



**NAVAL  
POSTGRADUATE  
SCHOOL**

**MONTEREY, CALIFORNIA**

**THESIS**

**WHAT'S IN A NAME: A COMPARATIVE ANALYSIS OF  
THE UNITED STATES' REAL ID ACT AND THE  
UNITED KINGDOM'S NATIONAL IDENTITY SCHEME**

by

Karrie Anne Jefferson

December 2015

Thesis Advisor:  
Second Reader:

Carolyn Halladay  
Nadav Morag

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.				
<b>1. AGENCY USE ONLY</b> (Leave blank)		<b>2. REPORT DATE</b> December 2015		<b>3. REPORT TYPE AND DATES COVERED</b> Master's thesis
<b>4. TITLE AND SUBTITLE</b> WHAT'S IN A NAME: A COMPARATIVE ANALYSIS OF THE UNITED STATES' REAL ID ACT AND THE UNITED KINGDOM'S NATIONAL IDENTITY SCHEME			<b>5. FUNDING NUMBERS</b>	
<b>6. AUTHOR(S)</b> Karrie Ann Jefferson				
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> Naval Postgraduate School Monterey, CA 93943-5000			<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>	
<b>9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> N/A			<b>10. SPONSORING / MONITORING AGENCY REPORT NUMBER</b>	
<b>11. SUPPLEMENTARY NOTES</b> The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ___N/A___.				
<b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b> Approved for public release; distribution is unlimited			<b>12b. DISTRIBUTION CODE</b> A	
<b>13. ABSTRACT (maximum 200 words)</b> <p>Since September 11, 2001, many governments have considered developing national identity management systems. Beyond identification, politicians and proponents of these systems have touted such system benefits as combating terrorism, preventing identity theft, facilitating travel, and combating illegal work and benefit fraud. For these reasons, the United States and United Kingdom both considered variations of these systems. While the United Kingdom passed the Identity Cards Act of 2006 and spent several years developing a national identity management system before ultimately scrapping the scheme in 2010, the United States sought to secure further the existing means of identification—driver's licenses and identity cards—through the passage of the REAL ID Act. Both measures met with widespread resistance.</p> <p>What does an examination of resistance to nationwide identity management schemes in the United States and United Kingdom reveal about the nature of national identity management systems and identity cards, and what does this resistance tell policymakers and security officials who promote such schemes? Through a comparative analysis of the REAL ID Act implementation and the National Identity Scheme, this thesis shows that Anglophone, common-law nations experience the same inhibiting factors, whether or not they attempt to implement a national identity management system or an identity card on a national scale.</p>				
<b>14. SUBJECT TERMS</b> personal identity management, national identity management system, national identity card, identity card, nationwide identity system, driver's license, REAL ID Act, national identity scheme, United Kingdom, national identity system, public policy, privacy, civil rights, civil liberties, public acceptance, terrorism, security			<b>15. NUMBER OF PAGES</b> 121	
			<b>16. PRICE CODE</b>	
<b>17. SECURITY CLASSIFICATION OF REPORT</b> Unclassified		<b>18. SECURITY CLASSIFICATION OF THIS PAGE</b> Unclassified	<b>19. SECURITY CLASSIFICATION OF ABSTRACT</b> Unclassified	<b>20. LIMITATION OF ABSTRACT</b> UU

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

**WHAT'S IN A NAME: A COMPARATIVE ANALYSIS OF THE UNITED STATES' REAL ID ACT AND THE UNITED KINGDOM'S NATIONAL IDENTITY SCHEME**

Karrie Ann Jefferson  
Policy Analyst, Office of Biometric Identity Management,  
National Protection and Programs Directorate,  
Department of Homeland Security, Washington, DC  
B.A., University of Maryland, College Park, 2008

Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES  
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL  
December 2015**

Approved by: Carolyn Halladay  
Thesis Advisor

Nadav Morag  
Second Reader

Erik Dahl  
Associate Chair of Instruction  
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

Since September 11, 2001, many governments have considered developing national identity management systems. Beyond identification, politicians and proponents of these systems have touted such system benefits as combating terrorism, preventing identity theft, facilitating travel, and combating illegal work and benefit fraud. For these reasons, the United States and United Kingdom both considered variations of these systems. While the United Kingdom passed the Identity Cards Act of 2006 and spent several years developing a national identity management system before ultimately scrapping the scheme in 2010, the United States sought to secure further the existing means of identification—driver’s licenses and identity cards—through the passage of the REAL ID Act. Both measures met with widespread resistance.

What does an examination of resistance to nationwide identity management schemes in the United States and United Kingdom reveal about the nature of national identity management systems and identity cards, and what does this resistance tell policymakers and security officials who promote such schemes? Through a comparative analysis of the REAL ID Act implementation and the National Identity Scheme, this thesis shows that Anglophone, common-law nations experience the same inhibiting factors, whether or not they attempt to implement a national identity management system or an identity card on a national scale.

THIS PAGE INTENTIONALLY LEFT BLANK

# TABLE OF CONTENTS

<b>I.</b>	<b>INTRODUCTION.....</b>	<b>1</b>
<b>A.</b>	<b>RESEARCH QUESTION .....</b>	<b>1</b>
<b>B.</b>	<b>PROBLEM STATEMENT .....</b>	<b>2</b>
<b>C.</b>	<b>LITERATURE REVIEW .....</b>	<b>3</b>
	<b>1. Identity Management System Nomenclature .....</b>	<b>4</b>
	<b>2. Identity Management System Models.....</b>	<b>6</b>
	<b>3. Identity Management System Architecture.....</b>	<b>8</b>
<b>D.</b>	<b>RESEARCH DESIGN/METHODOLOGY .....</b>	<b>12</b>
<b>E.</b>	<b>CHAPTER OUTLINE.....</b>	<b>13</b>
<b>II.</b>	<b>UNITED STATES AND UNITED KINGDOM’S IDENTITY MANAGEMENT SCHEMES.....</b>	<b>15</b>
<b>A.</b>	<b>UNITED STATES—REAL ID ACT.....</b>	<b>15</b>
	<b>1. REAL ID Act Overview.....</b>	<b>17</b>
	<i>a. Document Requirements.....</i>	<i>17</i>
	<i>b. Issuance Standards .....</i>	<i>17</i>
	<i>c. Other Requirements .....</i>	<i>18</i>
	<i>d. REAL ID Act Purpose.....</i>	<i>20</i>
	<b>2. What Is the REAL ID: A National Identity Management     System, a National ID Card, or Neither?.....</b>	<b>21</b>
	<i>a. The REAL ID Is Not a National ID Card or a         National Identity Management System .....</i>	<i>22</i>
	<i>b. The REAL ID Is Not a National Identity Card, but         May Lead to a National Identity Management         System.....</i>	<i>23</i>
	<i>c. REAL ID Is a “De Facto” National Identity Card or         Part of a “De Facto” National Identity Management         System.....</i>	<i>24</i>
	<i>d. The REAL ID Is a National Identity Card and         Creates a National Identity Management System.....</i>	<i>25</i>
	<i>e. Summary.....</i>	<i>26</i>
<b>B.</b>	<b>UNITED KINGDOM—IDENTITY CARDS ACT.....</b>	<b>27</b>
	<b>1. Identity Cards Act Overview .....</b>	<b>28</b>
	<i>a. National Identity Register.....</i>	<i>29</i>
	<i>b. ID Cards .....</i>	<i>31</i>
	<i>c. Scheme Provisions .....</i>	<i>31</i>
	<i>d. Identity Cards Act Purpose .....</i>	<i>34</i>

2.	<b>What Is the National Identity Scheme? A National Identity Management System, a National ID Card, or Neither?.....</b>	<b>37</b>
<b>III.</b>	<b>POLICY AND PRIVACY CONCERNS .....</b>	<b>39</b>
A.	<b>PURPOSE CONCERNS .....</b>	<b>39</b>
1.	<b>Schemes Will Not Enhance National Security or Prevent Terrorism.....</b>	<b>39</b>
2.	<b>Schemes Will Not Prevent Identity Theft .....</b>	<b>41</b>
3.	<b>Schemes Will Not Reduce Illegal Immigration or Unlawful Employment.....</b>	<b>42</b>
B.	<b>PRIVACY CONCERNS.....</b>	<b>43</b>
1.	<b>Function Creep.....</b>	<b>43</b>
2.	<b>Data Security and Privacy Protections .....</b>	<b>46</b>
3.	<b>Data Integrity .....</b>	<b>48</b>
4.	<b>Linking of Databases/Expanded Sharing of Data.....</b>	<b>50</b>
5.	<b>Increased Collection of Data (Type and Amount of Data Held).....</b>	<b>51</b>
<b>IV.</b>	<b>CIVIL RIGHTS AND CIVIL LIBERTIES CONCERNS .....</b>	<b>55</b>
A.	<b>RACIAL PROFILING AND DISCRIMINATION .....</b>	<b>55</b>
B.	<b>TRACKING INDIVIDUALS.....</b>	<b>59</b>
C.	<b>SURVEILLANCE SOCIETY .....</b>	<b>62</b>
<b>V.</b>	<b>PUBLIC RESPONSE .....</b>	<b>67</b>
A.	<b>PUBLIC ENGAGEMENT AND GOVERNMENT TRANSPARENCY .....</b>	<b>67</b>
B.	<b>PUBLIC ACCEPTANCE.....</b>	<b>72</b>
C.	<b>CULTURAL AND HISTORICAL FACTORS.....</b>	<b>75</b>
<b>VI.</b>	<b>CONCLUSION .....</b>	<b>79</b>
	<b>APPENDIX A. DATA ELEMENTS IN THE IDENTITY CARDS ACT 2006 .....</b>	<b>83</b>
	<b>APPENDIX B. DATA ELEMENTS IN THE AAMVA DRIVER’S LICENSE/ IDENTIFICATION CARD DESIGN SPECIFICATIONS, ANNEX D .....</b>	<b>87</b>
	<b>LIST OF REFERENCES.....</b>	<b>93</b>
	<b>INITIAL DISTRIBUTION LIST .....</b>	<b>101</b>

## LIST OF FIGURES

Figure 1.	UK National ID Card: Key Features Explained .....	11
-----------	---	----

THIS PAGE INTENTIONALLY LEFT BLANK

## LISTs OF ACRONYMS AND ABBREVIATIONS

AAMVA	American Association of Motor Vehicle Administrators
ASBO	Anti-Social Behavior Order
CCTV	closed-circuit television
CDLIS	Commercial Driver's License Information System
CRE	Commission for Racial Equality
DMV	Department of Motor Vehicles
DVLA	Driver and Vehicle Licensing Agency
EDL	enhanced driver's license
eID	electronic identity
eIDMS	eID Management Systems
FIDIS	Future of Identity in the Information Society
FIPPs	fair information practice principles
GCHQ	Government Communications Headquarters
HMRC	Her Majesty's Revenue and Customs
IDCA	Identity Card Act 2006
IdMS	identity management systems
IT	information technology
ITAA	Information Technology Association of America
LSE	London School of Economics
MRT	machine-readable technology
MRZ	machine-readable zone
NDR	National Driver Register
NHS	National Health Service
NHTSA	National Highway Transportation Safety Administration
NIDS	national identification scheme
NIS	National Identity Scheme
NPRM	Notice of Proposed Rulemaking
PDPS	Problem Driver Pointer System
PIA	Privacy Impact Assessment

SAVE	Systematic Alien Verification for Entitlements
SOR	state of record
SSN	social security number
TSA	Transportation Security Administration
UKPS	U.K. Passport Service
WHTI	Western Hemisphere Travel Initiative

## EXECUTIVE SUMMARY

Since September 11, 2001, many governments have considered developing national identity management systems. Beyond identification, politicians and proponents of these systems have touted such system benefits as combating terrorism, preventing identity theft, facilitating travel, and combating illegal work and benefit fraud. For these reasons, the United States and United Kingdom both considered variations of these systems. While the United Kingdom passed the Identity Cards Act 2006, and spent several years developing a national identity management system before ultimately scrapping the scheme in 2010, the United States sought to further secure the existing means of identification—driver’s licenses and identity cards—through the passage of the REAL ID Act. However, significant backlash has resulted from state governments in implementing the requirements of the Act.

The question this thesis explores is what does a comparative examination of resistance to nationwide identity management schemes in the United States and United Kingdom reveal about the nature of national identity management systems and identity cards? What does this resistance tell policymakers and security officials who promote such schemes?

The literature suggests that a variety of terms is used to describe national identity management. While the terms “identity cards” and “identity management systems” have been favored, these terms have complex definitions and assumptions associated with them. For this reason, a number of opinions have been proffered about whether the REAL ID-compliant driver’s licenses and identity cards constitute a national ID card or could be considered part of a national identity management system. The variation in terminology obscures the fact that identity cards that are national in scope face the same problems and issues as those experienced by national identity management systems. Through a comparative analysis of the REAL ID Act implementation and the National Identity Scheme, this thesis shows that Anglophone, common-law nations experience the same inhibiting factors, whether or not they attempt to implement a national identity management system or an identity card on a national scale.

Advocacy groups, academics, and even politicians have objected to parts of both schemes based on similar purpose, privacy, and civil rights and civil liberties concerns. They warned that the schemes might not be able to fulfill their proposed purposes and have expressed concern over a variety of privacy issues, including the potential for function creep, the security and integrity of data collected for the schemes, the implications of linking databases together, and the effects of increased collection and sharing of data. Advocacy groups and academics also expressed concern over the potential for increased civil rights and civil liberties violations based on the data collected. They worried that the schemes could plausibly increase racial profiling and discrimination, through stops and searches or through the possible inclusion of race on the identity cards in the United States, where the cards' lack of encryption creates the risk that commercial entities could collect and use personal data. Furthermore, the concern that the nationwide use of identity cards fosters a surveillance society, and facilitates the practices of data mining and profiling, is shared by groups in the United States and United Kingdom.

Academics in the United States and United Kingdom asserted similar concerns regarding the development of their respective legislation. They believed that the process was either too accelerated to allow for public debate or that it was flawed, as the design and functional components of the scheme had been decided up front. Both schemes have similarly high levels of public acceptance, until it is brought to the attention of the participants how the schemes will actually function. Finally, the United States and United Kingdom have similar inclinations to reject identity management schemes, identity cards, or identifiers based on a varied history of associated personal privacy and civil liberties concerns.

The parallel inhibiting factors experienced by both schemes demonstrate that while some do not consider the United States' REAL ID Act to be a national identity management system—and thus may not think of REAL ID-compliant driver's licenses and identity cards as national ID cards—the nomenclature used to describe the policy does not matter when it comes to issues surrounding identity management that must be negotiated and overcome. Whatever the name, whatever the architecture, government

systems built to identify the citizenry of a national will face significant resistance. United States policymakers must consider the inhibiting factors that face national identity management schemes in Anglophone, common-law nations when implementing nationwide identity cards, lest they fall into the trap of believing that the same issues will not appear. Only with this foresight in mind, will the United States be able to formulate and sustain lasting identity management policy.

THIS PAGE INTENTIONALLY LEFT BLANK

## ACKNOWLEDGMENTS

I am deeply thankful to the professors and staff of the Naval Postgraduate School Center for Homeland Defense and Security. You have truly challenged me to think in new ways and have expanded my mind. I would especially like to thank my committee, Dr. Carolyn Halladay and Dr. Nadav Morag, for their support and assistance. Your guidance has made my thesis journey possible.

I would like to express thanks to the Office of Biometric Identity Management, specifically my branch chief, Lisa MacDonald, and my immediate supervisor, Sarita Rijhwani, whose support allowed me to succeed in this program, as well as my colleagues, who have encouraged me throughout the process.

Thank you to my cohort, who is both smart *and* good-looking. You have all made this experience more amazing than I ever thought it could be. You have challenged me and helped me grow both as an individual and as a professional. I deeply cherish your friendship, guidance, and support.

I would also like to thank my family and friends for all of their support through this process. They have been my cheerleaders, my editors, my sanity checkers, and my advisors. Most of all, none of them ever doubted me, and that conviction made me believe in myself. For that, you have my most sincere gratitude.

I could not have succeeded in this program without the support of my husband, Phill, who has been my champion and motivator throughout this journey. It has not been easy, but you have kept me alive with my sanity intact. Without you, this would not have been possible.

THIS PAGE INTENTIONALLY LEFT BLANK

## **I. INTRODUCTION**

A country's ability to identify its citizens has always been important to modern governments, but the issue has become much more pressing in the Internet age, when a person's digital identity can be a primary method of obtaining goods and services from—and access to—both private and public organizations.

Particularly since September 11, 2001, many governments have considered developing national identity management systems. Beyond identification, politicians and proponents of these systems have touted such benefits as combating terrorism, preventing identity theft, facilitating travel, and combating illegal work and benefit fraud. For these reasons, the United States (U.S.) and United Kingdom (U.K.) both considered variations of these systems. The United Kingdom passed the Identity Cards Act of 2006 and spent the next four years developing a national identity management system before ultimately scrapping the scheme in 2010. In contrast, the United States considered developing such a system, but ultimately decided not to. Instead, the United States sought to further secure the existing means of identification—driver's licenses and identity cards—through the passage of the REAL ID Act. Still, privacy and civil liberties advocates and some academics have characterized this measure as tantamount to the creation of a de-facto national identification card for the United States. Opponents of national identity management systems have responded in a similar sentiment.

### **A. RESEARCH QUESTION**

The question this thesis is seeking to answer is what does a comparative examination of resistance to nationwide identity management schemes in the United States and United Kingdom reveal about the nature of national identity management systems and identity cards? What does this resistance tell policymakers and security officials who promote such schemes?

The answer to these questions will help to explain why the United States is experiencing backlash from state governments in implementing the requirements of the REAL ID Act. To answer the question, this thesis explores the inhibitors for the U.S.'

REAL ID Act implementation, as well as arguments against the U.K.'s National Identity Scheme (NIS) that ultimately prevented its implementation.

## **B. PROBLEM STATEMENT**

Discussions of national identity management systems in the United States and United Kingdom were invigorated after September 11 as a way to prevent and combat terrorism. These common-law countries, which share similar security concerns, believed, at least for a while, that a national identity management system would mitigate some of the threats facing the countries. For example, 13 of the terrorists and conspirators responsible for the September 11 attack had fraudulently obtained ID cards, and four of the hijackers boarded the planes they later took control of using U.S. driver's licenses.<sup>1</sup>

In addition to increased security, both countries also identified other benefits of a national identity management system. For example, a single identification card would prevent an individual from obtaining duplicate identifying documents. This measure, in turn, could reduce benefit fraud by preventing individuals from applying for assistance multiple times. It also might stop employment fraud by preventing undocumented immigrants from accepting jobs. Additionally, in the United Kingdom, a system was promoted as a way to facilitate easier delivery of services to citizens. No longer would a citizen have to apply for benefits and services in multiple places; the national identity management system would allow information to be shared across departments and agencies. These benefits, combined with the potential to increase security, made national identity management systems an attractive solution to the increasing terrorist threat.

The United Kingdom began work on an identity management system in 2006. Throughout the system's development, the government faced criticism from academia, as

---

<sup>1</sup> *Joint Hearing Before The Subcommittee on Immigration, Border Security, and Claims and The Subcommittee on Crime, Terrorism, and Homeland Security of The Committee on The Judiciary House of Representatives, Risk to Homeland Security from Identity Fraud and Identity Theft*, 107th Congress, 2 (2002), 2; Anna Ya Ni and Alfred Tat-Kei Ho, "A Quiet Revolution or a Flashy Blip? The Real ID Act and U.S. National Identification System Reform," *Public Administration Review* 68, no. 6 (2008): 1069; Nawaf al Hazmi and Khalid al Mihdhar obtained driver's licenses in California, while Mohamed Atta and Ziad Jarrah obtained licenses in Florida. National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* (Washington, DC: National Commission on Terrorist Attacks upon the United States, 2004), 220, 231.

well as privacy and civil rights advocates, for a variety of reasons related to cost, technology, privacy, and security. This criticism continued until the scheme was disbanded in 2010.

In contrast, the United States chose not to implement a national identity management system. Instead, based on a 9/11 Commissions Report recommendation, the government sought to strengthen driver's licenses to increase their security and integrity. Since its passage in 2005, the REAL ID Act has faced significant resistance, and implementation has been wrought with political battles. As a result, the timeline for enforcing state compliance with the requirements of the Act has been repeatedly delayed and the requirements themselves reduced.

While a significant amount of scholarly analysis of the U.K. identity management system and its dissolution is available, the U.S. forays into national identity management discourse have been studied less. Further, little comparative analysis of nationwide identity management systems beyond those established in continental Europe has been conducted. This thesis contributes to a greater understanding of the principles held by common law countries, as well as the cultural differences that make each country's analysis and decisions regarding national identity management unique. It also delves into the ambiguity in the literature about the differences between national identity management systems and identity cards, and how that ambiguity manifests itself when it comes to policy implementation.

### **C. LITERATURE REVIEW**

The literature review introduces the nomenclature used when discussing national identity management systems, different models for how identity management systems can be organized, and different architecture for how identity management systems can be structured. This information provides a foundation for further discussion of the U.S. and U.K. identity management schemes explored in Chapter II.

