See id.* at 8.

71. *Id.* at 8–9.

72. A search on www.google.com for "RFID Reader" found numerous readers for sale ranging in price from as low as $150 to nearly $2000.

73. Egelman & Cranor, *supra* note 6, at 155–69.

74. *See supra* text accompanying notes 24–29.

75. *See* CAGW, *supra* note 6, at 13, 15–16.

76. *See id.* at 13.

barcode, one could scan another's DL/ID RFID tag without that person's knowledge or permission. Thus, although RFID tag technology is an incredibly useful tool for entities such as businesses, libraries, and farmers trying to keep track of inventory, books, or livestock, when used for personal identification purposes, the RFID tag precariously places individuals' privacy rights at risk.[77]

C. Which Technology Option Is Best Under the REAL ID Act?

In order to better determine which technology is most appropriate in terms of balancing privacy interests with achieving the Act's goals, this section first discusses the reasoning behind requiring a common machine-readable technology element. It then examines two characteristics—capacity and encryption—of barcodes and RFID tags, as they relate to privacy. Although neither of these technologies is foolproof, both remain viable options for the DHS to use under the Act.

1. Purpose of the Common Machine-Readable Technology

The REAL ID Act is intended to improve the security and authenticity of DLs/IDs.[78] According to the American Association of Motor Vehicle Administrators, a DL/ID is intended to support law enforcement by aiding in identity and address verification, and administrative processing.[79] Common machine-readable technology is supposed to provide a quick and easy method to guarantee that the information displayed on the front of the DL/ID has not been altered since the DL/ID's printing, thus validating the DL/ID's integrity.[80] Therefore, in standardizing the use of such technology among the states, Congress intended to offer law enforcement and federal agencies an easier and more secure method of verifying identity and reducing fraud.

The common machine-readable technology provision, however, does not address privacy concerns. As mentioned *supra* in Part II.B, the Act does not consider the consequences of relying on DLs/IDs as the main form of identification throughout the country or the privacy concerns that common machine-readable technologies raise.[81] If the purpose of requiring the inclusion of technology in DLs/IDs is solely to offer a method of verifying identity and reducing fraud, then the DHS

77. *See id*. at 13–15.

78. OFFICE OF MGMT. & BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, STATEMENT OF ADMINISTRATION POLICY: H.R. 418–REAL ID ACT OF 2005 (2005), *available at* http://www.whitehouse.gov/omb/legislative/sap/109-1/hr418sap-h.pdf.

79. AM. ASS'N OF MOTOR VEHICLE ADMINISTRATORS, PERSONAL IDENTIFICATION–AAMVA INTERNATIONAL SPECIFICATION–DL/ID CARD DESIGN 42 (2005) [hereinafter AAMVA], *available at* http://www.aamva.org/AAMVA/DocumentDisplay.aspx?id={66260AD6-64B9-45E9-A253-B8AA32241BE0}.

80. *See* Egelman & Cranor, *supra* note 6, at 174.

81. *See supra* Part II.B.

should choose a technology that can fulfill this goal but simultaneously lacks the capability to offer other uses. It is only through this balance that the DHS can select a technology that balances the security and privacy interests that DLs/IDs affect.

2. Capacity

The capacity of the common machine-readable technology directly impacts privacy because it affects how much of an individual's personal information an authorized user can access through one's DL/ID. A smaller capacity is obviously better in terms of privacy because less personal information would be available via the technology.

As previously noted, the 2-D barcode can hold approximately 2000 bytes worth of information.[82] This capacity is sufficient to store all of the data printed on the front of the DL/ID, in addition to a few other pieces of information that are not typically displayed on DLs/IDs, such as an individual's place of birth, race, and hair color.[83] Additionally, barcodes typically have sufficient space to also hold a biometric identifier, which only a few states currently utilize, but lack the capacity to store significantly more data.[84] Thus, barcodes offer sufficient size to verify the DL/ID's authenticity without significantly impacting privacy because they contain little more than what is already displayed on the DL/ID itself.

The passive, read-only RFID tag, discussed *supra* in Part III.B, has a significantly smaller capacity to hold data than a 2-D barcode.[85] If the DHS chose to use RFID tags, it would presumably choose the passive, read-only tag due to cost concerns.[86] This type of RFID tag, however, would be unable to store all of the information displayed on the front of the DL/ID, making it insufficient to validate identity and reduce DL/ID fraud.[87] Therefore, to carry out the goals of requiring a common machine-readable technology, the DHS would need to choose a different type of RFID tag.

The next logical type of RFID tag that the DHS would use is the semipassive, read-write RFID tag because of its significantly larger storage capacity.[88] This tag is designed to allow data updates, which

82. *See supra* note 67.

83. AAMVA, *supra* note 79, at 51–53.

84. CAGW, *supra* note 6, at 12. As of 2002, seven states collected fingerprints when issuing DLs/IDs. REED F. MORRIS ET AL., NAT'L CONFERENCE OF STATE LEGISLATURES, DRIVER'S LICENSING: SECURITY CONCERNS, http://www.ncsl.org/programs/press/2002/issues/driverslicense.htm (last visited Sept. 6, 2006).

85. *See supra* note 67.

86. *See* CAGW, *supra* note 6, at 13–14; *see also* RFID, *supra* note 55, at 8.

87. Passive, read-only tags have "very little storage room" and are ideal for library and video rental cards which do not require space for a significant amount of information. CAGW, *supra* note 6, at 13.

88. *Id.* at 14; RFID, *supra* note 55, at 7.

requires it to have a larger memory capacity.[89] While this tag would provide sufficient space to store all of the information displayed on the DL/ID, it would actually offer too much space, leading privacy groups to conclude that the DHS would not limit the RFID tag to the storage of DL/ID information.[90] Additional information stored could include family history, health and financial records, or a variety of other personal information.[91] Although easy accessibility to this type of information could be beneficial in certain circumstances, the ability of anyone with a reader to remotely read an RFID tag seriously jeopardizes individuals' privacy.[92] Therefore, using the passive, read-write RFID tag greatly expands the possible uses of DLs/IDs beyond identity verification and fraud reduction, and adversely impacts privacy.

3. Encryption

Encryption protection directly affects privacy because it is one of the few ways to protect the data stored in the common machine-readable technology so that only authorized users can access it. Encryption is of greater necessity with RFID tags than with barcodes because RFID tags can be read remotely.

Barcodes, by their very nature, are a type of encryption.[93] Each space and line represents characters and text, and only a reader containing decoding software can decode the data.[94] Therefore, barcodes are encoded in the sense that their data cannot be interpreted by the naked eye.[95] Other security options include encoding the data before they are printed in the form of a barcode.[96] Using this method, one would have to proceed through two different types of decodings, first from the barcode to the encoded data, and second from the encoded data to the decoded data, before accessing the actual data itself.[97] Additionally, barcodes could be designed to respond only to readers that are specifically designed to read them, which is a method some states currently use with their present DL/ID barcodes.[98] Despite these options, the affordability of barcode readers and the ease of decrypting

89. CAGW, *supra* note 6, at 14.
90. *See id.* at 15.
91. *Id.*
92. *See* RFID, *supra* note 55, at 8–9.
93. *See* Product Manager Joint-Automatic Identification Technology, Bar Coding, http://www.eis.army.mil/ait/Technology/bar_coding.asp (last visited Sept. 6, 2006).
94. *See generally Barcode*, MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 92 (10th ed. 1999).
95. *See generally,* CAGW, *supra* note 6, at 12.
96. *See, e.g.*, CHARLES LYNCH & STEPHEN FREY, 2D BARCODES & BIOMETRICS: THE SECURE COMBINATION ON SEAFARER ID CARDS 7 (2004), http://www.biometrics.org/bc2004/CD/PDF_PROCEEDINGS/new_Lynch_Update.pdf.
97. *See id.*
98. *See* Google Answers, Missouri Drivers License Encryption, http://answers.google.com/answers/threadview?id=590107 (last visited Sept. 6, 2006).

barcodes make encryption techniques not particularly secure.[99] Because barcodes must come into near proximity or physical contact with a reader, however, they may provide sufficient security regardless of encryption flaws.[100]