## 1. Identity Management System Nomenclature

The relevant literature uses a myriad of terms to designate national identity management, most commonly national identity management system, or national ID cards. Many scholars fail to define these terms in their articles, assuming that the reader understands what these are and how they function in a greater context. However, a level of ambiguity surrounds what these terms actually mean. With the variety of different descriptors, it is not easy for the reader to discern the difference or similarities between the terminologies. In the book, *IDs—Not That Easy: Questions about Nationwide Identity*, authors Kent and Millett summarize this lack of clarity:

There is no recognized universal model for a nationwide identity system. Because different people mean different things when they discuss the concept, evaluating it requires clarification of what is intended. The range of possibilities for identity systems is broad and includes alternative approaches.<sup>2</sup>

Delving into the different terminology yields insights into the parameters of discourse surrounding national identity management. Kent and Millett intentionally favor the unique phrasing of “nationwide identity system.” They explain the intentional use of term “nationwide” instead of “national” so that the word indicates the scope of the system, without misleading the reader in terms of the scope of the population within the database, which may extend beyond citizens. Further, they explain that “system,” in this context, “implies linking together of many social, legal, and technological components in complex and interdependent ways.”<sup>3</sup> This definition comes without entering into a discussion of the technical architecture.

Kent and Millett specifically define approaches to a nationwide identity system in terms of the scope of the population included. With a U.S.-centric view, they state that approaches to a system could include information solely on U.S. citizens, non-citizens, or just parts of the country’s population.<sup>4</sup> Further parameters used to define an identity

---

<sup>2</sup> Stephen T. Kent and Lynette I. Millett, *IDs—Not that Easy: Questions about Nationwide Identity Systems* (Washington, DC: National Academy Press, 2002), 8.

<sup>3</sup> *Ibid.*, 11–13.

<sup>4</sup> *Ibid.*, 8–9.

system are the purpose of the system, the scope of the data, the user(s) of the system, the types of uses, whether it would be voluntary or mandatory, and the legal structures.<sup>5</sup>

Another unique, and more commonly European descriptor for national identity management, is “national identification scheme” (NIDS), used by authors Clement, Guerra, Johnson, and Stalder. This terminology refers to systems defined by their architectural designs, which may include identity cards, databases, identifiers, and/or biometrics.

Alternatively, scholars Kubicek and Noack use the terms “electronic identity” (eID) and “eID Management Systems” (eIDMS) in their analysis of the systems within eight different European countries that planned to use IDs for “online authentication for e-government services [services offered by the government over the Internet] based on a national ID card or a similar chip-card.”<sup>6</sup> They define an eID as identifiers “registered in national citizen registries based on a particular legislation and produced and distributed within an eID eIDMS operated by different agencies.”<sup>7</sup> Their review of the systems provides insight into an interesting limitation of defining characteristics of national eIDs on a broader scale:

The only common feature of the national eIDs in the eight countries is their organization from the national citizen registries, based on an obligation to register for every citizen by birth.<sup>8</sup>

Many of the differences identified between the different country’s systems related to eID issuance and technical design. Kubicek and Noack found that banks, rather than the government, issued the eIDs in four of the northern European countries analyzed, primarily because those countries demonstrated a much higher trust in the privacy provided by the banking system.<sup>9</sup> They also found that some countries had central

---

<sup>5</sup> Kent and Millett, *IDs—Not that Easy: Questions about Nationwide Identity Systems*, 9–11.

<sup>6</sup> Herbert Kubicek and Torsten Noack, “Different Countries-Different Paths Extended Comparison of the Introduction of eIDs in Eight European Countries,” *Identity in the Information Society* 3, no. 1 (2010): 236.

<sup>7</sup> *Ibid.*

<sup>8</sup> *Ibid.*, 237.

<sup>9</sup> *Ibid.*, 240, 242.

“registers,” or databases, rather than local registers, among other architectural differences. Almost in an acknowledgement of the unique terminology of eID and eIDMS, and despite using neither term, Kubicek and Noack’s article includes the keywords: “identity cards” and “identity management systems,” illustrating the ubiquity of this phraseology.

Legal professor Daniel J. Steinboch favors the term “national identity cards” in his article, “Fourth Amendment Limits on National Identity Cards,” acknowledging that they would likely be the heart of a U.S. national identity management system. This assertion in itself reveals a level of understanding about how identity cards fit within a greater system, while not necessarily being a required piece of the design. Steinboch describes national identity systems in the context of their most basic purpose—human identification—and relies on the definition created by scholar Richard Clarke: “[H]uman identification is the association of data with a particular human being.”<sup>10</sup>

Steinboch further acknowledges that a national identity management system relies on particular design elements to function: “Any such system, however, depends on two major features: the database (or databases) containing information about particular individuals and the means to connect a given person with that information.”<sup>11</sup>

## **2. Identity Management System Models**

The terminology associated with national identity management outlined previously has relied on some combination of structure or design of the system, the scope of population within the system, and/or the function of the system. However, in addition to simply defining the overarching terms for these schemes, academics have developed different models to differentiate identity management schemes. Academic scholars, Ya Ni and Tat-Kei Ho, conduct a comparison between a centralized, data clearinghouse, or federated approach to identity management reform in the United States, as opposed to the

---

<sup>10</sup> Richard Clarke, “Human Identification in Information Systems: Management Challenges and Public Policy Issues,” *Information Technology & People* 4, no. 7 (December 1994), 6–37, <http://www.rogerclarke.com/DV/HumanID.html>.

<sup>11</sup> Daniel J. Steinboch, “Fourth Amendment Limits on National Identity Cards,” in *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*, ed. Katherine J. Strandburg and Daniela Stan Raicu (New York: Springer U.S., 2006), 297.

current REAL ID framework. A centralized approach would consist of a national ID card and a single database “controlled by a central authority,” which would be the federal government.<sup>12</sup> Ya Ni and Tat-Kei Ho describe this approach as one taken by many European and Asian countries.<sup>13</sup> The data clearinghouse approach entails developing interoperability, “the ability of two or more systems or components to exchange information and to use the information that has been exchanged,” between existing state and federal databases, coupled with a single federal data-clearing house.<sup>14</sup> The federated approach involves standardizing existing state driver’s license systems, while allowing the states to manage their own systems.<sup>15</sup>

In a more generic approach, Miriam Lips describes an identity management system schema entirely based on who manages the data. The identity management system can either be organization-centric, in which a service provider manages the data, or user-centric, in which the user manages their own data.<sup>16</sup> Similarly, researchers Hansen et al. describe two models that are also based on data management. One model is the centralized identity model, in which the identity management system manages a user’s identity for them.<sup>17</sup> The other model is the federated identity model, in which either no single identity management provider exists or the users manage their own identity.<sup>18</sup>

Another set of researchers, Halperin and Backhouse and Fritsch, Fuglerud, and Solheim, describe identity management systems identified during the Future of Identity in the Information Society (FIDIS) European research project based on use and user control.

---

<sup>12</sup> Anna Ya Ni and Alfred Tat-Kei Ho, “A Quiet Revolution or a Flashy Blip? The Real ID Act and U.S. National Identification System Reform,” *Public Administration Review* 68, no. 6 (2008): 1065.

<sup>13</sup> *Ibid.*

<sup>14</sup> *Ibid.*, 1066; The Institute of Electrical and Electronics Engineers, *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries* (New York: The Institute of Electrical and Electronics Engineers, 1991), 114.

<sup>15</sup> Ya Ni and Tat-Kei Ho, “A Quiet Revolution or a Flashy Blip? The Real ID Act and U.S. National Identification System Reform,” 1067.

<sup>16</sup> Miriam Lips, “The Quest for Managing Identity Management,” *Online Information Review* 33, no. 3 (2009).

<sup>17</sup> Marit Hansen et al., “Privacy-Enhancing Identity Management,” *Information Security Technical Report* 9, no. 1 (2004): 41.

<sup>18</sup> *Ibid.*

They found that three different types of existing identity management systems are on the market today: identity management systems (IdMS) for accounting or account management, IdMS for profiling, and user-controlled IdMS.<sup>19</sup>

### **3. Identity Management System Architecture**

Amid the swirl of names, notions, and models of national identity management, the literature really boils down to discussions of either a card or a system. For the purpose of this thesis, cards and systems, collectively, are referred to as the primary identity management schemes. Articles using system terminology usually describe an identity management architecture involving an identity card and a centralized database, although it is not necessarily the only way a system can be designed. A card and database was the design of the U.K.'s scheme until it was repealed.

The other way national identity management architecture is conceptualized is simply based on identity cards. This architecture does not always involve centralized databases. Often, the identity card is discussed as being may be voluntary or mandatory, and can be administered and mandated by the nation or by federated states, which have some degree of governmental authority and reserved powers.

The problem with the dichotomy that appears in the literature is that it obscures the fact that identity management schemes can be structured using a variety of different components. Kent and Millett state:

An idea that has resurfaced as a result of the [September 11th] attacks is the creation of a “national identity card,” often referred to simply as a “national ID.” This term is a bit of a misnomer, in that a card would likely be but one component of a large and complex nationwide identity system, the core of which could be a database of personal information on the U.S. population.

While Kent and Millett note the intersections that exist between an identity card and an identity management system, the majority of the literature is not entirely clear where that overlap exists. Cards can be a part of a system, but they are often divorced

---

<sup>19</sup> Ruth Halperin and James Backhouse, “A Roadmap for Research on Identity in the Information Society,” *Identity in the Information Society* 1, no. 1 (2008): 77.

from their connection to information systems in the literature. The term “information system” may be referring simply to a computer system or more broadly to the interconnecting system of people and technology that allows information to be shared.<sup>20</sup> The literature may refer to the inherent issues with identity cards or the problems that can be found in identity management systems, but it is not always clear in individual articles what elements constitute each design. While a system is often thought of as a database, ultimately, ID cards are part of a system. They both involve a number of interconnected design elements that make them function.

Simplifying the design elements of both an ID card and an identity management system would include:

- *An Identifier*—A unique number belonging to a single individual or a biometric: “a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition.”<sup>21</sup>
- *Database*—The infrastructure where an identifier or biometric, as well as other personal data, may or may not be stored. The data can either be centralized in one single repository, or separated into different repositories that may be connected through interoperability.
- *Physical Token*—An object on which an identifier or biometric may or may not be held or displayed. An example would be an identity card.

In addition to these strictly architectural components, the model can either be voluntary or mandatory.

These elements can be combined into a number of different combinations, as described by Clement et al. in their paper on “National Identification Schemes,” depending on whether the physical token (ID card) is required to be presented, and what data is on the ID card and/or in the database.<sup>22</sup> Some of the combinations include:

---

<sup>20</sup> Bernd Hornung, “Information System,” Principia Cybernetica Web, accessed August 15, 2015, [http://pespmc1.vub.ac.be/ASC/INFORM\\_SYSTE.html](http://pespmc1.vub.ac.be/ASC/INFORM_SYSTE.html).

<sup>21</sup> “Biometrics Glossary,” accessed January 12, 2015, <http://www.biometrics.gov/Documents/Glossary.pdf>.

<sup>22</sup> Andrew Clement et al., “National Identification Schemes (NIDS),” in *Human Choice and Computers: Issues of Choice and Quality of Life in the Information Society*, ed. Klaus Brunnstein and Jacques Berleur, vol. 98 (Boston, MA: Springer US, 2002), 198.

- *Unique identifier (identity number), no physical token (no ID card), and database*

In this design, a unique ID number is assigned to an individual for identification purposes. That number is also maintained in a database, which is currently how the Social Security Number (SSN) is structured within the United States. The paper card is not considered a physical token, per say, since the use of the card is not required in this model.

- *Unique identifiers (identity number and biometrics), physical token (ID card), and centralized database*

In this design, the ID number and biometrics are maintained both in and on the ID card and in the database, which is how the U.K. NIS was to be structured. It would have consisted of a unique identifier (the National Identity Registration Number), and ID card with an encrypted chip inside that would hold the biometrics, and a central database called the “National Identity Register.”<sup>23</sup>

---

<sup>23</sup> “Identity Cards Scheme Will be Axed ‘within 100 Days’,” last updated May 27, 2010, <http://news.bbc.co.uk/2/hi/8707355.stm>; *Identity Cards Act 2006, Chapter 15*, Section 2, Sub-section 27, 2006, <http://www.legislation.gov.uk/ukpga/2006/15/notes/division/5/1/2>.



- *Unique identifier (identity number), physical token (ID card), and separate databases*

The identity number may appear on the ID card and in the database, which is how the driver's license is structured in the United States. Each individual who receives a license is assigned a unique license number that is printed on a card and maintained in the state's Department of Motor Vehicles (DMV) database.

#### **D. RESEARCH DESIGN/METHODOLOGY**

This thesis proves that Anglophone, common-law nations experience the same inhibiting factors, whether or not they attempt to implement a national identity management system or a nationwide identity card, by conducting a comparative case study of the inhibiting factors and tensions pertaining to REAL ID compliant driver's license and identity cards in the United States, as mandated by the REAL ID Act, and the NIS in the United Kingdom. It explores the reasons why the United States and the United Kingdom experienced opposition to the implementations to these efforts. The United Kingdom was chosen for this research because of its similar legal system, language, and dedication to protecting the privacy and civil liberties of its citizens.

This thesis includes a qualitative analysis to identifying common themes using primary and secondary source documents including testimony from congressional hearings on the REAL ID Act; public consultation documents regarding the U.K. identity card; legislative publications for both the United Kingdom and the United States; academic studies and academic journal articles discussing identity management architectures, technology, privacy, and public acceptance and attitudes towards both identity management systems and ID cards; articles that conduct comparisons of national identity management systems and analysis of the U.K. and U.S. legislation and their implementation; and white papers and press releases authored by advocacy groups. These sources help to trace the primary reasons for the countries' aversion to developing identity management schemes.

The scope of this research does not include a discussion of national identity management systems not directly related to these two countries. This thesis does not evaluate the effectiveness of a system at achieving the proposed purposes, nor does it

analyze the validity of the arguments against a national identity scheme. It does not include a comprehensive legal analysis. A full review of all identity documents used by the countries over the course of their history also is outside of the scope of this analysis.

## **E. CHAPTER OUTLINE**

The second chapter provides an in-depth look at both the REAL ID Act and the Identity Cards Act of 2006. The requirements of both Acts are described, as well as the associated statutory purposes. In addition, a discussion of what both schemes constitute in terms of a national identity management system, a national ID card, both, or neither.

The third chapter begins comparing opposing arguments to both the REAL ID Act implementation and the National Identity Scheme. It provides a comparison of the policy and privacy issues. The fourth chapter compares civil rights and civil liberties issues voiced by advocacy groups, politicians, and academia.

The fifth chapter provides a comparison of the issues involved in public engagement and government transparency, as well as a discussion of the levels of public acceptance. Finally, it provides a comparison of the cultural and historical factors that inform current identity management system approaches.

The thesis concludes with a discussion of the implications of the comparative analysis and how it impacts policymakers.

THIS PAGE INTENTIONALLY LEFT BLANK

## **II. UNITED STATES AND UNITED KINGDOM'S IDENTITY MANAGEMENT SCHEMES**

This chapter outlines the United States' REAL ID Act, specifically what is required by the law and the purposes for the creation of the legislation. The chapter then provides an overview of the various competing schools of thought on what the legislation means in terms of national identity management. It explores arguments as to whether or not the REAL ID Act constitutes a national identity management system, a national identity card, both, or neither. The chapter also provides an overview of the United Kingdom Identity Cards Act. It explains the components of the legislation, as well as its intended purposes. This section of the chapter also covers the general views on whether or not the scheme is a national identity management system, a national identity card, both, or neither.

The purpose of this chapter is to provide the necessary background on the legislation of both countries, the implications of which are explored in later chapters.

### **A. UNITED STATES—REAL ID ACT**

Following the terrorist attack on September 11, 2001, The National Strategy for Homeland Security, released in 2002 by the Bush Administration, recommended the development of minimum standards for driver's licenses by the states.<sup>24</sup> Two years later, *The 9/11 Commission Report* included a recommendation for secure identification standards established by the federal government:

Secure identification should begin in the United States. The federal government should set standards for the issuance of birth certificates and sources of identification, such as drivers licenses. Fraud in identification documents is no longer just a problem of theft. At many entry points to vulnerable facilities, including gates for boarding aircraft, sources of

---

<sup>24</sup> The White House, *National Strategy for Homeland Security* (Washington, DC: Office of Homeland Security, 2002), 49.

identification are the last opportunity to ensure that people are who they say they are and to check whether they are terrorists.<sup>25</sup>

In December 2004, President Bush signed into law the Intelligence Reform and Terrorism Prevention Act, or the National Intelligence Reform Act, in response to the September 11 attacks. The Act required that “the Secretary of Transportation, in consultation with the Secretary of Homeland Security, shall by regulation, establish minimum standards for driver’s licenses or personal identification cards [generally, ‘ID cards’] issued by a State for use by Federal agencies for identification purposes.”<sup>26</sup> Before publishing regulations, the Secretary of Transportation was required to establish a negotiated rulemaking committee to include state representatives. The Act required federal agencies to stop accepting non-compliant licenses and ID cards two years after the standards were promulgated. Additionally, the Secretary of Transportation was required to provide grants to the states to facilitate their compliance with the requirements. It also amended the Social Security Act to prevent SSNs from being displayed on driver’s licenses or ID cards, and prohibits them from being included within machine-readable technology (MRT), such as a magnetic strip or bar code.<sup>27</sup>

In May 2005, the REAL ID Act was signed into law as part of the Emergency Supplemental Appropriation for Defense, the Global War on Terror, and Tsunami Relief Bill. The Act maintained the same requirements for minimum standards, but added provisions for document and immigration status checks, provided more detail and guidance on implementation, and repealed specific sections (as discussed in the following sections).

---

<sup>25</sup> National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*, 390.

<sup>26</sup> *Intelligence Reform and Terrorism Prevention Act of 2004*, Pub. L. No. 108-458, 118 Stat. 3638 (2004).

<sup>27</sup> *Ibid.*

## **1. REAL ID Act Overview**

The REAL ID Act has a number of stipulations for document requirements, issuance requirements, and requirements relating to the security of the data and documents, among others. These requirements are further explained in this section.

### ***a. Document Requirements***

The Act required that the following minimum data elements appear on all driver's licenses and ID cards that would be accepted for federal use:

- The person's full legal name
- The person's date of birth
- The person's gender
- The person's driver's license or personal identification card number
- A digital photograph of the person
- The person's address of principal residence
- The person's signature<sup>28</sup>

The Act required the following technology and security features be included on the cards:

- Physical security features designed to prevent tampering, counterfeiting, or duplication of the document for fraudulent purposes
- A common MRT, the card must not extend longer than eight years and cards that do not meet the specified standards must have a "unique design or color," as well as explicitly state "on [the] face [of the card] that it may not be accepted by any Federal agency for federal identification or any other official purpose."<sup>29</sup>

### ***b. Issuance Standards***

In addition to the document requirements, the Act mandates a series of standards required for issuing the licenses or identity cards. An applicant for a license or card must

---

<sup>28</sup> *Emergency Supplemental Appropriations Act for Defense, The Global War on Terror, and Tsunami Relief*, 2005, Pub. L. No. 109-13, 109th Cong.

<sup>29</sup> *Ibid.*

present the following documents, which the state must confirm the authenticity of by verifying their validity with the issuing agency:

- (A) A photo identity document, except that a non-photo identity document is acceptable if it includes both the person's full legal name and date of birth.
- (B) Documentation showing the person's date of birth.
- (C) Proof of the person's social security account number or verification that the person is not eligible for a social security account number.
- (D) Documentation showing the person's name and address of principal residence.<sup>30</sup>

The Act requires states to validate that applicants are lawfully present in the United States to prevent illegal immigrants from receiving a driver's license. To do so, state DMVs must agree check the Systematic Alien Verification for Entitlements (SAVE) system for legal status of all applicants who are not U.S. citizens.<sup>31</sup> They must only issue temporary licenses and ID cards to these individuals, with an expiration date that corresponds to their authorized length of stay. The expiration date and the fact that the card is temporary must be clearly visible on the card.

*c. Other Requirements*

The Act contains a series of other requirements relating to security standards, data retention, employee training, and motor vehicle databases.

- *Security*—Two additional security requirements are that the location where the cards are produced must be physically secure and the materials used to create them must also be protected. Individuals who manufacture the cards must undergo a security clearance.
- *Retention*—The Act requires the retention of the physical copies of source documents and that a facial photo be captured for each applicant and stored in a transferable format.

---

<sup>30</sup> *Emergency Supplemental Appropriations Act for Defense, The Global War on Terror, and Tsunami Relief.*

<sup>31</sup> While many states call the agency that conducts vehicle registrations and issues driver's licenses a Department of Motor Vehicles (DMV), it is not true of all states. Some referred to this agency as a bureau, office, or division. For clarity, this thesis refers to all state agencies as DMVs.

- *Training of Employees*—The Act requires that states establish trainings to enable employees to recognize fraudulent documents.
- *Motor Vehicle Databases*—The Act requires that all states must “maintain a State motor vehicle database that contains, at a minimum, all data fields printed on drivers’ licenses and identification cards issued by the State” and drivers’ histories (which must include “motor vehicle violations, suspensions, and points on licenses”). States must then have “electronic access” to each other’s databases.<sup>32</sup>

The Act repealed the requirement that the Secretary of the Department of Homeland Security (DHS) issue grants to states to relieve some of their monetary burden. Instead, the issuance of grants is now at the Secretary’s discretion. Finally, the Act repealed the requirement for a negotiated rulemaking committee. Now, the “authority to issue regulations, set standards, and issue grants” belongs to the Secretary of Homeland Security, “in consultation with the Secretary of Transportation and the States.”<sup>33</sup> The Secretary of Homeland Security is also responsible for determining when states have met the requirements and issuing them a certificate to show that they have done so. States were required to comply with the requirements by May 11, 2008; after that date, federal facilities would no longer accept non-compliant driver’s licenses and ID cards for official uses, to include “accessing Federal facilities, entering nuclear power plants, and boarding federally-regulated commercial aircraft.”<sup>34</sup>

DHS published a Notice of Proposed Rulemaking in the Federal Register in March 2007 asking for public comment on their proposed regulations.<sup>35</sup> This publication occurred two years after the Act was passed in May 2005 and it generated significant concerns from the states, which were required to comply with the Act by May 2008, but

---

<sup>32</sup> *Emergency Supplemental Appropriations Act for Defense, The Global War on Terror, and Tsunami Relief.*

<sup>33</sup> *Ibid.*

<sup>34</sup> *Ibid.*, “REAL ID Frequently Asked Questions for the Public,” accessed June 11, 2015, <http://www.dhs.gov/real-id-public-faqs>.