Encryption of RFID tags involves converting data into code using a mathematical value called a "key" and an algorithm.[101] The algorithm creates a particular type of text that only authorized users can access and interpret.[102] The specific key is required to decode the encrypted information.[103] Although secure encryption of an RFID tag is possible, a hacker could quickly crack a weak encryption code.[104] Nevertheless, when strong enough encryption is properly used, the encryption technique can securely ensure the integrity and confidentiality of the encrypted data.[105]

While offering numerous benefits and safeguards, RFID tag encryption remains costly.[106] It is highly unlikely that the DHS would encrypt RFID tags even if it chose to use them.[107] The REAL ID Act does not require any type of safeguard, implying that the DHS is not required to implement one.[108]

Another option that the DHS could employ to protect information on RFIDs is blocking technology. Blocking technology consists of a device that would block transmission of the reader's radio signals so that only an authorized user could access the data.[109] The technology, however, is cumbersome and would require an individual to place a blocker tag directly on top of the RFID tag.[110] A similar option is an actual physical barrier, such as a piece of metal, to serve as the blocker.[111] The State Department is considering including metal pieces in passport jackets to serve as blockers for passport RFID tags.[112] While these blocking technology options are technically feasible, it is unreasonable to

99. Several entities offer software for barcode decryption. *See, e.g.*, Swipe, The SWIPE Toolkit, http://www.turbulence.org/Works/swipe/barcode.html (last visited Sept. 6, 2006). Often, one must only scan a barcode and then download software to decode it. *See* Barcode-SDK, About the Project, http://www.intelcom.ru/2d/english/index.php (last visited Sept. 6, 2006).

100. *See* CAGW, *supra* note 6, at 12.

101. RFID, *supra* note 55, at 20.

102. *Id.*

103. *Id.*

104. Olga Kharif, *What's Lurking in That RFID Tag?*, BUSINESSWEEK ONLINE, Mar. 16, 2006, http://www.businessweek.com/technology/content/mar2006/tc20060316_117677.htm?campaign_id=rss_tech.

105. *See id.*

106. *See generally* Answers.com, RFID, http://www.answers.com/topic/rfid (last visited Sept. 6, 2006) (noting that some manufacturers and retailers have chosen to use weak encryption schemes due to cost reasons, even though those schemes can be hacked).

107. *See* CAGW, *supra* note 6, at 14.

108. *See generally* Ramasastry, *supra* note 63.

109. RFID, *supra* note 55, at 23.

110. *Id.*

111. *Id.* at 23–24.

112. *Id.*; Paul Prince, *United States Sets Date for E-Passports*, RFID JOURNAL, Oct. 25, 2005, http://www.rfidjournal.com/article/articleview/1951/1/1/.

expect an individual to carry two cards (the DL/ID and the blocker) or to carry his DL/ID in a passport-type jacket containing a physical barrier.

Despite greater availability of encryption and security measures, RFID tags still generate privacy concerns because of their remote access capabilities. Although barcodes do not offer guarantees against unauthorized access, they provide better security because access remains in the DL/ID-holder's control.

IV. CONCLUSION

Although barcodes are not foolproof, based on current technology, they provide the best balance between security and privacy. Due to the limited storage capacity of 2-D barcodes, they prohibit the storage of extraneous information. At the same time, because physical scanning of the barcode is required to obtain the necessary information, barcodes also allow an individual to control his or her stored data. The necessity of physically scanning a barcode through a reader offers a sufficient level of security, despite limited encryption technologies.

RFID tags are valuable assets in many circumstances, but current technology does not make them feasible for use in DLs/IDs. Their storage capability is too large to limit their use to verifying identity and reducing fraud, and their remote reading features create vast opportunities for privacy invasion. While encryption technology is available, the DHS has expressed little interest in using it under the REAL ID Act. Therefore, RFID tags do not currently represent a viable option. Perhaps in the future, RFID tags may provide a legitimate and feasible alternative. To guarantee sufficient privacy protection, however, RFID tag security measures require improvements, in terms of both infrastructure and cost. Therefore, DHS should implement 2-D barcodes as the machine-readable technology of choice on new DLs/IDs under the REAL ID Act.