<sup>35</sup> *Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*, 72 Fed. Reg. 10820–10858 (March 9, 2007).

still did not have the final requirements from DHS.<sup>36</sup> Ten months later, the Final Rule was promulgated on January 2008, instructing the states in specific requirements that they would need to implement to comply with REAL ID regulations.<sup>37</sup> It established a May 11, 2011 deadline for compliance. DHS later expanded the compliance date to January 15, 2013.<sup>38</sup> Since then, DHS has granted extensions annually to states that have shown continued progress towards compliance. A revised Final Rule was published on December 29, 2014 that changes the deadline for “document enrollment” to October 1, 2020.<sup>39</sup> This phrase refers to the date after which federal agencies will no longer accept for official purposes a driver’s license or identification card that is not REAL ID compliant and is not issued by a certified state.

*d. REAL ID Act Purpose*

The REAL ID Act states that the official purpose of REAL ID compliant driver’s licenses and identification cards, “includes but is not limited to accessing Federal facilities, boarding federally regulated commercial aircraft, entering nuclear power plants, and any other purposes that the Secretary shall determine.”<sup>40</sup> DHS considers the REAL ID Act a useful tool in fighting terrorism. As stated in the Proposed Rulemaking for the Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes,

The primary benefit of REAL ID is to improve the security and lessen the vulnerability of federal buildings, nuclear facilities, and aircraft to terrorist attack. The rule would give states, local governments, or private sector

---

<sup>36</sup> Jim Harper, “Testimony regarding SB 262 and the U.S. Federal REAL ID Act: Committee on Transportation New Hampshire State Senate,” CATO Institute, accessed June 23, 2015, <http://www.cato.org/publications/testimony/testimony-regarding-sb-262-us-federal-real-id-act>.

<sup>37</sup> Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 73 Fed. Reg. 5272–5340 (January 29, 2008).

<sup>38</sup> Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 76 Fed. Reg. 12269–12271 (March 7, 2011).

<sup>39</sup> Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 79 Fed. Reg. 77836–77838 (December 29, 2014).

<sup>40</sup> *Emergency Supplemental Appropriations Act for Defense, The Global War on Terror, and Tsunami Relief*.

entities an option to choose to require the use of REAL IDs for activities beyond the official purpose defined in this regulation.<sup>41</sup>

While not considered official purposes, a wide range of ancillary benefits the government expects to see includes:

- Reducing identity theft
- Reducing unqualified driving
- Reducing fraudulent access to government subsidies and welfare programs
- Reducing illegal immigration
- Reducing unlawful employment
- Reducing unlawful access to firearms
- Reducing voter fraud
- Possibly reducing underage drinking and smoking<sup>42</sup>

The federal register notice also notes—in regards to the official purpose—that, “DHS, under the discretionary authority granted to the Secretary of Homeland Security under the Act, may expand this definition in the future.”<sup>43</sup>

## **2. What Is the REAL ID: A National Identity Management System, a National ID Card, or Neither?**

In the United States, literature on the REAL ID compliant driver’s licenses and identity cards indicates a range of opinions on the Act’s role in national identity management. Some authors assert that the REAL ID is a national ID system, while others state that the REAL ID has created a “de facto” national identity card or a “de facto” national identification scheme, national identity system, or nationwide identity system. Still others say that REAL ID does not constitute a system, but is paving the way for one

---

<sup>41</sup> Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 72 Fed. Reg. 10845 (March 9, 2007).

<sup>42</sup> Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 72 Fed. Reg. 10846 (March 9, 2007).

<sup>43</sup> Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 72 Fed. Reg. 10823 (March 9, 2007).

to appear in the future. Finally, some state that the REAL ID is not a system, nor will it facilitate the creation of any future system.<sup>44</sup>

**a. *The REAL ID Is Not a National ID Card or a National Identity Management System***

The government is the primary voice stating that the REAL ID driver's license and identity card is not part of a national identity management system. The DHS REAL ID Frequently Asked Questions for the public specifically addresses this question. It states:

REAL ID is not a national identification card. States and territories will continue to issue driver's licenses and identification cards, and there is no Federal database of driver information. Each jurisdiction will issue its own unique license and maintain its own records.<sup>45</sup>

This statement is in line with the Homeland Security Act of 2002, which created DHS. It explicitly stated that the agency was not authorized to create a system or card:

SEC. 1514. NATIONAL IDENTIFICATION SYSTEM NOT AUTHORIZED.

Nothing in this Act shall be construed to authorize the development of a national identification system or card.<sup>46</sup>

When asked at the Transatlantic Homeland Security Conference in September 2004, Secretary of Homeland Security Tom Ridge stated that the Department would not develop a national ID card. He elaborated that, "The legislation that created the Department of Homeland Security was very specific on the question of a national ID card. They said there will be no national ID card."<sup>47</sup> However, Secretary Ridge mentioned the Department was working with state governors to create standards for driver's licenses, as they are "probably the most frequently reached for form of

---

<sup>44</sup> *Homeland Security Act of 2002*, Pub. L. No. 107-296, 116 Stat. 2135 (2002); Department of Homeland Security, *REAL ID Frequently Asked Questions for the Public*.

<sup>45</sup> "REAL ID Frequently Asked Questions for the Public."

<sup>46</sup> *Homeland Security Act of 2002*.

<sup>47</sup> Tom Ridge, "Transcript of Secretary of Homeland Security Tom Ridge at the Center for Transatlantic Relations at Johns Hopkins University 'Transatlantic Homeland Security Conference'," Department of Homeland Security, accessed August 10, 2015, <https://www.hsdl.org/?view&did=475404>.

identification.” He explained, “We are constrained from developing a national ID card, but not constrained from trying to develop some just basic standards, that regardless of the kind of card you issue -- transportation worker, nuclear worker, federal employee -- there will be some basic information on it that we can all refer to and consider as reliable.”<sup>48</sup> It is clear from the Secretary’s remarks that the Department considers a national identity card to be one issued by the federal government. Cards issued individually by the states, but requiring the same data, would not be considered national identity cards in the government’s eyes.

***b. The REAL ID Is Not a National Identity Card, but May Lead to a National Identity Management System***

Some academics and civil rights advocacy groups express the view that REAL ID driver’s licenses and identity cards are not national identity cards, but may lead to a national identity system.<sup>49</sup> In her overview of the debate surrounding the REAL ID Act and voter identification, J.D. Candidate Debra Milberg states, “REAL ID pushes the nation one step closer to a national identification card that requires personal information to be stored in a central database.”<sup>50</sup> Expressing a similar sentiment, during the 2007 hearing on the REAL ID Act and Western Hemisphere Travel Initiative (WHTI), American Civil Liberties Union Washington Legislative Office Director Caroline Fredrickson noted her view of the options facing Congress for the future of the REAL ID Act:

---

<sup>48</sup> Ridge, “Transcript of Secretary of Homeland Security Tom Ridge at the Center for Transatlantic Relations at Johns Hopkins University ‘Transatlantic Homeland Security Conference’.”

<sup>49</sup> Debra Milberg, “National Security Surveillance and National Authentication System: The National Identification Debate: “REAL ID” and Voter Identification,” *I/S: A Journal of Law & Policy for the Information Society* 3, no. 3 (Winter 2007), 443–472; *Oversight of Government Management, the Federal Workforce, and the District of Columbia Subcommittee of the Committee on Homeland Security and Governmental Affairs, The Impact of Implementation: A Review of the REAL ID Act and the Western Hemisphere Travel Initiative, Senate*, S. Hrg. 110-555 Cong., 110th Cong., 2 (2008), 1.

<sup>50</sup> Milberg, “National Security Surveillance and National Authentication System: The National Identification Debate: “REAL ID “and Voter Identification,” 443–472.

Along one path Congress can choose to do nothing and the Real ID Act will limp along for the next decade gradually creating the backbone for a National ID card system.<sup>51</sup>

This testimony conceptualizes the “National ID card system” to include a broader set of systematic identification, including the WHTI and enhanced driver’s license (EDL) programs. More reticent in his statements on what the REAL ID Act accomplishes, Professor Steinboch states, “If the Act, which takes effect in 2008, does not actually establish a de facto national identity card it certainly makes the prospect of one increasingly likely.”<sup>52</sup>

**c. *REAL ID Is a “De Facto” National Identity Card or Part of a “De Facto” National Identity Management System***

Many academics, privacy and civil liberties minded politicians, and advocacy groups, have called the REAL ID driver’s license a “de facto” national identity card, or acknowledged the nexus between the two.<sup>53</sup> In her 2009 article, “Tinkering Towards a National Identification System: An Experiment on Policy Attitudes,” Valentina Bali, an Associate Professor at Michigan State University stated, “The REAL ID Act of 2005 has sought precisely such a profound regulatory transformation, bringing the United States closer to a *de facto* national identification system based on state driver’s licenses.”<sup>54</sup> While Bali’s statement indicates the belief that the United States does not have a national identification system yet, the rest of the article closely aligns REAL ID driver’s licenses and identity cards with national identity cards. Bali noted the role of driver’s licenses in identification, stating, “In the United States the Social Security card and, more distinctly so, the state’s driver’s licenses and personal identification cards have acted as the

---

<sup>51</sup> *Oversight of Government Management, The Federal Workforce, and the District of Columbia Subcommittee of the Committee on Homeland Security and Governmental Affairs, The Impact of Implementation: A Review of the REAL ID Act and the Western Hemisphere Travel Initiative, Senate, S. Hrg. 110- 555 Cong., 110th Cong., 2 (2008), 1.*

<sup>52</sup> “Fourth Amendment Limits on National Identity Cards,” 296.

<sup>53</sup> This includes the U.S. Public Policy Committee of the Association for Computing Machinery (USACM); Cameron, “USACM Questions Real ID Act’s Security Standards,” Association for Computer Machinery U.S. Public Policy Council (USACM), April 5, 2005, <http://techpolicy.acm.org/blog/?p=240>.

<sup>54</sup> Valentina Bali, “Tinkering Toward a National Identification System: An Experiment on Policy Attitudes,” *Policy Studies Journal* 37, no. 2 (May 2009): 236.

effective identification cards.”<sup>55</sup> Driver’s licenses are the most commonly used identification in the United States and are used in many governmental and business transactions.<sup>56</sup> Bali’s acknowledgement that driver’s licenses have acted “as the effective identification cards” in the United States, while not defining what constitutes a national ID card, has essentially established the context in the article that driver’s licenses are national ID cards.<sup>57</sup> Furthermore, the study asked Michigan residents about their opinions on the REAL ID Act, but first asked them about their approval or disapproval of national identity cards without mentioning the REAL ID Act; thus, implying the nexus between national identity cards and the REAL ID Act.

***d. The REAL ID Is a National Identity Card and Creates a National Identity Management System***

The REAL ID has been called a “national ID system” based on three tenants called the “hallmarks of a national ID,” that it is “national in scope,” is “used for identification,” and “is legally or practically required.”<sup>58</sup> The claim that it is national scope is based on the fact that although personal data is maintained in individual state databases, the REAL ID requirement for the states to be able to access each other’s data essentially creates a federal requirement and unites the systems on a national level. The prevalence of driver’s licenses, and the necessity that an individual obtain one to drive, make them a practical requirement for much of the country. The requirement that licenses not be issued to illegal immigrants is also seen as “moving the license into the realm of a national ID card.”<sup>59</sup>

It would be remiss not to point out some of the contradictions occurring between the model created by Clement et al., discussed in Chapter I, and the discourse

---

<sup>55</sup> Bali, “Tinkering Toward a National Identification System: An Experiment on Policy Attitudes,” 234.

<sup>56</sup> *Ibid.*, 236.

<sup>57</sup> *Ibid.*, 234.

<sup>58</sup> Harper, “Testimony regarding SB 262 and the U.S. Federal REAL ID Act: Committee on Transportation New Hampshire State Senate.”

<sup>59</sup> Edgar A. Whitley, *The Identity Project: An Assessment of the UK Identity Cards Bill and its Implications* (London, UK: Department of Information Systems, London School of Economics and Political Science, 2005), 87.

surrounding SSNs and REAL ID compliant driver's licenses. While the authors of the article consider the combination of architectural elements (to include a unique identifier [identity number], no physical token [no ID card], and a database) to be a type of national identification,<sup>60</sup> and specifically cite the SSN as an example of this type of national identity architecture, the U.S. government does not see it as such. In fact, steps have been taken to prevent the SSN from being considered a universal identifier. The U.S. resistance to universal identifiers is explained in further detail in Chapter IV, which outlines cultural and historical factors surrounding the identity card debate.

In contrast to the government's intention for the SSN, Ya Ni and Tat-Kei Ho conceptualize the SSN as a type of ID and consider it to be part of the "de facto national identification system" for the United States, while acknowledge that they were not "designed for national ID purposes."<sup>61</sup> These academics consider a "national identity system" to be so basic as to simply require a "database and communication system that establishes and maintains specific information on every individual, including characterizes such as U.S. citizenship, state residence, or criminal record."<sup>62</sup>

*e. Summary*

Academia has a more nuanced view of the REAL ID Act than other stakeholders, as scholars have different opinions as to where the Act falls in the spectrum of national identity management models. This discrepancy illuminates a definitional issue. Having different understandings and beliefs about what constitutes a national identity card or a national identity management system, means that no two individuals or groups will think about schemes in the same way. The impact of definitional confusion, on real world policymaking, yields schemes that are conceptualized differently, but ultimately, face the same challenges.

---

<sup>60</sup> Clement et al., "National Identification Schemes (NIDS)", 195–205.

<sup>61</sup> Ya Ni and Tat-Kei Ho, "A Quiet Revolution or a Flashy Blip? The Real ID Act and U.S. National Identification System Reform," 1064.

<sup>62</sup> Ibid.

## **B. UNITED KINGDOM—IDENTITY CARDS ACT**

In 2002, the U.K. government began a public consultation on whether it should create an “entitlement card scheme.”<sup>63</sup> It did so through the publication of a white paper, “Entitlement Cards and Identity Fraud: A Consultation Paper,” in which the government introduced the main ideas behind how a system would work and solicited public comment. The scheme would, in essence, be a national identity management system that would involve the public’s use of national ID cards to confirm their identity for a wide variety of purposes that would benefit the U.K. citizens and residents, government/public sector, and the private sector.

The forward of the initial public consultation document, written by Home Secretary David Blunkett, begins with a reference to the September 11 terrorist attacks in the United States. Mr. Blunkett writes that he was asked if the United Kingdom would implement the use of identity cards following the attack. He states that the identity card system developed would focus on citizenship and entitlement services over national security. This emphasis can be seen in the government’s stated benefits of the card:

- (i) provide people who are lawfully resident in the U.K. with a means of confirming their identity to a high degree of assurance;
- (ii) establish for official purposes a person’s identity so that there is one definitive record of an identity which all Government departments can use if they wish;
- (iii) help people gain entitlement to products and services provided by both the public and private sectors, particularly those who might find it difficult to so do at present;
- (iv) help public and private sector organisations to validate a person’s identity, entitlement to products and services and eligibility to work in the U.K.<sup>64</sup>

In this original conceptualization of the scheme, the system would depend on the use of existing photo-ID, such as a “photocard” driver’s license, the newly announced

---

<sup>63</sup> Home Office, *Entitlement Cards and Identity Fraud: A Consultation Paper* (Norwich, England: The Stationary Office, 2002).

<sup>64</sup> *Ibid.*, 7.

passport card, or a low-cost non-driving license entitlement card.<sup>65</sup> Information held on the card would also be contained in a centralized database, which would be interoperable with other government databases. The system would be voluntary, rather than required or “compulsory,” meaning that the public would not need to participate or carry around identity cards.<sup>66</sup>

The government conducted two additional consultations from April through July 2004.<sup>67</sup> In November of that year, the government introduced the Identity Cards Bill into Parliament. A slightly different version was re-introduced in May 2005 after the general election.<sup>68</sup> It passed in March and the Identity Cards Act (2006) became law.<sup>69</sup> Several years after its inception, the developing system was given the name of the NIS by the government.<sup>70</sup>

## 1. Identity Cards Act Overview

Like the REAL ID Act, the Identity Cards Act created a legal framework for the national identity management scheme, leaving specific details to be defined later through regulation.<sup>71</sup> The statutory purpose was two-fold. The scheme created a “convenient method for individuals to prove their identity” and “provide[d] a secure and reliable means of identifying individuals” when it is in the public interest to do so.<sup>72</sup> Public interest is defined in the Identity Cards Act as for the purposes of:

- National security (including the prevention of terrorism)

---

<sup>65</sup> Home Office, *Entitlement Cards and Identity Fraud: A Consultation Paper*, 8.

<sup>66</sup> *Ibid.*, 7.

<sup>67</sup> Whitley, *The Identity Project: An Assessment of the UK Identity Cards Bill and its Implications*, 32.

<sup>68</sup> Edgar A. Whitley et al., “Reflections on the Academic Policy Analysis Process and the UK Identity Cards Scheme,” *Information Society* 23, no. 1 (January 2007): 52.

<sup>69</sup> *Ibid.*

<sup>70</sup> Home Office Identity & Passport Service, *Introducing the National Identity Scheme: How the Scheme Will Work and how it Will Benefit You* (London: Home Office Identity & Passport Service, 2008), 1–19.

<sup>71</sup> Phillip Ward, *The Identity Cards Bill (Bill 9 of 2005-06) House of Commons Research Paper 05/43* (London: House of Commons Library, 2005), 3.

<sup>72</sup> *Identity Cards Act 2006, Chapter 15*, Explanatory Notes, Section 1, Sub-section 16, <http://www.legislation.gov.uk/ukpga/2006/15/notes/division/5/1/1>.

- Prevention and detection of crime (including identity fraud and theft)
- Enforcement of immigration controls
- Enforcement of prohibitions on unauthorised working or employment
- Efficient and effective provision of public services<sup>73</sup>

**a. *National Identity Register***

As anticipated, the Identity Cards Act established the National Identity Register, a centralized database for which the Secretary of State is responsible for maintaining. The database would include a total of 50 data elements, referred to as “registrable facts,” for individuals inside the United Kingdom, including the following:

- Full name and any other names the individual has gone by
- Gender
- Date of birth, place of birth, and/or date of death (if individual is deceased)
- Identifying information including photograph including the head and shoulders, signature, fingerprints, and other biometric information (including an iris scan)
- Address—current and for all past residences inside and outside the United Kingdom
- Nationality
- Immigration status
- Identification numbers and documents associated with that individual<sup>74</sup>
- An audit record of who and when information in the Register about the individual was provided to another person or body

---

<sup>73</sup> *Identity Cards Act 2006, Chapter 15*, Explanatory Notes, Section 1, Sub-section 17, <http://www.legislation.gov.uk/ukpga/2006/15/notes/division/5/1/1>.

<sup>74</sup> In accordance with the Data Protection Act of 1998, the Registry cannot include identification numbers that reveal sensitive personal data, which includes racial or ethnic origin, political opinion, sexual life, and the commission of offences. *Identity Cards Act 2006, Chapter 15*, Section 1, Sub-section 20, <http://www.legislation.gov.uk/ukpga/2006/15/notes/division/5/1/1>.

- Other information included at a person's request<sup>75</sup>

Neither medical information, nor criminal records would have been included in the Register.<sup>76</sup>

The Act stated that individuals who had reached the age 16 and resided in the United Kingdom would be able to apply to be entered into the Register. It was intended that individuals would have legally resided in the United Kingdom for at least three months to be eligible for registration, including foreign nationals.<sup>77</sup> In addition, the Act was flexible in allowing for the Secretary of State, through regulation, to allow individuals who had resided in the United Kingdom in the past to apply for entry into the Register.<sup>78</sup> Each person's identity would be checked against passport, driving license, and immigration databases before being added to the Registers to confirm that each entry belongs to a unique individual to prevent duplicate entries.<sup>79</sup> Following their addition to the Registry, individuals would be assigned a unique number called the national identity registration number.<sup>80</sup> The Act also required individuals to apply for inclusion in the Register if they were applying for a "designated document."<sup>81</sup> What constituted a designated document was left open to be determined by the Secretary of State, but was intended to include passports.<sup>82</sup> The Act did not require individuals to register, called "compulsory registration." Doing so would require future legislation.<sup>83</sup> It does however,

---

<sup>75</sup> For the full list of data elements, see Appendix A. *Identity Cards Act 2006, Chapter 15*, Schedule 1, <http://www.legislation.gov.uk/ukpga/2006/15/schedule/1/enacted>.

<sup>76</sup> *Ibid.*, 27.

<sup>77</sup> *Identity Cards Act 2006, Chapter 15*, Explanatory Notes, Section 2, Sub-section 24, <http://www.legislation.gov.uk/ukpga/2006/15/notes/division/5/1/2>.

<sup>78</sup> *Ibid.*, Sub-section 23.

<sup>79</sup> "Identity Cards: The Next Steps, Cm 6020," November 2003, 5, <http://www.statewatch.org/news/2003/nov/id.pdf>.

<sup>80</sup> *Identity Cards Act 2006, Chapter 15*, Section 2, Sub-section 27, <http://www.legislation.gov.uk/ukpga/2006/15/notes/division/5/1/2>.

<sup>81</sup> *Identity Cards Act 2006, Chapter 15*, Section 5, Sub-section 2, <http://www.legislation.gov.uk/ukpga/2006/15/section/5/enacted>.

<sup>82</sup> *Identity Cards Act 2006, Chapter 15*, Section 4, Sub-section 1, <http://www.legislation.gov.uk/ukpga/2006/15/section/4/enacted>; *Identity Cards Act 2006, Chapter 15*, Explanatory Notes, Section 4, Sub-section 14, <http://www.legislation.gov.uk/ukpga/2006/15/notes/division/5/1/4>.

<sup>83</sup> *Identity Cards Act 2006, Chapter 15*, Explanatory Notes, Section 7, Sub-section 58, <http://www.legislation.gov.uk/ukpga/2006/15/notes/division/5/2/2>.

set specific requirements for individuals “subject to compulsory registration,” showing that the government did intend to pursue this avenue in the future.<sup>84</sup> The Act was always intended to be the basis for a compulsory scheme.<sup>85</sup>

***b. ID Cards***

The scheme involved the issuance of an identity card (ID card) to individuals who registered. While not specified in the Act, it was later determined that the individual’s data would be held on both the ID card and in the Register. The Act also specified that certain information on the cards would be encrypted and that different people may have different validity periods.<sup>86</sup> In addition, the Identity Cards Act amended legislation to allow ID cards to become a type of travel document similar to a passport.<sup>87</sup> The government had not set a date for when the cards would become compulsory; however, compulsion would require additional Parliamentary approval. Still, it was never intended for individuals to be required to carry them at all times.<sup>88</sup>

***c. Scheme Provisions***

In addition to promulgating the physical architecture of the scheme, the Identity Card Act stipulates a number of provisions that describe how the scheme will function and the services it will provide.

(1) Requirement to Provide Information. To keep the information in the Register accurate, the Act gave the Secretary of State and designated documents authorities the ability to require individuals with ID cards to provide updates to the government when their personal information changed. It was the individual’s responsibility to keep their information up-to-date once they were added to the Register,

---

<sup>84</sup> *Identity Cards Act 2006, Chapter 15*, Section 7, <http://www.legislation.gov.uk/ukpga/2006/15/section/7/enacted>.

<sup>85</sup> *Identity Cards Act 2006, Chapter 15*, Explanatory Notes, Summary and Background, Sub-section 4, <http://www.legislation.gov.uk/ukpga/2006/15/notes/division/2>.

<sup>86</sup> *Identity Cards Act 2006, Chapter 15*, Section 6, Sub-section 50, <http://www.legislation.gov.uk/ukpga/2006/15/notes/division/5/2>.

<sup>87</sup> *Identity Cards Act 2006, Chapter 15*, Section 39, <http://www.legislation.gov.uk/ukpga/2006/15/section/39/enacted>.

<sup>88</sup> *Ibid.*, 17; “Identity Cards: The Next Steps, Cm 6020,” 2.

which included their current address. This requirement did not apply to individuals in the Register who were not issued ID cards.<sup>89</sup>

(2) Identity Verification. The Act specified that the scheme would involve an identity verification service, which would have provided specific information from the Register to a requesting party to confirm the individual's identity.<sup>90</sup> A requesting party was intended to include both public and private sector organizations (e.g., a government agency or business).<sup>91</sup> An accreditation process would have needed to be established so that only approved parties could make these requests, but they could only do so with the individual's consent.<sup>92</sup> In addition, the Act stated that regulation could be promulgated "to make public services conditional on identity checks."<sup>93</sup> Public services were defined broadly and could extend beyond National Health Service (NHS) services to, for example, the issuance of firearms certificates.<sup>94</sup> The Act limited what information could be provided to requesting agencies.<sup>95</sup> For example, an individual's biometric information (e.g., fingerprint) may not be provided, but confirmation that the biometric information submitted by the requestor matches that on file for the individual may be provided.<sup>96</sup>

(3) Oversight. The Act established NIS Commissioner, who was responsible for reviewing operational decisions made by the Secretary of State and designated documents authorities and for reviewing the uses of the ID cards.<sup>97</sup> Specific to the operation of the scheme, the Commissioner was responsible for "securing the confidentiality and integrity of the information" in the Register as well as dealing with complaints.<sup>98</sup> The Commissioner was required to report to the Secretary of State and

---

<sup>89</sup> *Identity Cards Act 2006, Chapter 15*, Explanatory Notes, Section 10, Sub-section 74, <http://www.legislation.gov.uk/ukpga/2006/15/notes/division/5/2/5>.

<sup>90</sup> *Identity Cards Act 2006, Chapter 15*, Section 12, Sub-section 1-2, <http://www.legislation.gov.uk/ukpga/2006/15/section/12/enacted>.

<sup>91</sup> *Ibid.*, 16.

<sup>92</sup> *Identity Cards Act 2006, Chapter 15*, Explanatory Notes, Section 12, Sub-sections 83, 90, <http://www.legislation.gov.uk/ukpga/2006/15/notes/division/5/3/1>.

<sup>93</sup> *Identity Cards Act 2006, Chapter 15*, Section 13, <http://www.legislation.gov.uk/ukpga/2006/15/notes/division/5/4/1>.

<sup>94</sup> *Identity Cards Act 2006, Chapter 15*, Explanatory Notes, Section 42, Sub-section 220, <http://www.legislation.gov.uk/ukpga/2006/15/notes/division/5/11/2>.

<sup>95</sup> *Identity Cards Act 2006, Chapter 15*, Section 12, Sub-section 2-3, <http://www.legislation.gov.uk/ukpga/2006/15/section/12/enacted>.

<sup>96</sup> *Identity Cards Act 2006, Chapter 15*, Explanatory Notes, Section 12, Sub-section 86, <http://www.legislation.gov.uk/ukpga/2006/15/notes/division/5/3/1>.

<sup>97</sup> *Identity Cards Act 2006, Chapter 15*, Section 22, Sub-sections 1-2, <http://www.legislation.gov.uk/ukpga/2006/15/section/22/enacted>.

<sup>98</sup> *Identity Cards Act 2006, Chapter 15*, Section 22, Sub-section 3, <http://www.legislation.gov.uk/ukpga/2006/15/section/22/enacted>.

Parliament annually.<sup>99</sup> The Act also gave the Intelligence Services Commissioner responsibility for oversight of the intelligence services' use and interaction with the Register.<sup>100</sup>

(4) Allowable Uses. The Act allowed the data in the Register to be shared with national security and intelligence agencies to carry out their functions without the consent of the individual in question. These agencies included the Security Services, the Secret Intelligence Service, the Government Communications Headquarters (GCHQ), and the Serious Organized Crime Agency.<sup>101</sup> Information could also be shared with a chief officer of police or Commissioners of Her Majesty's Revenue & Customs "in the interests of national security; for purposes connected with the prevention or detection of crime; or for other purposes specified by order made by the Secretary of State."<sup>102</sup> The Commissioners were also allowed to receive information for functions relating to national insurance contributions and for other purposes connected to their mission.<sup>103</sup> Finally, information could be shared with a specified government department or a Northern Ireland department for the purpose of carrying out their functions.<sup>104</sup>

(5) Criminal Offenses and Civil Penalties. The Act created a number of new criminal offenses including the possession, use, or creation of false identity documents issued by the United Kingdom or other countries (e.g., ID card, passport, driving license, immigration document, etc.); the "unauthorized disclosure of information" from the Register; "providing false information" for inclusion in the Register; and "tampering with the Register."<sup>105</sup> In addition to criminal offenses, the Secretary of State may issue civil penalties, or fines, to ensure compliance with the Act.<sup>106</sup>

(6) Fees and Costs. Through regulation, the Act allowed the Secretary of State to impose fees in relation to the scheme, such as for issuing ID cards or for confirming information in the register.<sup>107</sup> To keep track of the costs of the scheme, the Secretary of State was required to report to Parliament, six months after the Act was passed, the

---

<sup>99</sup> *Identity Cards Act 2006, Chapter 15*, Section 23, Sub-section 1–3, <http://www.legislation.gov.uk/ukpga/2006/15/section/23/enacted>.

<sup>100</sup> *Identity Cards Act 2006, Chapter 15*, Section 24, Sub-section 2, <http://www.legislation.gov.uk/ukpga/2006/15/section/24/enacted>.

<sup>101</sup> *Identity Cards Act 2006, Chapter 15*, Section 17, Sub-section 2, <http://www.legislation.gov.uk/ukpga/2006/15/section/17/enacted>.

<sup>102</sup> *Ibid.*, Sub-section 3, 4.

<sup>103</sup> *Ibid.*, Sub-section 4.

<sup>104</sup> *Ibid.*, Sub-section 5.

<sup>105</sup> *Identity Cards Act 2006, Chapter 15*, Section 25–29, <http://www.legislation.gov.uk/ukpga/2006/15/contents/enacted>.

<sup>106</sup> *Identity Cards Act 2006, Chapter 15*, Section 31, Sub-section 1, <http://www.legislation.gov.uk/ukpga/2006/15/section/31/enacted>.

<sup>107</sup> *Identity Cards Act 2006, Chapter 15*, Section 35, Sub-section 1, <http://www.legislation.gov.uk/ukpga/2006/15/section/35/enacted>.

anticipated cost of the scheme over the next 10 years.<sup>108</sup> The Secretary would be required to report on the cost every six months after that.

*d. Identity Cards Act Purpose*

The U.K. government—specifically the Home Office—cited a variety of potential uses for the card in their initial consultation document, “Entitlement Cards and Identity Fraud: A Consultation Paper,” which would benefit the government and public sector, U.K. citizens and residents, and private sector businesses. The focus of the scheme is very different from that of the REAL ID Act. The system purpose is primarily to prevent and combat identity theft and facilitate entitlement to services; the focus on terrorism is ancillary. As Home Secretary David Blunkett, wrote in the Forward:

After the terrorist atrocities in the United States on 11 September 2001, I was asked whether the Government was considering introducing identity cards. I said at the time that any debate about identity cards should not centre exclusively on issues of national security. Far more important are the issues of citizenship and entitlement to services and it is in this context that I would like to see the debate unfold.<sup>109</sup>

To understand the purposes for the system further, the following sections delve deeper into the benefits to the government, and the public and private sectors.

(1) Individual Purpose: To Create a Convenient Method for Individuals to Prove Their Identity. The government intended the scheme to provide a benefit to the U.K. residents who would be enrolled in the Register and/or receive an ID card. Since private companies were meant to be able to access the information collected, the scheme was touted as a simple way for individuals to verify their identity to make secure transactions with organizations, such as banks.<sup>110</sup> Since address information would be collected in the Register, the government proposed that citizens would only need to change their address data in one location rather than filling out multiple forms for different government agencies.<sup>111</sup> The identity card was described as a means for young people to validate their age when buying restricted products, such as alcohol, and could potentially facilitate travel through Europe.<sup>112</sup>

---

<sup>108</sup> *Identity Cards Act 2006, Chapter 15, Section 37*, <http://www.legislation.gov.uk/ukpga/2006/15/section/37/enacted>.

<sup>109</sup> Home Office, *Entitlement Cards and Identity Fraud: A Consultation Paper*, 3.

<sup>110</sup> *Ibid.*, 7.

<sup>111</sup> *Ibid.*, 27.

<sup>112</sup> *Ibid.*, 8.

(2) Societal Purpose: To provide a secure and reliable means of identifying individuals when it is in the public interest, in addition to the specific benefits provided to an individual U.K. resident, the government has explained a number of ways in which the scheme is intended to better society. These benefits broadly include increased security, reduced fraud, and enhanced service delivery.

- Enhance National Security and Facilitate the Prevention and Detection of Crime

One of the purposes of the scheme was to prevent people engaged in or funding terrorist and criminal activities from being able to maintain multiple identities.<sup>113</sup> The ability to maintain different aliases or obtain fraudulent documents helps terrorists and criminals conceal their identity and further their enterprises. The scheme was meant to prevent these individuals from receiving legitimate government documents. It was also meant to prevent identity theft and fraud by making it harder for bad actors to forge documents.<sup>114</sup> This obstruction would help combat the high costs of identity fraud, which a 2002 government estimate found to have cost the U.K. public and private sectors a total of 1.3 billion pounds.<sup>115</sup>

The scheme would have allowed law enforcement, intelligence, and security agencies to track individuals based on a historical record of what organizations are requesting a check of the Register. The government anticipated that requests would have been made for services, such as renting a hotel room, hiring a rental car, or buying a mobile phone. Thus, the government would have been able to reconstruct past locations of individuals based on their attempted to purchase these items and services.<sup>116</sup>

Additionally, the scheme would have created a large repository of fingerprints available to query. Police would have been able to check fingerprints left at the scene of a crime, called latent fingerprints, against the holdings of the Register to help identify suspects.<sup>117</sup>

- Facilitate the Enforcement of Immigration Controls and Prohibitions on Unauthorized Working or Employment

The system was intended to eliminate the “pull factor” that brought immigrants into the United Kingdom, particularly the perception that they would be able to easily obtain benefits and services once they entered into the country.<sup>118</sup> The government states that illegal migration results in lost tax revenue and forces the agencies to contend with

---

<sup>113</sup> Home Office, *Identity Cards Bill Regulatory Impact Assessment* (London: Home Office, 2004), 12.

<sup>114</sup> *Ibid.*, 12–13.

<sup>115</sup> *Ibid.*, 6.

<sup>116</sup> *Ibid.*, 13.

<sup>117</sup> *Ibid.*, 14.

<sup>118</sup> Home Office, *Entitlement Cards and Identity Fraud: A Consultation Paper*, 7.

fraudulent benefit claims.<sup>119</sup> Those who facilitate the entry of illegal workers into the United Kingdom are often tied to organized crime—like trafficking—or are engaged in other criminal activity. The scheme is conceptualized to reduce this activity.

Additionally, another potential benefit of the scheme was to assist the government in prosecuting companies that hired workers illegally, as those companies could no longer rely on the excuse that they did not understand how to read the myriad of European Union immigration documents.<sup>120</sup> The scheme was considered a benefit to would-be migrant workers, as its enforcement was said to provide protection to those who would have been working for very little money in poor conditions by preventing this situation from occurring.<sup>121</sup> Finally, the scheme was proposed to aid companies by creating an easier, more centralized way for them to validate the immigration status of job applicants and employees.<sup>122</sup>

- Efficient and Effective Provision of Public Services

As stated previously, service delivery can be understood to be the most significant purpose of the scheme. This concept is referring to facilitating government services to the public; it was to be a means of efficiently validating individuals' identity to ensure their entitlement to goods and services.

In the United Kingdom, situations in which it is statutorily required that an individual provide identification extend beyond claiming benefits. They also include accepting “a place in Higher Education, applying for a student loan, or in applying for social housing.”<sup>123</sup> In addition, the Act stated that when it became compulsory for certain populations of individuals to register, those individuals would be required to produce their ID card for public services that were free of charge (e.g., free non-emergency NHS treatment) or to receive a government payment (e.g., social security benefits).<sup>124</sup>

The clear benefit to the government was to have access to a definitive record of an individual's identity.<sup>125</sup> The scheme could also aid in the facilitation of e-government, or government services provided over the Internet, a benefit to both the public sector and the private citizen.<sup>126</sup>

---

<sup>119</sup> Home Office, *Identity Cards Bill Regulatory Impact Assessment*, 9.

<sup>120</sup> Home Office, *Entitlement Cards and Identity Fraud: A Consultation Paper*, 7; Home Office, *Identity Cards Bill Regulatory Impact Assessment*, 10.

<sup>121</sup> *Ibid.*, 9.

<sup>122</sup> Home Office, *Entitlement Cards and Identity Fraud: A Consultation Paper*, 7.

<sup>123</sup> Home Office, *Identity Cards Bill Regulatory Impact Assessment*, 19.

<sup>124</sup> *Ibid.*, 20; *Identity Cards Act 2006, Chapter 15*, Section 13, Sub-section 2, <http://www.legislation.gov.uk/ukpga/2006/15/section/13/enacted>.

<sup>125</sup> Home Office, *Entitlement Cards and Identity Fraud: A Consultation Paper*, 7.

<sup>126</sup> *Ibid.*, 28.

The scheme was also suggested to benefit the private sector commercially. It would help companies respond to their customers more efficiently and prevent them from having to spend valuable time reviewing personal information on forms filled out by customers.<sup>127</sup> The consultation paper proposed that having a single definitive way to confirm customers' identity would create a cost savings, but did not explain how. The paper did, however, propose that the identity card could create a cost savings by becoming the vehicle that companies could use to facilitate their loyalty programs, rather than producing their own cards.<sup>128</sup>

## **2. What Is the National Identity Scheme? A National Identity Management System, a National ID Card, or Neither?**

The system developed in the United Kingdom has been called a NIS, national identity card scheme, or simply referred to as a national identity card or an entitlement card.

With the plethora of academic constructed models for identity management architecture, it is easy to see why a level of ambiguity exists in the literature on identity cards and the literature on identity management systems. This confusion is readily apparent in the discourse that surrounded the U.K. identity management scheme.

As described earlier, the name of the bill that began the development of the national identity management system was the "Identity Cards Bill." Similarly, many of the consultation papers conducted by the Home Office have titles that include the terms "entitlement cards" or "identity cards."<sup>129</sup> In fact, a study conducted by several professors into public attitudes on the identity card implementation scenarios in the United Kingdom found that acceptance of national identity cards declined when subjects were specifically asked how they would feel about an implementation plan that would include storing their information in a centralized database, rather than only having the information stored on the card (with that information "backed up on a computer held by a

---

<sup>127</sup> Home Office, *Entitlement Cards and Identity Fraud: A Consultation Paper*, 28.

<sup>128</sup> Ibid.

<sup>129</sup> Home Office, *Identity Cards: A Summary of Findings from the Consultation on Legislation on Identity Cards* (Norwich: The Stationery Office, 2004); Home Office, *Entitlement Cards and Identity Fraud: A Consultation Paper*, 1–146.

trusted third party such as a bank, police station, or [lawyers' office]”).<sup>130</sup> They found that, “The results of the present study suggest that potential users of an identity card are aware of the potential security risks of a centralized database, and find a distributed approach more acceptable.”<sup>131</sup> When prompted with the concept of a database (whether centralized or held by a third party), the support for identity cards decreases regardless of who maintains the database. This finding supports the idea that people do not immediately associate ID cards with a database; these two components are conceptualized as being different entirely.

---

<sup>130</sup> Adam N. Joinson et al., “Watching Me, Watching You: Privacy Attitudes and Reactions to Identity Card Implementation Scenarios in the United Kingdom,” *Journal of Information Science* 32, no. 4 (2006): 341.

<sup>131</sup> *Ibid.*

### **III. POLICY AND PRIVACY CONCERNS**

The factors and tensions, drivers and inhibitors found in the discourse surrounding the REAL ID Act stipulations for driver's licenses and identity cards and the U.K. NIS are actually quite similar. They tend to highlight the tensions that exist between privacy and security and between convenience and intrusiveness.<sup>132</sup> In looking at the similarities between detracting arguments, this chapter begins with examining the privacy and policy concerns surrounding these schemes. From this basis, the chapter establishes evidence of the similarity between opposing arguments to national identity cards and schemes characterized as being national identity management systems.

#### **A. PURPOSE CONCERNS**

One of the questions posed by scholars and academics is whether the REAL ID Act and the NIS would actually accomplish the purposes for which they were created. In this regard, the arguments against both approaches are similar.

##### **1. Schemes Will Not Enhance National Security or Prevent Terrorism**

For both schemes, academics and privacy and civil liberties advocates have questioned whether the ID cards will actually improve national security, prevent terrorism, and increase safety. Privacy advocacy groups are quick to point out that little empirical research is available on the effects of national identity cards on terrorism prevention. As of April 2004, the following statistics existed for assessing the impact of national identity cards:

While a link between identity cards and anti-terrorism is frequently suggested, the connection appears to be largely intuitive. Almost no empirical research has been undertaken to clearly establish how identity tokens can be used as a means of preventing terrorism.

Of the 25 countries that have been most adversely affected by terrorism since 1986, eighty per cent have national identity cards, one third of which incorporate biometrics. This research was unable to uncover any instance

---

<sup>132</sup> Halperin and Backhouse, "A Roadmap for Research on Identity in the Information Society," 73, 75.

where the presence of an identity card system in those countries was seen as a significant deterrent to terrorist activity.<sup>133</sup>

One argument made against both the REAL ID Act and the NIS is that neither scheme would prevent terrorism because the adoption of enhanced ID cards will actually attract bad actors. REAL ID compliant driver's licenses and identity cards were posited to "entice criminals and terrorists to acquire them" since they are a trusted source of identity verification.<sup>134</sup> Similarly, those critical of the UK scheme believe that the national ID card would further advance criminality:

Whenever governments attempt to introduce an ID card, it is always based on the aim of eliminating false identity. The higher the "integrity" (infallibility) of a card, the greater is its value to criminals and illegal immigrations. A high-value card attracts substantially larger investment in corruption and counterfeit activity. The equation is simple: higher value ID equals greater criminal activity.<sup>135</sup>

Additionally, the UK national identity card was derided for its inability to prevent individuals from doing harm since the government had only assigned a civil penalty of 2,500 pounds to people who fail to register. The lack of a strong monetary fine created a concern among academics that the wealthy, as well as individuals seeking to avoid the system, would only need to pay their way out of it. As the London School of Economics (LSE) stated, "This fine could effectively become a tax on criminals and terrorists operating in the UK."<sup>136</sup> Since visitors and students who remained in the United Kingdom for less than three months were not expected to obtain ID cards, some argued that this loophole would prevent ID cards from being fully effective.<sup>137</sup>

---

<sup>133</sup> "Mistaken Identity; Exploring the Relationship between National Identity Cards & the Prevention of Terrorism," April 2004, <http://www.privacyinternational.org/issues/idcard/uk/id-terrorism.pdf>.

<sup>134</sup> *Oversight of Government Management, The Federal Workforce, and the District of Columbia Subcommittee of the Committee on Homeland Security and Governmental Affairs, The Impact of Implementation: A Review of the REAL ID Act and the Western Hemisphere Travel Initiative, Senate, 5.*

<sup>135</sup> "Privacy International's FAQ on the UK Government's Proposed National Identity Card," accessed October 28, 2015, <https://web.archive.org/web/20120207124540/https://www.privacyinternational.org/issues/idcard/uk/uk-idcard-faq.html>; <http://www.privacyinternational.org/issues/idcard/uk/uk-idcard-faq.html#forged>, quoted in *Research Paper 05/43: The Identity Cards Bill, Bill 9 of 2005-06* (June 13, 2005), 52.

<sup>136</sup> Whitley, *The Identity Project: An Assessment of the UK Identity Cards Bill and its Implications*, 44.

<sup>137</sup> *Ibid.*

Another argument made against both schemes is that they will not be able to prevent terrorists from committing fraud to obtain valid IDs. This belief relies on the assertion that bad actors will find ways to get hold of REAL ID compliant licenses fraudulently in the same way that the 9/11 terrorists were able to.<sup>138</sup> The ID cards would then allow them to operate clandestinely since the cards are considered a highly trusted and secure form of documentation. The use of legitimate documentation to circumvent the system is known as logical avoidance and could become a preferred strategic measure, given terrorists' proclivity to operate under their own names, as noted by Privacy International:<sup>139</sup>

Almost two thirds of known terrorists operate under their true identity. The remainder use a variety of techniques to forge or impersonate identities. It is possible that the existence of a high integrity identity card would provide a measure of improved legitimacy for these people.<sup>140</sup>

Opponents of the national identity schemes argue that those operating under their true identities could also evade the system through physical avoidance. In doing so, terrorists may instead choose to target locations that do not require identification, such as malls.<sup>141</sup> This assumption is not unrealistic, considering that threats by such terrorist groups as Al Shabaab have already been made toward public spaces like the Mall of America.

## **2. Schemes Will Not Prevent Identity Theft**

Critics in the United States have argued that the REAL ID Act will attract identity thieves due to the valuable personal information contained within the DMV databases.<sup>142</sup>

---

<sup>138</sup> *Oversight of Government Management, The Federal Workforce, and the District of Columbia Subcommittee of the Committee on Homeland Security and Governmental Affairs, The Impact of Implementation: A Review of the REAL ID Act and the Western Hemisphere Travel Initiative, Senate, 5.*

<sup>139</sup> Harper, "Testimony regarding SB 262 and the U.S. Federal REAL ID Act: Committee on Transportation New Hampshire State Senate," 3.

<sup>140</sup> "Mistaken Identity; Exploring the Relationship between National Identity Cards & the Prevention of Terrorism," 2.

<sup>141</sup> Harper, "Testimony regarding SB 262 and the U.S. Federal REAL ID Act: Committee on Transportation New Hampshire State Senate."

<sup>142</sup> *Oversight of Government Management, The Federal Workforce, and the District of Columbia Subcommittee of the Committee on Homeland Security and Governmental Affairs, The Impact of Implementation: A Review of the REAL ID Act and the Western Hemisphere Travel Initiative, Senate, 4.*

U.K. opponents have noted that the centralization of data in the National Identity Register could lead to increased instances of fraud:

Centralised identity systems often give rise to fraud through the abuse of centralised data either by insiders (staff) or outsiders (malicious hackers).<sup>143</sup>

The creation of a unique identifier, namely the national identity registration number, also raised concern that it could exacerbate the identity theft problem since, “In some cases, the use of unique identifiers for citizens has become the key enabler of identity theft.”<sup>144</sup> The same concern exists for the unique identifier associated with a REAL ID license or identity card, as its reliability may increase its use in the private sector, and thus, it could gain the same value in enabling fraudulent transactions as the SSN.<sup>145</sup>

In addition to these arguments, the LSE strongly questioned the NIS’ ability to reduce identity theft noting that its 1.3 billion-pound cost to the U.K. economy—that the government increasingly touted as an important reason for the scheme—depended on different definitions of identity fraud, not all of which would be prevented by the introduction of an identity card.<sup>146</sup>

### **3. Schemes Will Not Reduce Illegal Immigration or Unlawful Employment**

Finally, opponents argued that the schemes would not reduce illegal immigration or unlawful employment. One of the concerns within the United States is that the REAL ID will “undermine national security by pushing immigrants deeper into the shadows and

---

<sup>143</sup> Whitley, *The Identity Project: An Assessment of the UK Identity Cards Bill and its Implications*, 98.

<sup>144</sup> *Ibid.*

<sup>145</sup> Department of Homeland Security, *Privacy Impact Assessment for the REAL ID Act In Conjunction with the Notice of Proposed Rulemaking, Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes* (Washington, DC: Department of Homeland Security, 2007), [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_pia\\_realid.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_realid.pdf).

<sup>146</sup> Whitley et al., “Reflections on the Academic Policy Analysis Process and the UK Identity Cards Scheme,” 53; Whitley, *The Identity Project: An Assessment of the UK Identity Cards Bill and its Implications*, 98.

forcing many to drive without licenses.”<sup>147</sup> In the United Kingdom, it was argued that if the existing framework of legislation for tackling unlawful employment was not effective, then an ID card would not solve the problem.<sup>148</sup> The LSE commented:

The only measures that could change the situation are a compulsion on all individuals to carry ID cards in order to permit spot-checks by the Home Office, a requirement on all employers to report, and a requirement to verify the data against the national register.<sup>149</sup>

However, a requirement for compulsory registration was never established before the scheme was disbanded and the legislation expressly prohibited the requirement that individuals carry the card with them.

## **B. PRIVACY CONCERNS**

A number of privacy concerns are associated with both schemes. Many have to do with how the scheme will function or how data collected will be used, maintained, and protected.

### **1. Function Creep**

Large repositories of data are valuable tools that allow federal government agencies to accomplish their respective missions. Due to this value, privacy advocates have raised concerns that the schemes will suffer “function creep.” In other words, the system would eventually be used for purposes beyond what it was originally intended for and data would also be used for purposes beyond what it was originally collected for. The SSN has been cited as a prime example of function creep, “Initially designed only for administering social security benefits, SSNs are now common data elements in public and private sector databases, allowing for easy sharing and correlation of disparate

---

<sup>147</sup> Milberg, “National Security Surveillance and National Authentication System: The National Identification Debate: “REAL ID “and Voter Identification.”

<sup>148</sup> Whitley, *The Identity Project: An Assessment of the UK Identity Cards Bill and its Implications*, 134.

<sup>149</sup> *Ibid.*

records.”<sup>150</sup> What was originally a unique identifier for one system is now used to identify people in many different systems.

The expanded use of identity cards and unique identifiers beyond their original purpose is exactly the concern that privacy-minded groups have about the REAL ID licenses and identity cards and the National Identity System and associated national identity registration number. This type of function creep is not an unrealistic expectation. In the Notice of Proposed Rulemaking (NPRM) for the Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, DHS noted the ability to expand the official purpose of the REAL ID Act, stating:

DHS proposes to limit the regulatory definition of “official purpose” at this time, to those purposes expressly stated in the Act—accessing Federal facilities, boarding commercial aircraft, and entering nuclear power plants. DHS, under the discretionary authority granted to the Secretary of Homeland Security under the Act, may expand this definition in the future.<sup>151</sup>

In the Notice of Proposed Rulemaking, DHS requested that the public provide comments on how the Department could expand the purpose of the ID card to “other federal activities.” Privacy advocates have pointed out that even the ancillary benefits called out in the NPRM, such as preventing “unlawful access to firearms, voter fraud, and possibly underage drinking and smoking,” are beyond the official purpose of the Act, and are a further sign that future uses of the cards will extend far beyond what was originally intended.<sup>152</sup>

As it stands today, some see the REAL ID Act itself as function creep. Driver’s licenses were created only to certify that a person is authorized to drive a motor vehicle.

---

<sup>150</sup> Kent and Millett, *IDs—Not that Easy: Questions about Nationwide Identity Systems*, 8.

<sup>151</sup> Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 72 Fed. Reg. 10823 (March 9, 2007)

<sup>152</sup> *Senate Committee on Homeland Security and Governmental Affairs Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers’ Licenses and Identification Cards*, S. Hrg. 110-291 Cong., 110th Cong., 1 (2007), 94, <https://www.hsdl.org/?view&did=484478>; Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 72 Fed. Reg. 10846 (March 9, 2007)

The use of the identity card for verifying age or address, or even as a means to prevent terrorism, is beyond its original intended purpose.<sup>153</sup>

Members of the U.K. Parliament also voiced concerns regarding the potential for function creep.<sup>154</sup> Multiple times over the course of the scheme's development and implementation, the Home Affairs Select Committee noted their worries, which were not without precedent. In a 2004 report, the Committee harkened back to 1939, at the beginning of WWII, when a national identity card established for three purposes, had expanded to 39 purposes by 1950.<sup>155</sup> In 2008, several years after the passage of the Identity Cards Act, but before the first ID cards were due to be distributed, members of the Home Affairs Select Committee re-visited the issue of the potential expansion of the scheme:

We are concerned...about the potential for 'function creep' in terms of the surveillance potential of the National Identity Scheme. Any ambiguity about the objectives of the Scheme puts in jeopardy the public's trust in the Scheme itself and in the Government's ability to run it.<sup>156</sup>

They requested assurance that the scheme's purposes would not be broadened without first consulting the Information Commissioner, as well as Parliament. The LSE noted that if the scheme were to assist the police in the way that they had requested, the function of the card would need to be expanded to allow officers to require individuals to produce their cards during stop and search procedures. The ability to compel people to show their ID cards would also be the only effective way to combat illegal immigration using the card.<sup>157</sup>

---

<sup>153</sup> Kent and Millett, *IDs—Not that Easy: Questions about Nationwide Identity Systems*, 22; Bruce Schneier, "Security and Function Creep," *IEEE Security & Privacy* 8, no. 1 (January/February, 2010), 88.

<sup>154</sup> House of Commons, Home Affairs Committee, *A Surveillance Society? Fifth Report of Session 2007–08 Volume 1* (London: House of Commons Library, 2008), 73.

<sup>155</sup> House of Commons, Home Affairs Committee, *Identity Cards: Fourth Report of Session 2003–04, Volume 1* (London: The Stationery Office Limited, 2004), 41.

<sup>156</sup> House of Commons, Home Affairs Committee, *A Surveillance Society? Fifth Report of Session 2007–08 Volume 1*, 73.

<sup>157</sup> Whitley, *The Identity Project: An Assessment of the UK Identity Cards Bill and its Implications*, 126.

## 2. Data Security and Privacy Protections

Another issue that faced the administrators of both the U.K. NIS and the REAL ID Act implementation was concern over data security. Both schemes risk potential data breaches, both intentional and unintentional. The risk of data breaches is germane to both discussions of national ID systems and ID cards because the information in both will be held in a database, whether or not it is centralized (like in the United Kingdom) or decentralized in multiple databases (like the U.S. DMV databases that exist for each state).

As it stands, in the Notice of Proposed Rulemaking, the federal government did not require that the states meet federal standards for privacy and data security. Privacy advocates call this omission a blunder since the NPRM cites Executive Order 13132, which states, “[f]ederalism is rooted in the belief that issues that are not national in scope or significance are most appropriately addressed by the level of government closest to the people.”<sup>158</sup> The act of citing that particular Executive Order signals to privacy advocates that the federal government does not see privacy as national in scope, a sentiment with which they adamantly disagree. Advocates believe that the Privacy Act of 1974, which establishes information privacy and security practices that federal agencies must abide by, applies to this systematic collection of data because the Privacy Act, “stipulates that systems of records operated under contract or, in some instances, State or local governments operating under Federal mandate ‘by or on behalf of the agency... to accomplish an agency function’ are subject to the provisions ...of the Act.”<sup>159</sup> In this argument, the databases operated by each state for collecting information on drivers to fulfill the requirements of the REAL ID Act are seen as a wider system of records.<sup>160</sup>

---

<sup>158</sup> Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 72 Fed. Reg. 10847 (March 9, 2007).

<sup>159</sup> Electronic Privacy Information Center (EPIC), *REAL ID Implementation Review: Few Benefits, Staggering Costs* (Washington, DC: Electronic Privacy Information Center, 2008), 11; Office of Management and Budget, *Privacy Act Implementation: Guidance and Responsibilities*, 40 Fed. Reg. 28,948, 28,951 (July 9, 1975), [https://www.whitehouse.gov/sites/default/files/omb/inforeg/implementation\\_guidelines.pdf](https://www.whitehouse.gov/sites/default/files/omb/inforeg/implementation_guidelines.pdf).

<sup>160</sup> *Ibid.*, 11.

Not all advocacy groups feel that the REAL ID Act is detrimental to privacy, however. Some groups say that the REAL ID Act increases privacy protections by increasing the physical security of DMV production facilities and requiring more stringent background checks for workers.<sup>161</sup> In addition, they highlight the fact that the data has not been consolidated into a single centralized federal database and left to the states to maintain in separate databases.<sup>162</sup>

The NPRM issued by DHS for REAL ID standards leaves the states to work out a collective governance structure, business process, and data access rules. All states are currently required to check applicants against the National Driver Register (NDR)/Problem Driver Pointer System (PDPS) and the Commercial Driver's License Information System (CDLIS). The NDR is a database of information on "problem" drivers in all 51 jurisdictions and the PDPS allows users to query the NDR database.<sup>163</sup> The PDPS also acts as a pointer system that notifies the user of the individual's state of record (SOR), which contains their driver status and history information. The PDPS is maintained by the U.S. Department of Transportation, National Highway Transportation Safety Administration (NHTSA).<sup>164</sup> The DHS Privacy Impact Assessment (PIA) for the REAL ID Act notes that the PDPS adopts principles of the Privacy Act of 1974 including "individual participation and collection, use, and disclosure limitation."<sup>165</sup> While CDLIS has more limited privacy protections, DHS states that no known privacy issues exist with how it is implemented.<sup>166</sup>

---

<sup>161</sup> Janice Kephart, *Repealing REAL ID? Rolling Back Driver's License Security* (Washington, DC: Center for Immigration Studies, 2009), 3.

<sup>162</sup> *Ibid.*

<sup>163</sup> "Problem Driver Pointer System (PDPS)," accessed September 22, 2015, <http://www.aamva.org/PDPS/>.

<sup>164</sup> *Ibid.*

<sup>165</sup> Department of Homeland Security, *Privacy Impact Assessment for the REAL ID Act In Conjunction with the Notice of Proposed Rulemaking, Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*.

<sup>166</sup> *Ibid.*

Similarly, the Identity Cards Act did not address security for the National Identity Register database.<sup>167</sup> With the proposed system being unprecedentedly large at the time, the question of how to secure the information was greatly important. The system would have needed to be “highly secure to protect the data it holds from unauthorised access or modification and to protect the privacy, safety and security of the millions of citizens identified in its records.”<sup>168</sup> Academics and other advocacy groups questioned the government’s ability to safeguard the information based on prior instances of information technology (IT) security failure. These failures included the Child Support Agency, as well as Her Majesty’s Revenue and Customs (HMRC), which lost the personal data of every child in Britain, in addition to their guardian’s national insurance numbers and bank account information, in 2007.<sup>169</sup> This loss totaled the records of 25 million individuals.<sup>170</sup>

### 3. Data Integrity

Data integrity—the accuracy, consistency, and reliability of data—is key to large databases.<sup>171</sup> Data must be reliable if it is to be used for decision-making; without confidence that the data in the system is accurate, all decisions based on the data are suspect. Poor data integrity has the potential to jeopardize and compromise the entire endeavor.<sup>172</sup>

In the United Kingdom, since data is critical for the scheme’s purpose of the verifying an individual’s identity to make a decision about that individual, academics expressed concern over how inaccuracies in citizens’ data, through no fault of their own,

---

<sup>167</sup> Whitley, *The Identity Project: An Assessment of the UK Identity Cards Bill and its Implications*, 151.

<sup>168</sup> *Ibid.*, 187.

<sup>169</sup> *Ibid.*, 151; “Child Support Agency: A History of IT Failure,” July 24, 2006, <http://www.computerweekly.com/news/2240062052/Child-Support-Agency-a-history-of-IT-failure>.

<sup>170</sup> Gareth Crossman, “Nothing to Hide, Nothing to Fear?” *International Review of Law, Computers & Technology* 22, no. 1–2 (2008): 115.

<sup>171</sup> Angela Stringfellow, “What is Data Integrity? Data Protection 101,” *Digital Guardian*, last modified September 28, 2015, <https://digitalguardian.com/blog/what-data-integrity-data-protection-101>.

<sup>172</sup> James Cotton, “Data: The Importance of Accuracy, Integrity and Real-Time Integration,” *Information Builders*, December 15, 2014, <http://www.informationbuilders.com/blog/james-cotton/19152>.

would affect them.<sup>173</sup> Since the card was designed to limit access to public services, individuals may be excluded from receiving services they are authorized to receive if they do not have their card. This situation could occur if an individual was waiting for a replacement for a card that had been lost or stolen or that needed to be updated based on new information (such as a new address).<sup>174</sup>

In the United States, beyond a general concern over accuracy of the data, advocacy groups are specifically concerned over the decision not to standardize the mechanisms for correcting records. The Notice of Proposed Rulemaking indicates that states will need to adopt the fair information practice principles (FIPPs), privacy principles at the heart of the Privacy Act of 1974, to receive DHS certification that they are fulfilling the requirements of the REAL ID Act.<sup>175</sup> One of the principles is the data quality and integrity, which includes the correction and redress of records.<sup>176</sup> Privacy advocates feel that the requirement for adopting the FIPPs is not enough, since privacy and security go hand in hand.<sup>177</sup> They believe the full federal privacy standards, as specified in the Privacy Act of 1974, should be applied to the states to create uniform redress standards:

Full application of the Privacy Act requirements to government record systems is the only way to ensure that data is accurate and complete, which is especially important in this context, where mistakes and misidentifications are costly.<sup>178</sup>

---

<sup>173</sup> Paul Beynon-Davies, "The UK National Identity Card," *Journal of Information Technology Teaching Cases* 1, no. 1 (March 2011), 16.

<sup>174</sup> Paul Beynon-Davies, "Personal Identity Management and Electronic Government: The Case of the National Identity Card in the UK," *Journal of Enterprise Information Management* 20, no. 3 (2007), 266.

<sup>175</sup> Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 72 Fed. Reg. 10826 (March 9, 2007).

<sup>176</sup> *Ibid.*

<sup>177</sup> Electronic Privacy Information Center (EPIC) and Melissa Ngo, *Comments Re: DOCKET NO. DHS 2006-0030 Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes* (Washington, DC: Department of Homeland Security, 2007), 11, <http://www.regulations.gov/#!documentDetail;D=DHS-2006-0030-7239>.

<sup>178</sup> *Ibid.*, 12.

Without consistent procedures, privacy advocates say that standards for each state will be created independently, which would result in different criterion for adjudication and confusion for individuals seeking redress.<sup>179</sup>

#### **4. Linking of Databases/Expanded Sharing of Data**

Officials in the United States and the United Kingdom faced additional concern over the linking of databases—which expands the sharing of data—for both privacy and IT security reasons. In the United Kingdom, advocacy groups and academia were concerned over the linking of government and private sector databases to the National Identity Register.<sup>180</sup> The U.K. government envisioned that connecting existing government databases to the Register would be a way to obtain further facts that individuals could confirm about themselves, thus acting as additional sources of verification.<sup>181</sup> Conversely, advocacy groups were concerned that connecting multiple government databases with the Register would decrease privacy for the U.K. citizen. As the U.K. legislative framework for the government’s use of personal information strongly protects the individual, the pursuit of data sharing with other agencies represents a break from tradition.<sup>182</sup> In one example of this intended partnership, the Home Office voiced a desire to obtain legislative provision for sharing data with the U.K. Passport Service (UKPS) and the Driver and Vehicle Licensing Agency (DVLA) to facilitate identity theft and fraud prevention.<sup>183</sup>

The future commercial use of the scheme was just as concerning to these groups. The U.K. government anticipated that the scheme would be utilized by the private sector

---

<sup>179</sup> Electronic Privacy Information Center (EPIC) and Melissa Ngo, *Comments Re: DOCKET NO. DHS 2006-0030 Notice of Proposed Rulemaking: Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*, 11.

<sup>180</sup> See e.g., “ID Card Scheme an Expensive Flop,” April 26 2004, <http://www.fipr.org/press/040426id.html>; Whitley, *The Identity Project: An Assessment of the UK Identity Cards Bill and its Implications*, 235.

<sup>181</sup> *Ibid.*

<sup>182</sup> Cabinet Office, *Privacy and Data-Sharing: The Way Forward for Public Services* (London: Cabinet Office, 2002), 100.

<sup>183</sup> Whitley, *The Identity Project: An Assessment of the UK Identity Cards Bill and its Implications*, 235; Home Office, *Entitlement Cards and Identity Fraud: A Consultation Paper*, 41.

as a way for businesses to verify the identity of an individual. In this way, corporations could verify work authorization to prevent illegal working, as well as reduce fraud.<sup>184</sup> Groups were concerned that corporations, such as financial institutions or airlines, would eventually require the card to use their services.<sup>185</sup>

In the United States, many groups opposed linking the DMV databases, as required by the REAL ID Act. The primary argument against this provision was that connecting the databases would decrease the overall security of the system. Civil liberties groups believed that the requirement would make it easier for hackers to access the data in all databases, while only having to hack into one.<sup>186</sup> This connectivity was even characterized to be “more insecure than creating a large centralized database in terms of safeguarding the data” by IT Security expert and author William Eyre.<sup>187</sup> He further explained:

it has the level of intrusiveness of a national ID database in that the data is all in one place (logically or virtually, as opposed to physically) by virtue of the ability to search distributed databases from multiple entry points. In computer parlance, to say it is logically in one place means that according to the computer’s logical instructions, it matters not if all of the information is physically in one computers system...The computer’s logic, with the connections that the computers make with each other, and the speed of access and the speed with which the data can be moved from one computer to another, has the net result that the database is one “logical” entity.<sup>188</sup>

## **5. Increased Collection of Data (Type and Amount of Data Held)**

One of the arguments against the U.K. and U.S. schemes is that they increase the amount of data collected by the government so much so that the collection becomes an

---

<sup>184</sup> Whitley, *The Identity Project: An Assessment of the UK Identity Cards Bill and its Implications*, 235.

<sup>185</sup> “ID Card Scheme an Expensive Flop.”

<sup>186</sup> *Oversight of Government Management, The Federal Workforce, and the District of Columbia Subcommittee of the Committee on Homeland Security and Governmental Affairs, The Impact of Implementation: A Review of the REAL ID Act and the Western Hemisphere Travel Initiative, Senate*, 6.

<sup>187</sup> William Eyre, “Chapter 4: Technology of the Real ID Act,” in *The Real ID Act: Privacy and Government Surveillance* (El Paso, TX: LFB Scholarly Publishing LLC, 2011), 121.

<sup>188</sup> *Ibid.*

invasion of privacy. U.K. advocacy groups expressed a concern over the amount of data the Register would hold, some of which they felt was overly intrusive, like prior addresses and immigration status.<sup>189</sup> The scheme was also characterized as constituting a change in the relationship between the government and the individual:

Of course the [Identity Card Act 2006 (IDCA)] does not by itself signal the end of personal privacy in the UK. However, it does symbolize a shift in the approach of the state towards the collection of information. It is arguable that we are moving away from a society where information is not shared unless necessary, towards one where it will be shared unless there is a reason not to.<sup>190</sup>

In the United States, privacy advocates have the same concern, although there has been some debate about whether the amount of data collected and retained has increased.<sup>191</sup> Some advocates say that the government's requirements call for an increased collection and retention, although the Notice of Proposed Rulemaking published by DHS contends that no increase has occurred:<sup>192</sup>

A frequently-heard concern relates to the amount of additional information the Federal Government will have about driver's license holders and what the Federal Government will do with that data. In fact, however, neither the Real ID Act nor these proposed regulations gives the Federal Government any greater access to information than it had before.<sup>193</sup>

However, advocacy groups say that DHS is incorrect in its assertion:

DHS claims that it is not expanding data collection and retention, but it is enlarging schedules and procedures for retention and distribution of

---

<sup>189</sup> "The Case Against ID Cards," accessed September 16, 2015, <https://www.liberty-human-rights.org.uk/human-rights/privacy/id-cards/case-against-id-cards>.

<sup>190</sup> Crossman, "Nothing to Hide, Nothing to Fear?", 115.

<sup>191</sup> See e.g., *Senate Committee on Homeland Security and Governmental Affairs Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia. Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers' Licenses and Identification Cards*, S. Hrg. 110-291 Cong., 110 Cong., 1 (2007), 93, <https://www.hsdl.org/?view&did=484478>; Electronic Privacy Information Center (EPIC), *REAL ID Implementation Review: Few Benefits, Staggering Costs*, 14.

<sup>192</sup> *Senate Committee on Homeland Security and Governmental Affairs Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia. Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers' Licenses and Identification Cards*, 93.

<sup>193</sup> Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 72 Fed. Reg. 10824 (March 9, 2007).

identification documents and other personal data. This broad expansion of data collection and retention in a national database creates significant threats to privacy and security.<sup>194</sup>

These groups note that all state DMV databases must now include all fields from licenses and identity cards, as well as fulfill the requirement for collecting and retaining identity documents for up to 10 years.<sup>195</sup> These documents include SSNs, birth certificates, and citizenship documents, all of which are currently maintained in separate authoritative systems, but would be consolidated under a state's DMV to comply with the REAL ID Act.

---

<sup>194</sup> Electronic Privacy Information Center (EPIC) and Ngo, *Comments Re: DOCKET NO. DHS 2006-0030 Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*, 31.

<sup>195</sup> *Ibid.*

THIS PAGE INTENTIONALLY LEFT BLANK

## IV. CIVIL RIGHTS AND CIVIL LIBERTIES CONCERNS

This next chapter draws parallels between the civil rights and civil liberties issues found in both the REAL ID Act implementation and the NIS. Civil Rights are “basic rights and freedoms granted to citizens of a country,” that have “traditionally revolved around the basic right to be free from unequal treatment based on certain protected characteristics (race, gender, disability, etc.).”<sup>196</sup> Civil liberties can be defined as “freedom from coercive or otherwise intrusive governmental actions designed to secure the national against real or, sometimes, imagined internal and external enemies.”<sup>197</sup> The opposing arguments to both schemes based on these concerns are outlined in the following sections.

### A. RACIAL PROFILING AND DISCRIMINATION

In the United Kingdom and the United States, advocacy groups expressed concern that the schemes could increase the potential for racial profiling, which is the “consideration of race, ethnicity, or national origin by an officer of the law in deciding when and how to intervene in an enforcement capacity.” In the United Kingdom, the police themselves expressed concern about the potential for racial discrimination by police officers since the very first iterations of identity management schemes were introduced.

Discussions of a national identity card scheme began long before the Identity Cards Act. The idea was discussed as early as 1994, and the Home Secretary introduced a voluntary scheme in 1996 as a tool to assist police in fighting crime and fraud. Prior to its introduction, policing organizations voiced support for a voluntary scheme, but they, as well as the government, expressed concern over the potential negative effects that “a

---

<sup>196</sup> “Civil Liberties,” accessed November 5, 2015, <http://www.politics.co.uk/reference/civil-liberties>; “Civil Rights Vs. Civil Liberties,” accessed November 5, 2015, <http://civilrights.findlaw.com/civil-rights-overview/civil-rights-vs-civil-liberties.html>.

<sup>197</sup> Richard A. Posner, *Not a Suicide Pact: The Constitution in a Time of National Emergency* (New York; Oxford: Oxford University Press, 2006), 4.

compulsory scheme may have on the relationship between the police and ethnic minority groups.”<sup>198</sup>

In fact, the U.K. police consistently voiced opposition to making a scheme compulsory before and after its 1996 introduction for this reason.<sup>199</sup> They were acutely aware of the public’s concern over the potential for abuse by police officers, specifically the concern that prejudiced behavior would manifest itself in officers disproportionately stopping members of minority populations and requiring them to produce an ID.<sup>200</sup> The end result would be increased discrimination against minority populations. Furthermore, civil rights groups and police officers believed that the scheme would eventually evolve into a *de facto* compulsory scheme, without legislative authority, as they believed officers would come to rely on the card and could potentially treat individuals without the card as suspicious.<sup>201</sup>

In recent years, the U.K. police have actively supported the voluntary NIS as they have done in the past. However, organizations that previously only supported a voluntary scheme, such as Association of Chief Police Officers, have changed their mind, possibly due to the heightened security threats facing Britain:<sup>202</sup>

The overwhelming view within ACPO is that the ID card scheme should operate on a “compulsory” and “universal” basis. Whilst we understand the rationale behind the proposed incremental approach we believe there are benefits to be accrued if individuals were required to carry or produce the card upon request to an appropriate authority. Those engaged in criminal activity will not be deterred if the scheme is not robust.”<sup>203</sup>

---

<sup>198</sup> Adrian Beck and Kate Broadhurst, “National Identity Cards: The Impact on the Relationship between the Police and Ethnic Minority Groups,” *Policing and Society* 8, no. 4 (1998): 402–403.

<sup>199</sup> *Ibid.*, 417.

<sup>200</sup> *Ibid.*, 418.

<sup>201</sup> *Ibid.*, 420.

<sup>202</sup> Whitley, *The Identity Project: An Assessment of the UK Identity Cards Bill and its Implications*, 116–117.

<sup>203</sup> House of Commons, Home Affairs Committee, Select Committee on Home Affairs Written Evidence Session 2003–04, *Memorandum submitted by the Association of Chief Police Officers*, April 2004, <http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/130we02.htm>.

In discussions of the NIS, police have cited the benefits of cards in improving stop and search procedures, as it will allow officers to verify the identity of individuals quickly using their ID cards.<sup>204</sup> They state that using mobile readers to scan an individuals' ID card will allow them to identify individuals in violation of Anti-Social Behavior Orders (ASBOs) or Football Banning Orders expeditiously, both of which prevent individuals from visiting particular locations.<sup>205</sup> Police anticipate that the cards will ultimately increase safety and security.

Ironically, stop and search procedures using the national ID cards were noted as an area of concern early on in the NIS' implementation as they augment insecurity in minority populations due to their potential for abuse. In its review of the Identity Cards Act, the Commission for Racial Equality (CRE) felt that discrimination could occur in four areas, including "police stops and searches, service provision and employment, disclosure without consent, [and with] gypsies and travelers."<sup>206</sup> The CRE expressed concerns regarding the statistically disproportionate use of stop and search procedures on ethnic minorities. They believed that once the scheme became compulsory, as was intended by the government, this situation would only be exacerbated with police requiring a disproportionate number of minority individuals to display their cards.<sup>207</sup> The CRE also felt that the Secretary of State's power to "provide information without the consent of the individual" could lead to increased racial or religious profiling and noted that the requirement to provide an address or face fines will negatively impact gypsies and travellers, cultural and ethnic communities in the United Kingdom, some of which are nomadic.<sup>208</sup>

---

<sup>204</sup> House of Commons, Home Affairs Committee, Select Committee on Home Affairs Written Evidence Session 2003–04, *Memorandum submitted by the Association of Chief Police Officers*.

<sup>205</sup> *Ibid.*

<sup>206</sup> Home Office, *Identity Cards: A Summary of Findings from the Consultation on Legislation on Identity Cards*, 65, 102.

<sup>207</sup> *Ibid.*, 65.

<sup>208</sup> *Ibid.*, 65–66.; "Gypsy, Roma and Traveller Communities," National Association of Teachers of Travellers + Other Professionals, accessed October 13, 2015, <http://www.natt.org.uk/gypsy-roma-and-traveller-communities>.

In the 2003–04 session, the House of Commons Home Affairs Committee agreed with CRE that “the Bill should be accompanied by a full Race Impact Assessment and that there should be a further Assessment at the time of the move to compulsion.”<sup>209</sup> The chair of the Commission for Racial Equality “argued that there was little hard evidence about the impact of an identity card scheme on different ethnic groups and communities in the United Kingdom, but experience in other European countries was not encouraging.”<sup>210</sup>

The government conducted a partial race equality impact assessment for the scheme in 2004 to identify major issues. They found the scheme to be non-discriminatory because it was applicable to everyone residing in the United Kingdom for longer than three months.<sup>211</sup> The assessment noted that the scheme must comply with the Race Relations Act 1976 as amended by the Race Relations (Amendment) Act 2000, meaning that it “must have due regard to the elimination of unlawful racial discrimination, the promotion of equal opportunities and good relations between people from different racial groups.”<sup>212</sup> The document registered the same concern as many of the advocacy and civil rights organizations representing ethnic minority groups regarding the government’s stipulation that individuals present their ID cards to receive services:

People from black and minority ethnic groups might be asked to provide the card as proof of identity more frequently than white people which in some cases might lead to people being denied access to services to which they are entitled if they cannot produce their card.”<sup>213</sup>

This concern is compounded when discussions of the card turn to its broader use in society:

There were concerns that the cards will be used detrimentally due to institutional racism existing in public and private service authorities,

---

<sup>209</sup> House of Commons, Home Affairs Committee, *Identity Cards: Fourth Report of Session 2003–04, Volume I*, 63.

<sup>210</sup> *Ibid.*

<sup>211</sup> Home Office, *Legislation on Identity Cards: A Consultation* (UK: The Stationery Office Limited, 2004), 112.

<sup>212</sup> *Ibid.*, 111–112.

<sup>213</sup> *Ibid.*, 115.

particularly where there was a reliance on discretion. A view expressed was that, in this context, a compulsory scheme would be less discriminatory as everyone would be able to produce a card.<sup>214</sup>

In a similar vein, within the United States, advocacy groups warn that because holders of REAL ID driver's licenses and identity cards have been verified to have U.S. citizenship, those who do not obtain cards but "look foreign" will be subject to increased scrutiny and discrimination.<sup>215</sup> In addition, they believe that the REAL ID Act will result in increased identity checks for minorities and foster a climate of suspicion against those without IDs, "Failure to carry a national I.D. card would likely come to be viewed as a reason for search, detention or arrest of minorities."<sup>216</sup>

## **B. TRACKING INDIVIDUALS**

Due to concerns about the potential ability of the government or commercial entities to track individuals based on the data they provided, ethnicity was not a field the U.K. government planned to record in the National Identity Register or on the face of the ID card. As part of the scheme, an audit trail would have been recorded for every check of the National Identity Register; every query made by government agencies, as well as future commercial entities, would be captured and stored indefinitely.<sup>217</sup> The data recorded for each check of the database is known as transactional data, which is "data that records events taking place between individuals, groups, and organisations."<sup>218</sup> Advocacy groups were concerned about what might be done with the data, noting, "Personal identity data combined with historical and transactional data held about the individual would make it theoretically possible for government to build behavioural

---

<sup>214</sup> Home Office, *Legislation on Identity Cards: A Consultation*, 115–116.

<sup>215</sup> Electronic Privacy Information Center (EPIC) and Ngo, *Comments Re: DOCKET NO. DHS 2006-0030 Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*, 12.

<sup>216</sup> "5 Problems with National ID Cards," accessed October 19, 2015, <https://www.aclu.org/5-problems-national-id-cards>.

<sup>217</sup> Ward, *The Identity Cards Bill (Bill 9 of 2005-06) House of Commons Research Paper 05/43*, 47.

<sup>218</sup> Beynon-Davies, *Personal Identity Management and Electronic Government: The Case of the National Identity Card in the UK*, 265.

profiles of its citizenry.”<sup>219</sup> Since U.K. citizens are some of “the most monitored in the world,” privacy-conscious individuals believe the combination of closed-circuit television (CCTV) with transactional data could be taken advantage of by future authoritarian governments.<sup>220</sup>

In the United States, advocacy groups have the same concerns as in the United Kingdom that citizens could be tracked based on their race, which would increase the potential for discrimination against them. These groups were troubled by the fact that the government had not taken steps to prevent race from being recorded on the driver’s licenses and identity cards, as the U.K. government had when they decided not to record ethnicity on the National Identity Register or on the cards.

In the proposed rulemaking, DHS stated that it considered five different types of MRT.<sup>221</sup> These included a 1D bar code, a 2D bar code, an optical stripe, a contact integrated circuit chip, and a contactless integrated circuit chip.<sup>222</sup> Ultimately, they selected the PDF-417 2D bar code as it is the most common MRT standard and is already used by 45 states.<sup>223</sup> DHS also proposed the standard data elements consist of the majority of the data elements found in the 2005 American Association of Motor Vehicle Administrators (AAMVA) Driver’s License/Identification Card Design Specifications, Annex D:

The AAMVA list of data elements includes expiration date, bearer’s name, issue date, date of birth, gender, address, and a unique identification number. DHS proposes that States consider storing in the machine-readable zone (MRZ) only the minimum data elements necessary for the purpose for which the REAL IDs will be used.<sup>224</sup>

---

<sup>219</sup> Beynon-Davies, *The UK National Identity Card*, 15.

<sup>220</sup> Beynon-Davies, *Personal Identity Management and Electronic Government: The Case of the National Identity Card in the UK*, 265.

<sup>221</sup> Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 72 Fed. Reg. 10837 (March 9, 2007).

<sup>222</sup> *Ibid.*

<sup>223</sup> *Ibid.*, 10837–10838.

<sup>224</sup> For the full list of data elements, see Appendix B. Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 72 Fed. Reg. 10838.

Race/ethnicity is an optional data element in the 2005 AAMVA driver's license/identification card design specifications. Civil libertarians were particularly concerned about the potential inclusion of this field, as demonstrated in the written remarks from Jim Harper, Director of Information Policy Studies for libertarian think-tank, The CATO Institute, at a 2007 Congressional hearing on the REAL ID Act:

DHS does not require all the data elements from the standard, and it does not require the "race/ethnicity" data element, but the standard it has chosen will likely be adopted in its entirety by state driver licensing bureaus. The DHS has done nothing to prevent or even discourage the placement of race and ethnicity in the machine readable zones of this national ID card.<sup>225</sup>

Scholars have noted that while DHS addressed the concern in the final rule for the proposed regulations—stating that "the AAMVA standard was not intended to include race as a data element in the MRZ for REAL ID"—it did not explicitly prevented its inclusion.<sup>226</sup> States still retained the ability add other data elements into their state licenses and identity cards, including the race/ethnicity field, as they saw fit.<sup>227</sup>

The concern about DHS's refusal to prevent race from being recorded on state driver's license and ID cards was compounded by DHS' decision not to mandate the encryption of data stored on the 2D bar code, the MRZ located on the cards. DHS considered requiring encryption to increase the security of data stored on the cards and reduce the privacy risk.<sup>228</sup> If the MRZ is not encrypted then retailers can collect any data stored on the card when it is swiped at their businesses. The data about the individuals, along with their purchase history, can be used by that company or packaged and resold to

---

<sup>225</sup> *Senate Committee on Homeland Security and Governmental Affairs Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia. Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers' Licenses and Identification Cards*, 98.

<sup>226</sup> Eyre, *Chapter 4: Technology of the Real ID Act*, 115; Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 73 Fed. Reg. 5305 (January 29, 2008).

<sup>227</sup> *Ibid.*, 116.

<sup>228</sup> Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 72 Fed. Reg. 10838.

other companies.<sup>229</sup> Privacy and civil liberties groups recognized that the lack of encryption, and the ability of companies to access the data, could result in commercial entities tracking an individuals' race, which they could then use to discriminate against them:

in May 2008, many Americans may start carrying nationally uniform cards that include race or ethnicity in machine-readable formats. This will be available for scanning and collection by anyone with a bar code reader. Government agencies and corporations alike may affiliate racial and ethnic data more closely than ever before with information about our travels through the economy and society.<sup>230</sup>

In fact, the standardization of the MRT and the data elements makes skimming this information even easier. Prior to the REAL ID Act, states had different types of MRT on their licenses and identification cards. Privacy groups have argued that uniformity in the technology and the data held on the cards will increase the likelihood that cards will be used in more contexts, primarily due to the economies of scale for commercial entities in purchasing card readers and software. The standardization of driver's licenses and ID cards will mean that all cards from any state could be scanned by a single card-reader, which makes it cost efficient for commercial entities to invest in them to record and use the data.<sup>231</sup> Despite these concerns, DHS decided not to propose the encryption of the MRZ because of the technical and security complexities involved in enabling law enforcement to decrypt the data.

### **C. SURVEILLANCE SOCIETY**

The creation of identity cards is viewed as contributing to the development of a surveillance society. The U.K. Information Commissioner defined the surveillance society as the following:

---

<sup>229</sup> *Oversight of Government Management, The Federal Workforce, and the District of Columbia Subcommittee of the Committee on Homeland Security and Governmental Affairs, The Impact of Implementation: A Review of the REAL ID Act and the Western Hemisphere Travel Initiative, Senate*, 10.

<sup>230</sup> *Senate Committee on Homeland Security and Governmental Affairs Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia. Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers' Licenses and Identification Cards*, 39–40.

<sup>231</sup> *Ibid.*, 94.

The surveillance society is a society which is organised and structured using surveillance based techniques. To be under surveillance means having information about one's movements and activities recorded by technologies, on behalf of the organisations and governments that structure our society. This information is then sorted, sifted and categorised, and used as a basis for decisions which affect our life chances. Such decisions concern our entitlement and access to benefits, work, products and services and criminal justice; our health and well-being and our movement through public and private spaces.<sup>232</sup>

Surveillance was further defined as:

Where we find purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection, we are looking at surveillance.<sup>233</sup>

As previously mentioned, the REAL ID compliant driver's licenses and identity cards and the U.K. national identity card were criticized for their intrusion into personal privacy and their impact on free movement since they can be tracked by the government and commercial entities. Recording an individual's personal data can have additional unintended effects on personal privacy and civil liberties and can increase the potential for discrimination. Social sorting and profiling from the use of data mining are two ways that a person's civil liberties can be impacted.

Social sorting is the act of analyzing and categorizing personal information in databases to "define target markets and risky populations."<sup>234</sup> This practice of digitally segmenting the population can have unintended consequences, in which certain groups receive different opportunities. The purposes of the card, such as the prevention of terrorism and identity fraud, lend themselves to the establishment of dichotomies of people within the system (i.e., terrorist/non-terrorist, legitimate beneficiary/fraudulent beneficiary) and can further disadvantage already disenfranchised groups:<sup>235</sup>

---

<sup>232</sup> The Surveillance Studies Network, *A Report on the Surveillance Society: Summary Report for the Information Commissioner*, 2006, 2.

<sup>233</sup> *Ibid.*, 3.

<sup>234</sup> *Ibid.*

<sup>235</sup> *Ibid.*, 4; David Lyon, "National ID Cards: Crime-Control, Citizenship and Social Sorting," *Policing: A Journal of Policy and Practice* 1, no. 1 (January 1, 2007), 115.

Terrorist suspects are likely to be members of minority groups; claimants to government benefits and services are likely to be already disadvantaged and immigrants, whether legal or not, are also in positions of relative powerlessness. The social sorting of new IDs touches the lives of the weakest and most marginalized member of the population.<sup>236</sup>

In addition, the report, “Surveillance Society,” warned that data mining poses the danger of inadvertently grouping individuals into stigmatized categories. Data mining is “the mass automated profiling and matching of otherwise innocuous information to throw up anomalies that might indicated some illicit behavior is taking place.”<sup>237</sup> It can be used by the government as a way of determining who may be up to no good:

Significantly, use of data-mining and profiling to identify risks shifts surveillance practices toward the screening of the actions and transactions of the general population. This screening can then be used to target interventions on people or groups of people who are considered to be at risk or to pose risks for others.<sup>238</sup>

However, scholars note that these practices can lead to racial and religious profiling.<sup>239</sup> Some argue that data mining can reduce the potential for discrimination if it is a computer, rather than a human, that generates the profile used based on past behaviors of terrorists, which thus removes human bias from the equation.<sup>240</sup> However, human judgment is still required at the onset in deciding who constitutes a known terrorist.<sup>241</sup> Furthermore, data mining can also cause people to be deemed a potential threat simply based on their similarity to others who have committed criminal acts.<sup>242</sup> It is a shortcoming of law enforcement and counterterrorism efforts scholars say, because it

---

<sup>236</sup> Lyon, “National ID Cards: Crime-Control, Citizenship and Social Sorting,” 115.

<sup>237</sup> Crossman, *Nothing to Hide, Nothing to Fear?*, 117.

<sup>238</sup> The Surveillance Studies Network, *A Report on the Surveillance Society: Summary Report for the Information Commissioner*, 6.

<sup>239</sup> *Ibid.*, 4.; Crossman, *Nothing to Hide, Nothing to Fear?*, 117.

<sup>240</sup> Daniel J. Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security* (New Haven, CT: Yale University Press, 2011), 190–191.

<sup>241</sup> *Ibid.*, 191.

<sup>242</sup> The Surveillance Studies Network, *A Report on the Surveillance Society: Summary Report for the Information Commissioner*, 4; Crossman, *Nothing to Hide, Nothing to Fear?*, 117.

focuses entirely on prior patterns of behavior, while failing to imagine the potential for future adversaries that do not fit the existing profile.<sup>243</sup>

It is important to note that a fine line exists between profiling and intelligence-led identification; the first is based on a generalization of people in a specific group, while the other is based on behavior consistent with perpetrating crime that police are trying to prevent.<sup>244</sup> It is profiling, rather than intelligence-led identification, that concerns advocates as “profiling to identify people as potential criminals’ risks treating all people who fit a certain profile as potential terrorists or criminals.”<sup>245</sup>

Moreover, some believe profiling is not very effective. Legal scholar and former U.S. Court of Appeals judge Richard Posner argues that racial profiling does not reduce the amount of crime occurring, but only creates a shift in who is committing it as heightened scrutiny of one group will pave the way for another group to step in to the “open market.”<sup>246</sup> Similarly, he argues that racial profiling will not prevent terrorism because these groups will simply change whom they chose as operatives to avoid scrutiny and prevent detection.<sup>247</sup> Due to the ability of criminals and terrorists to thwart the use of profiling by law enforcement and the intelligence community, the benefit is minimal compared to the harm and alienation felt by minority communities.

---

<sup>243</sup> Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security*, 188.

<sup>244</sup> Crossman, *Nothing to Hide, Nothing to Fear?*, 117.

<sup>245</sup> House of Commons, Home Affairs Committee, *A Surveillance Society? Fifth Report of Session 2007-08 Volume 1*, 36–37.

<sup>246</sup> Posner, *Not a Suicide Pact: The Constitution in a Time of National Emergency*, 117.

<sup>247</sup> *Ibid.*, 117–118.

THIS PAGE INTENTIONALLY LEFT BLANK

## V. PUBLIC RESPONSE

This chapter focuses on the public's reception of and reaction to the REAL ID Act in the United States and the NIS in the United Kingdom. Specifically, it explores issues surrounding government transparency, public engagement, public acceptance, and the historical and cultural factors that informed the discussion of the REAL ID Act and NIS. The chapter discusses how both schemes encountered a lack of public debate and government transparency and how this lack has affected their political success. It explores the schemes' levels of public acceptance and how public support is affected by discussions of how the scheme will actually function. Finally, it explains how cultural and historical factors have demonstrated a resistance to identity management policies, which has manifested itself throughout the development and implementation of the REAL ID Act and National Identity Scheme. This resistance may again prove to be an impediment to lasting success.

### A. PUBLIC ENGAGEMENT AND GOVERNMENT TRANSPARENCY

Transparency is key to the public's adoption of a system:

Research has shown that a lack of transparency and accountability in the collection and use of personal information may create high levels of distrust. This lack of trust can, in turn, affect the adoption and use of information-collecting technologies, such as smart cards.<sup>248</sup>

Furthermore, the public's acceptance of a system is critical to the systems' success:

Many consider the acceptance of biometric systems by users groups an important requirement for success. It is believed that without user acceptance, perfectly functioning systems are doomed to fail.<sup>249</sup>

Both the U.S. and U.K. schemes experienced a lack of public engagement in the development of the foundational legislation. In general, the lack of public debate and

---

<sup>248</sup> Joinson et al., "Watching Me, Watching You: Privacy Attitudes and Reactions to Identity Card Implementation Scenarios in the United Kingdom," 336.

<sup>249</sup> Aaron K. Martin, "National Identity Infrastructures: Lessons from the United Kingdom," in *ICT Critical Infrastructures and Society*, ed. Magda David Hercheui and others, vol. 386 (Berlin: Springer, 2012), 45.

government transparency proved to be a political stumbling block that threatened the success of both schemes throughout their implementation.

The REAL ID Act did not get the benefit of public scrutiny. When the legislation was passed in 2005, it was included as part of a bill for military spending and aid to countries affected by the December 2004 tsunami and March 2005 earthquake, as well as by the Avian influenza virus.<sup>250</sup> As such, it passed quickly without debate. Opponents of the Act argued that it was not politically feasible for Congressmen to oppose the bill and were critical of the fact that the REAL ID Act language was appended after the bill passed the House, which prevented discussion or the potential to amend the text.<sup>251</sup> In the month prior to the Act's passage, 12 Republican and Democratic Senators wrote a letter to Senate Majority Leader Bill Frist asking him to oppose the inclusion of the REAL ID language in the emergency supplemental spending bill. Instead, they asked him to refer the legislation to the Senate Judiciary Committee for discussion and debate. They wrote, "Legislating in such a complex area without the benefit of hearings and expert testimony is a dubious exercise and one that subverts the Senate's deliberative process."<sup>252</sup>

While the Republican-controlled House Judiciary Committee argued that the Senate had the chance for debate during the year prior when most of the provisions were included in the 2004 Intelligence Reform and Terrorism Prevention Act (they were taken out for the bill to pass the Senate), privacy advocates dismiss that claim as "procedural maneuvering" and cite the lack of hearings during that time.<sup>253</sup>

---

<sup>250</sup> "All Bill Information (Except Text) for H.R. 1268—Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005," accessed June 23, 2015, <https://www.congress.gov/bill/109th-congress/house-bill/1268/all-info>.

<sup>251</sup> Harper, "Testimony regarding SB 262 and the U.S. Federal REAL ID Act: Committee on Transportation New Hampshire State Senate."

<sup>252</sup> "Twelve Senators Urge Frist to Keep REAL ID Act Off Supplemental Appropriations Bill," April 12, 2005, <https://www.hsgac.senate.gov/media/majority-media/twelve-senators-urge-frist-to-keep-real-id-act-off-supplemental-appropriations-bill>.

<sup>253</sup> "House-Passed 'Real ID Act' Folded into Supplemental Spending Bill," in *CQ Almanac 2005*, 61st ed., 13-3-13-4, Washington, DC: Congressional Quarterly, 2006, <http://library.cqpress.com/cqalmanac/cqal05-766-20098-1042121>; Kim Zetter, "National ID Battle Continues," *Wired*, May 12, 2005, <http://archive.wired.com/politics/security/news/2005/05/67498?currentPage=all>.

Academics note the quick passage of the bill and lack of public debate meant that lawmakers did not have time to build support for the policy:

[W]hile the Bush administration was very effective in capitalizing on the national mood and policy circumstances to get the law passed, it never allowed sufficient open debate of the policy to shake up the policy subsystems and soften (but not silence) the opposition, nor was it effective in building a strong, long-lasting coalition to support the policy change.<sup>254</sup>

Furthermore, the lack of sustained support is detrimental to the long-term success of a policy:

As the multiple streams policy literature suggests, national crises may offer a window of opportunity for policy entrepreneurs to get a policy on the agenda or even to get it passed under a certain national mood. However, they may be insufficient to sustain a policy shift in the long run unless policy entrepreneurs also invest time and political capital to realign the established interests. The development of the Real ID Act also affirms why a major policy shift often takes decades to build up momentum in a democratic system. Policy options have to be sorted out, debated, evaluated, and examined critically by diverse groups and all these need time. The translation from an idea to a policy can be painfully slow, but rushing it through the political system can actually be counterproductive and may risk policy backpedaling later.<sup>255</sup>

The lack of public debate partially explains the continued opposition from state governors and legislatures. In 2007, the Maine legislature passed a resolution refusing to implement the law, becoming the first state to do so.<sup>256</sup> It was not the only one. Many states have either passed resolutions or legislation to resist compliance, petitioned DHS to repeal or revise the minimum standards, or just flat out refused to participate.<sup>257</sup> DHS

---

<sup>254</sup> Ya Ni and Tat-Kei Ho, *A Quiet Revolution Or a Flashy Blip? the Real ID Act and U.S. National Identification System Reform*, 1073.

<sup>255</sup> Ibid.

<sup>256</sup> Harper, "Testimony regarding SB 262 and the U.S. Federal REAL ID Act: Committee on Transportation New Hampshire State Senate."

<sup>257</sup> These states include Alaska, Arizona, Colorado, Hawaii, Idaho, Illinois, Louisiana, Maine, Massachusetts, Michigan, Minnesota, Missouri, Montana, Nebraska, New Hampshire, North Dakota, Oklahoma, Oregon, Pennsylvania, South Carolina, South Dakota, Tennessee, Utah, Virginia, and Washington. Milberg, "National Security Surveillance and National Authentication System: The National Identification Debate: "REAL ID "and Voter Identification," 454; Harper, "Testimony regarding SB 262 and the U.S. Federal REAL ID Act: Committee on Transportation New Hampshire State Senate"; Jim Harper, *REAL ID: A State-by-State Update* (Washington, DC: CATO Institute, 2014).

repeatedly and deliberately interpreted letters from governors expressing how they would be implementing standards for their states—independent from the minimum standards dictated in the Federal Register—as requests for extensions.<sup>258</sup> Still, the Department is able to say that currently, 54 out of 56 jurisdictions are in compliance—with 31 of those having an extension until January, October, or June 2016; only two are considered to be non-compliant.<sup>259</sup> However, the requirement for having a REAL ID-compliant driver’s license or identity card to board an aircraft has been delayed to no sooner than 2016.<sup>260</sup> While Congress believes that the residents of non-compliant states fault their governors and legislatures, opponents say that Congress, DHS, and the Transportation Security Administration (TSA) will be recognized as the source of the problem when the ID requirement for domestic flights comes to pass.<sup>261</sup>

In the United Kingdom, it was argued that while the government held several consultations to solicit public input, the process of democratic participation was conducted superficially.<sup>262</sup> The government’s plans for the architecture of the scheme, including the national centralized database (the National Identity Register), a consistent and permanent identifier (National Identity Registration Number), and the inclusion of biometrics on the ID card, did not change at all throughout the process.<sup>263</sup> Apart from discussions regarding the inclusion of medical information on the card, the government did not appear genuinely to evaluate the public’s suggestions or input on how to structure the scheme.<sup>264</sup> In spite of the lack of impact the public consultation had on the scheme, the legislation still benefited from several years’ worth of debate that included expert testimony and in-depth analysis, which the United States did not have.

---

<sup>258</sup> Harper, “Testimony regarding SB 262 and the U.S. Federal REAL ID Act: Committee on Transportation New Hampshire State Senate.”

<sup>259</sup> “REAL ID Enforcement in Brief,” accessed October 25, 2015, <http://www.dhs.gov/real-id-enforcement-brief>.

<sup>260</sup> *Ibid.*

<sup>261</sup> Harper, “Testimony regarding SB 262 and the U.S. Federal REAL ID Act: Committee on Transportation New Hampshire State Senate”; Zetter, “National ID Battle Continues.”

<sup>262</sup> Lyon, “National ID Cards: Crime-Control, Citizenship and Social Sorting,” 114.

<sup>263</sup> Whitley, *The Identity Project: An Assessment of the UK Identity Cards Bill and its Implications*, 40.

<sup>264</sup> *Ibid.*

However, the LSE studied the scheme intensely and found that the government had not built a “foundation of public trust and confidence.”<sup>265</sup> While several public consultations had been held prior to the Identity Card Act’s passage, the government’s lack of transparency into how the scheme’s cost was calculated created mistrust in the general public, who were not convinced that the government could prevent the scheme from running over budget. The LSE developed and publicized an independent cost estimate far higher than the Home Offices’. While the Home Office believed the scheme would cost about £5.84 billion over a 10-year period, the LSE estimated the cost to be between £10.6 billion and £19.2 billion.<sup>266</sup>

This discrepancy and the controversy surrounding it caused the Home Office to bring in an independent contractor, KPMG, to review. The independent analysis did not increase transparency, however, as the government was unwilling to disclose its costing model to Parliament, stating that the details were “commercial confidential.”<sup>267</sup> Eventually, the scope of the government’s cost parameters was revealed during a public meeting; it proved to be significantly narrower than the LSE’s. This disclosure informed the public that the cost of the scheme would be far greater than the original estimate provided by the Home Office. In response, one of the Parliamentary Houses approved an amendment to delay implementation until the scheme’s full costs were presented and approved.<sup>268</sup>

In sum, both schemes demonstrated a lack of public engagement, whether intentionally through an accelerated passage of the law, as occurred in the United States, or perhaps unintentionally by failing to adjust the scheme adequately to address major public concerns brought up in consultation, as occurred in the United Kingdom. While the lack of public engagement was just one factor that led to the repeal of the U.K. scheme, it remains to be seen whether or not the U.S. government has generated enough

---

<sup>265</sup> Whitley, *The Identity Project: An Assessment of the UK Identity Cards Bill and its Implications*, 9.

<sup>266</sup> Whitley et al., “Reflections on the Academic Policy Analysis Process and the UK Identity Cards Scheme,” 54.

<sup>267</sup> *Ibid.*, 55.

<sup>268</sup> *Ibid.*, 56.

momentum to sustain the policy of requiring REAL ID compliant licenses and identity cards for entering federal facilities—and boarding commercial aircrafts—on a long-term basis.

## **B. PUBLIC ACCEPTANCE**

The current level of public support for the REAL ID Act is difficult to determine. Few national opinion polls have been conducted within the United States; these few have been funded by industry trade organizations, which casts doubt on the objectivity of the results. A poll conducted in 2007 by Public Opinion Strategies, funded by the Information Technology Association of America (ITAA), found that 82 percent of adults favored the “new national rules and regulations regarding state-issued driver’s licenses and identification cards designed to help prevent terrorism, identity theft and other crimes.”<sup>269</sup>

More data available is available on American opinions of national identity cards. Polling has shown that the level of approval for national ID cards is similar to that in the United Kingdom. A 2001 poll conducted by Pew Research Center, found that 70 percent of Americans favored the adoption of a national ID card, which was an all-time high for the country.<sup>270</sup> By August 2002, that support had dropped to 59 percent and remained steady at 57 percent during polls conducted in January and December 2006.<sup>271</sup>

Additionally, research has shown that when fees are brought to the public’s attention, support for the scheme decreases. In a 2006 study of Michigan residents, only 40 percent of respondents supported the validation and storage of documentation by the state when it was noted that this provision could heighten costs and wait times.<sup>272</sup> Overall, the study found that 61 percent of respondents supported the introduction of a

---

<sup>269</sup> “Survey Shows Public Support for Goals Similar to Real ID,” accessed October 25, 2015, <http://www.govtech.com/security/Survey-Shows-Public-Support-for-Goals.html>.

<sup>270</sup> “Free Trade Agreements Get a Mixed Review,” accessed December 26, 2015, <http://www.people-press.org/2006/12/19/free-trade-agreements-get-a-mixed-review/>.

<sup>271</sup> *Ibid.*

<sup>272</sup> Bali, “Tinkering Toward a National Identification System: An Experiment on Policy Attitudes,” 242.

national ID card, while 69 percent supported the REAL ID Act.<sup>273</sup> However, at the time of the study, the REAL ID Act regulations had not yet been implemented, and as such, the author noted that Americans may not have known much about the legislation and that public opinion could change.<sup>274</sup> Since then, no national polls about national identity cards or the REAL ID Act have been conducted.<sup>275</sup>

In the United Kingdom, despite the concern over cost, the public's support for the NIS was generally very high throughout its implementation until the scheme was repealed. Polls administered in 2003 and 2004 by groups for and against the scheme revealed around an 80 percent approval rating.<sup>276</sup> Although the general public supported the scheme in the polls, it was questionable how much they understood about it. A 2004 poll showed that 73 percent of British people knew "just a little" to nothing about the scheme.<sup>277</sup> Only 5 percent knew "a great deal." The lack of general knowledge is unsurprising, considering that the U.K. government spent more time deciding how it would enroll biometrics, focusing its marketing efforts on companies that could help them in this endeavor, than on informing the general public of how the scheme would benefit them.<sup>278</sup> The lack of focus on the scheme's intended uses was another reason that critics questioned whether the scheme was just a "massive government data collection exercise."<sup>279</sup>

Additionally, when the public was asked about specific parts of the scheme, their trust clearly waned.<sup>280</sup> This trend indicated support for the general purposes of the

---

<sup>273</sup> Bali, "Tinkering Toward a National Identification System: An Experiment on Policy Attitudes," 241–242.

<sup>274</sup> *Ibid.*, 235.

<sup>275</sup> The Pew Research Center, Marist College Institute for Public Opinion, Polling Report, Quinnipiac University Poll, Washington Post Polls, Fed Stats, Data.gov, ProQuest, LexusNexus were all consulted.

<sup>276</sup> Whitley, *The Identity Project: An Assessment of the UK Identity Cards Bill and its Implications*, 139.

<sup>277</sup> "British 'Favour ID Cards'," accessed October 24, 2015, <https://www.ipsos-mori.com/research/publications/researcharchive/622/British-Favour-ID-Cards.aspx>.

<sup>278</sup> Martin, "National Identity Infrastructures: Lessons from the United Kingdom," 49–50.

<sup>279</sup> *Ibid.*

<sup>280</sup> Whitley, *The Identity Project: An Assessment of the UK Identity Cards Bill and its Implications*, 139.

scheme (e.g., preventing terrorism, reducing illegal working, preventing identity theft, etc.) but not necessarily how the government was going about achieving those goals.<sup>281</sup> As in the United States, disapproval manifested when polls focused on costs, particularly when the public was asked about paying for the ID card and about the fines associated with not informing the government of their new address, in the event that a person moves.<sup>282</sup>

Academics also found a discrepancy in the level of support for the scheme. A 2005–2006 study of U.K. citizens and residents focused on the type of database proposed and what the authors describe as the “level of compulsion” involved. The study’s participants were asked how they felt about the use of a centralized database in the scheme, versus an architecture without a centralized database, in which personal information “would be held on [an ID] card and backed up locally in a secure database maintained by a trusted third party (e.g., a bank, police station, or [lawyers’ office].”<sup>283</sup>

Respondents also were asked how they felt about a registration process that was very structured, which the authors called “high compulsion,” versus a registration process that was very flexible, termed “low compulsion.” Participants received instruction that high compulsion meant that individuals would be given an exact time and place to register their personal and biometric information, and would incur a fine if they failed to appear.<sup>284</sup> Low compulsion meant that individuals could visit a location of their choosing at the time of their choosing to provide personal information and a biometric of their choosing (e.g., a fingerprint, facial photograph, or iris scan).<sup>285</sup> The authors found that “the largest shift against ID cards was when the level of compulsion was high (e.g., no choice when to go for the biometric scanning, possible fines) combined with a centralized

---

<sup>281</sup> Whitley, *The Identity Project: An Assessment of the UK Identity Cards Bill and its Implications*, 139.

<sup>282</sup> *Ibid.*, 140; Bali, “Tinkering Toward a National Identification System: An Experiment on Policy Attitudes,” 236.

<sup>283</sup> Joinson et al., *Watching Me, Watching You: Privacy Attitudes and Reactions to Identity Card Implementation Scenarios in the United Kingdom*, 338.

<sup>284</sup> *Ibid.*, 337.

<sup>285</sup> *Ibid.*, 338.

government database.”<sup>286</sup> This approach was the scheme proposed by the U.K. government. The survey also found that “regardless of the type of implementations scenario, attitudes towards ID cards moved toward the ‘against’ end of the scale following the scenarios.”<sup>287</sup> This datum lends credence to the theory that the public supports the scheme without fully understanding how it will be implemented; once people have a better understanding of how the scheme will function, and what they will be required to do, support decreases.

### C. CULTURAL AND HISTORICAL FACTORS

National identity schemes, identity cards, or unique identifiers have historical context within the United Kingdom and United States that carry negative connotations for their citizens and residents. While the United States has never implemented a national identity management scheme, Americans have a history of rejecting the institutionalization of unique identifiers when they sense that the potential impact to the privacy and security of an individual’s information—if compromised—has become too great. A prime example is the response to the SSN over time. Created in 1939 as an account number for the Social Security System, its use has greatly expanded through the years.<sup>288</sup> Despite its ubiquity, significant efforts have been made to prevent the SSN from being considered a universal identifier. When the Privacy Act of 1974 was drafted, a provision was included that explicitly prevented government agencies from denying individuals their lawful rights, benefits, or privileges if they refused to provide their SSN.<sup>289</sup> Congress added this provision due to the concern over the large amounts of personal data they saw being linked to a single identifier. It was thought that by including

---

<sup>286</sup> Joinson et al., *Watching Me, Watching You: Privacy Attitudes and Reactions to Identity Card Implementation Scenarios in the United Kingdom*, 339.

<sup>287</sup> *Ibid.*

<sup>288</sup> Electronic Privacy Information Center (EPIC), *REAL ID Implementation Review: Few Benefits, Staggering Costs*, 1.

<sup>289</sup> “Overview of the Privacy Act of 1974: Social Security Number Usage,” accessed October 27, 2015, <http://www.justice.gov/opcl/social-security-number-usage>.

this language, fewer people would provide their SSN if not required, and thus, fewer agencies would use it as an identifier.<sup>290</sup>

Later in 1977, the U.S. Privacy Protection Study Commission issued a report entitled, “Personal Privacy in an Information Society,” in which the Commission described their fear that “a government record system, such as that maintained by the Social Security Administration or the Internal Revenue Service, will become a de facto central population register unless prevented by conscious policy decisions.”<sup>291</sup> The Commission recommended, “the Federal government should act positively to halt the incremental drift toward creation of a standard universal label and central population register.”<sup>292</sup>

In 1993, the Clinton Administration introduced the National Health Security Plan, under which all Americans would be issued a health security card with associated health security ID numbers.<sup>293</sup> This effort ultimately failed in part due to privacy concerns over the government’s ability to protect the security of the data and due to the potential for individuals to be tracked based on their ID numbers.<sup>294</sup> Finally, as mentioned in Chapter II, Congress added language to the Homeland Security Act of 2002 to preventing it from being construed as an authorization for developing a national identification system or card.

In contrast, the United Kingdom has a history of using identity management schemes during wartimes. The concept of a national identity management scheme was first introduced in 1915 at the end of World War I. The *National Registration Act (1915)* established a register of all adults in the United Kingdom between the ages of 15 and 65

---

<sup>290</sup> “Social Security Numbers,” accessed October 27, 2015, <https://epic.org/privacy/ssn/>.

<sup>291</sup> “Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission, Chapter 16: The Social Security Number,” accessed October 28, 2015, <https://epic.org/privacy/ppsc1977report/c16.htm>.

<sup>292</sup> Ibid.

<sup>293</sup> “Clinton’s Failure: Lessons from the National Health Security Plan,” Yale Journal of Medicine and Law: An Undergraduate Publication, accessed October 28, 2015, <http://www.yalemedlaw.com/clinton’s-failure-lessons-from-the-national-health-security-plan/>.

<sup>294</sup> Ibid.; Michael Tackett, “Health Card Potentially A Miracle and A Menace,” *Chicago Tribune*, October 28, 1993, [http://articles.chicagotribune.com/1993-10-28/news/9310280372\\_1\\_smart-cards-health-security-card-medical-records](http://articles.chicagotribune.com/1993-10-28/news/9310280372_1_smart-cards-health-security-card-medical-records).

to organize the workforce and enforce military conscription.<sup>295</sup> Each citizen was given a certificate of registration. A 1918 Amendment to the law required that citizens provide certificates to police officers or authorized persons when asked.<sup>296</sup>

The next wartime scheme was developed in the 1930s at the onset of World War II. The United Kingdom passed the National Registration Act (1939), which required all civilians to carry identification cards with them at all times and produce the card when demanded by a police officer.<sup>297</sup> The original purpose of the card was to enforce required national service in the military, increase security, and assist in food rationing, but its purpose was expanded over time.<sup>298</sup> In 1945, it could be used to register to vote in the general election, and by 1952, 39 government agencies were using the ID card.<sup>299</sup>

In 1951, the Act was challenged in court.<sup>300</sup> The plaintiff, Clarence Harry Willcock, argued that the use of power granted in a national emergency—that is the power of the police to require individuals to produce their ID without being accused of a crime—was no longer valid because the monarchy had acknowledged already that the war had ended.<sup>301</sup> While the court ruled against Willcock, one of the dissenting judges noted that the Act was being used for purposes well beyond what was originally intended.<sup>302</sup> The following year, the National Registration Act was repealed.<sup>303</sup>

---

<sup>295</sup> “War and National Registration,” accessed June 3, 2015, <http://www.gla.ac.uk/schools/social-political/research/economicsocialhistory/historymedicine/scottishwayofbirthanddeath/warandnationalregistration/>; Ward, *The Identity Cards Bill (Bill 9 of 2005-06) House of Commons Research Paper 05/43*, 7.

<sup>296</sup> Ibid.

<sup>297</sup> Ibid.

<sup>298</sup> Ibid.

<sup>299</sup> Ibid.

<sup>300</sup> Ryan Dille, “When the British Fought Off ID Cards,” *BBC News*, last updated September 23, 2003, [http://news.bbc.co.uk/2/hi/uk\\_news/magazine/3129302.stm](http://news.bbc.co.uk/2/hi/uk_news/magazine/3129302.stm).

<sup>301</sup> Ward, *The Identity Cards Bill (Bill 9 of 2005-06) House of Commons Research Paper 05/43*, 7.

<sup>302</sup> “Extract: A Speeding Liberal Knocks Down ID Cards,” accessed October 28, 2015, <http://samathieson.com/card-declined/extracts-and-articles/extract-a-speeding-liberal-knocks-down-id-cards-clarence-willcock/>.

<sup>303</sup> Ibid.

The late 1980s and early 1990s saw identity card proposals far different from those devised while Britain was at war. The Football Supporters Act of 1989, designed to reduce violence at soccer matches in England and Wales, proposed a national membership system involving the creation of a centralized database (called a “central register”) and identity cards issued to spectators.<sup>304</sup> ID cards were never issued, however, as the scheme was never implemented.<sup>305</sup> Six years later, in 1995, the Home Office published a consultation document discussing options for issuing identity cards to the public.<sup>306</sup> The Home Affairs Committee conducted an inquiry, after which it determined that making cards voluntary was the best course of action.<sup>307</sup> No bill was ever introduced however, as there was little focus on the issue politically.<sup>308</sup>

---

<sup>304</sup> Ward, *The Identity Cards Bill (Bill 9 of 2005-06) House of Commons Research Paper 05/43*, 7; *Football Spectators Act 1989, Chapter 37, Section 5, Sub-section 2*, <http://www.legislation.gov.uk/ukpga/1989/37>.

<sup>305</sup> *Ibid.*

<sup>306</sup> *Ibid.*, 7-8.

<sup>307</sup> *Ibid.*, 8.

<sup>308</sup> *Ibid.*

## VI. CONCLUSION

Not all academics, and certainly, not all politicians and government officials deciding and developing identity management policies, understand the nuances that exist in the definitions surrounding identity management. While the terms “identity cards” and “identity management systems” have been favored in the literature, these terms have complex definitions and assumptions associated with them. The variation in terminology obscures the fact that identity cards that are national in scope face the same problems and issues as those experienced by national identity management systems. Using a comparative analysis of the REAL ID Act implementation and the NIS, this thesis has shown that Anglophone, common-law nations experience the same inhibiting factors, whether or not they attempt to implement a national identity management system (like the United Kingdom) or an identity card on a national scale (like the United States). The two different schemes—one purposefully intended *not* to be national identity management system and the other purposefully intended to be one—ultimately must overcome similar issues and establish the same balance between security and privacy.

The previous chapters have established that there are a wide variety of interpretations as to what the REAL ID Act in the United States means when it comes to the identification of individuals on a national scale. A number of opinions about whether the REAL ID-compliant driver’s licenses and identity cards constitute a national ID card or could be considered to be part of a national identity management system have been voiced. Despite these definitional issues, a comparison of the U.K. and U.S. schemes yields a variety of similar inhibiting factors, the most prominent of which are privacy and civil liberties related.

Advocacy groups, academics, and even politicians have objected to parts of both schemes based on similar purpose, privacy, and civil rights and civil liberties concerns. They warned that the schemes might not be able to fulfill their proposed purposes. They expressed concern over a variety of privacy issues, including the potential for function creep, the security and integrity of data collected for the schemes, the implications of linking databases together, and the effects of increased collection and sharing of data.

Advocacy groups and academics also expressed concern over the potential for increased civil rights and civil liberties violations based on the data collected. They worried that the schemes could plausibly increase racial profiling and discrimination, through stops and searches or through the possible inclusion of race on the identity cards in the United States, where the cards' lack of encryption creates the risk that personal data would be collected and used by commercial entities. Furthermore, the concern that the nationwide use of identity cards fosters a surveillance society, and facilitates the practices of data mining and profiling, is shared by U.S. and U.K. groups.

Academics in the United States and United Kingdom asserted similar concerns regarding the development of their respective legislation. They believed that the process was either too accelerated to allow for public debate, or that it was flawed, as the design and functional components of the scheme had been decided up front. Both schemes have similarly high levels of public acceptance, until it is brought to the attention of the participants how the schemes will actually function. Finally, the United States and United Kingdom have similar inclinations to reject identity management schemes, identity cards, or identifiers based on a varied history of associated personal privacy and civil liberties concerns.

When considering identifiers, it is perplexing to compare the fervor over the REAL ID Act to the resistance against the use of SSNs. If all U.S. citizens have SSNs, but not all citizens have driver's licenses, why then has more outrage occurred over REAL ID-compliant driver's licenses and identity cards than SSNs? If everyone actually has social security cards, why are they less contested than the driver's licenses? It is because numerous steps have been taken to prevent the social security cards from being an identifying document, while acting as an identifying document is precisely the purpose of the driver's license and ID cards as required by the REAL ID Act. The function of the document is what drives the opposition. National identity management systems and identity cards have the same function.

The parallel inhibiting factors experienced by both schemes demonstrate that while some do not consider the U.S. REAL ID Act to be a national identity management system—and thus, may not think of REAL ID-compliant driver's licenses and identity

cards as national ID cards—the nomenclature used to describe the policy does not matter when it comes to issues surrounding identity management that must be negotiated and overcome. Whatever the name, whatever the architecture, government systems built to identify the citizenry of a national will face significant resistance. U.S. policymakers must consider the inhibiting factors that face national identity management schemes in Anglophone, common-law nations when implementing nationwide identity cards, lest they fall into the trap of believing that the same issues will not appear. Only with this foresight in mind, will the United States be able to formulate and sustain lasting identity management policy.

THIS PAGE INTENTIONALLY LEFT BLANK

# APPENDIX A. DATA ELEMENTS IN THE IDENTITY CARDS ACT 2006

Appendix A contains the list of data elements intended to be recorded in the National Identity Register, as required by the Identity Cards Act of 2006.

*Identity Cards Act 2006 (c. 15)* 1  
*SCHEDULE 1 – Information that may be recorded in Register*  
*Document Generated: 2015-11-17*  

---

*Status: This is the original version (as it was originally enacted).*

---

## SCHEDULES

### SCHEDULE 1

Section 3

#### INFORMATION THAT MAY BE RECORDED IN REGISTER

##### *Personal information*

- 1 The following may be recorded in an individual's entry in the Register—
- (a) his full name;
  - (b) other names by which he is or has been known;
  - (c) his date of birth;
  - (d) his place of birth;
  - (e) his gender;
  - (f) the address of his principal place of residence in the United Kingdom;
  - (g) the address of every other place in the United Kingdom or elsewhere where he has a place of residence.

##### *Identifying information*

- 2 The following may be recorded in an individual's entry in the Register—
- (a) a photograph of his head and shoulders (showing the features of the face);
  - (b) his signature;
  - (c) his fingerprints;
  - (d) other biometric information about him.

##### *Residential status*

- 3 The following may be recorded in an individual's entry in the Register—
- (a) his nationality;
  - (b) his entitlement to remain in the United Kingdom;
  - (c) where that entitlement derives from a grant of leave to enter or remain in the United Kingdom, the terms and conditions of that leave.

##### *Personal reference numbers etc.*

- 4 (1) The following may be recorded in an individual's entry in the Register—
- (a) his National Identity Registration Number;
  - (b) the number of any ID card issued to him;
  - (c) any national insurance number allocated to him;
  - (d) the number of any immigration document relating to him;
  - (e) the number of any United Kingdom passport (within the meaning of the Immigration Act 1971 (c. 77)) that has been issued to him;

---

*Status: This is the original version (as it was originally enacted).*

---

- (f) the number of any passport issued to him by or on behalf of the authorities of a country or territory outside the United Kingdom or by or on behalf of an international organisation;
  - (g) the number of any document that can be used by him (in some or all circumstances) instead of a passport;
  - (h) the number of any identity card issued to him by the authorities of a country or territory outside the United Kingdom;
  - (i) any reference number allocated to him by the Secretary of State in connection with an application made by him for permission to enter or to remain in the United Kingdom;
  - (j) the number of any work permit (within the meaning of the Immigration Act 1971) relating to him;
  - (k) any driver number given to him by a driving licence;
  - (l) the number of any designated document which is held by him and is a document the number of which does not fall within any of the preceding sub-paragraphs;
  - (m) the date of expiry or period of validity of a document the number of which is recorded by virtue of this paragraph.
- (2) In this paragraph “immigration document” means—
- (a) a document used for confirming the right of a person under the Community Treaties in respect of entry or residence in the United Kingdom;
  - (b) a document which is given in exercise of immigration functions and records information about leave granted to a person to enter or to remain in the United Kingdom; or
  - (c) a registration card (within the meaning of section 26A of the Immigration Act 1971);
- and in paragraph (b) “immigration functions” means functions under the Immigration Acts (within the meaning of the Asylum and Immigration (Treatment of Claimants, etc.) Act 2004 (c. 19)).
- (3) In this paragraph “driving licence” means—
- (a) a licence to drive a motor vehicle granted under Part 3 of the Road Traffic Act 1988 (c. 52); or
  - (b) a licence to drive a motor vehicle granted under Part 2 of the Road Traffic (Northern Ireland) Order 1981 (S.I.1981/154 (N.I. 1)).

*Record history*

- 5 The following may be recorded in an individual’s entry in the Register—
- (a) information falling within the preceding paragraphs that has previously been recorded about him in the Register;
  - (b) particulars of changes affecting that information and of changes made to his entry in the Register;
  - (c) his date of death.

*Registration and ID card history*

- 6 The following may be recorded in an individual’s entry in the Register—
- (a) the date of every application for registration made by him;

- (b) the date of every application by him for a modification of the contents of his entry;
- (c) the date of every application by him confirming the contents of his entry (with or without changes);
- (d) the reason for any omission from the information recorded in his entry;
- (e) particulars (in addition to its number) of every ID card issued to him;
- (f) whether each such card is in force and, if not, why not;
- (g) particulars of every person who has countersigned an application by him for an ID card or a designated document, so far as those particulars were included on the application;
- (h) particulars of every notification given by him for the purposes of regulations under section 11(1) (lost, stolen and damaged ID cards etc.);
- (i) particulars of every requirement by the Secretary of State for the individual to surrender an ID card issued to him.

*Validation information*

- 7 The following may be recorded in the entry in the Register for an individual—
- (a) the information provided in connection with every application by him to be entered in the Register, for a modification of the contents of his entry or for the issue of an ID card;
  - (b) the information provided in connection with every application by him confirming his entry in the Register (with or without changes);
  - (c) particulars of the steps taken, in connection with an application mentioned in paragraph (a) or (b) or otherwise, for identifying the applicant or for verifying the information provided in connection with the application;
  - (d) particulars of any other steps taken or information obtained (otherwise than in connection with an application mentioned in paragraph (a) or (b)) for ensuring that there is a complete, up-to-date and accurate entry about that individual in the Register;
  - (e) particulars of every notification given by that individual for the purposes of section 10.

*Security information*

- 8 The following may be recorded in the entry in the Register for an individual—
- (a) a personal identification number to be used for facilitating the making of applications for information recorded in his entry, and for facilitating the provision of the information;
  - (b) a password or other code to be used for that purpose or particulars of a method of generating such a password or code;
  - (c) questions and answers to be used for identifying a person seeking to make such an application or to apply for or to make a modification of that entry.

*Records of provision of information*

- 9 The following may be recorded in the entry in the Register for an individual—
- (a) particulars of every occasion on which information contained in the individual's entry has been provided to a person;

---

*Status: This is the original version (as it was originally enacted).*

---

- (b) particulars of every person to whom such information has been provided on such an occasion;
- (c) other particulars, in relation to each such occasion, of the provision of the information.

**APPENDIX B. DATA ELEMENTS IN THE AAMVA DRIVER'S  
LICENSE/IDENTIFICATION CARD DESIGN SPECIFICATIONS,  
ANNEX D**

Appendix B contains the list of mandatory and optional data elements found in the 2005 American Association of Motor Vehicle Administrators (AAMVA) Driver's License/Identification Card Design Specifications, Annex D. Mandatory data elements were proposed by DHS for inclusion on REAL ID compliant driver's licenses and identity cards in the notice of proposed rulemaking, Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 72 FR 10820.

## APPENDIX B

**From: Personal Identification — AAMVA International Specification — DL/ID Card Design, Annex D: “Mandatory PDF417 Bar Code”**

### MINIMUM MANDATORY DATA ELEMENTS

**Jurisdiction-Specific Vehicle Class**

Jurisdiction-specific vehicle class / group code, designating the type of vehicle the cardholder has privilege to drive.

**Jurisdiction-Specific Restriction Codes**

Jurisdiction-specific codes that represent restrictions to driving privileges (such as airbrakes, automatic transmission, daylight only, etc.).

**Jurisdiction-Specific Endorsement Codes**

Jurisdiction-specific codes that represent additional privileges granted to the cardholder beyond the vehicle class (such as transportation of passengers, hazardous materials, operation of motorcycles, etc.).

**Document Expiration Date** Date on which the driving and identification privileges granted by the document are no longer valid.  
(MMDDCCYY for U.S., CCYYMMDD for Canada)

**Customer Family Name** Family name of the cardholder. (Family name is sometimes also called “last name” or “surname.”) Collect full name for record, print as many characters as possible on front of DL/ID.

**Customer Given Names** Given names of the cardholder. (Given names include all names other than the Family Name. This includes all those names sometimes also called “first” and “middle” names.) Collect full name for record, print as many characters as possible on front of DL/ID.

**Document Issue Date** Date on which the document was first issued.  
(MMDDCCYY for U.S., CCYYMMDD for Canada)

**Date of Birth** Date on which the cardholder was born. (MMDDCCYY for U.S., CCYYMMDD for Canada)

**Physical Description – Sex** Gender of the cardholder. 1 = male, 2 =female.

**Physical Description – Eye Color**  
Color of cardholder's eyes. (ANSI D-20 codes)

**Physical Description – Height**  
Height of cardholder. Inches (in): number of inches followed by " in" ex. 6'1" = " 73 in" Centimeters (cm): number of centimeters followed by " cm" ex. 181 centimeters="181 cm"

**Address – Street 1** Street portion of the cardholder address.

**Address – City** City portion of the cardholder address.

**Address – Jurisdiction Code**  
State portion of the cardholder address.

**Address – Postal Code** Postal code portion of the cardholder address in the U.S. and Canada. If the trailing portion of the postal code in the U.S. is not known, zeros will be used to fill the trailing set of numbers.

**Customer ID Number** The number assigned or calculated by the issuing authority.

**Document Discriminator** Number must uniquely identify a particular document issued to that customer from others that may have been issued in the past. This number may serve multiple purposes of document discrimination, audit information number, and/or inventory control.

**Country Identification** Country in which DL/ID is issued. U.S. = USA, Canada = CAN.

**Federal Commercial Vehicle Codes**  
Federally established codes for vehicle categories, endorsements, and restrictions that are generally applicable to commercial motor vehicles. If the vehicle is not a commercial vehicle, "NONE" is to be entered.

#### **OPTIONAL DATA ELEMENTS**

**Address – Street 2** Second line of street portion of the cardholder address.

<b>Hair color</b>	Brown, black, blonde, gray, red/auburn, sandy, white
<b>Place of birth</b>	Country and municipality and/or state/province
<b>Audit information</b>	A string of letters and/or numbers that identifies when, where, and by whom a driver license/ID card was made. If audit information is not used on the card or the MRT, it must be included in the driver record.
<b>Inventory control number</b>	A string of letters and/or numbers that is affixed to the raw materials (card stock, laminate, etc.) used in producing driver licenses and ID cards.
<b>Alias / AKA Family Name</b>	Other family name by which cardholder is known.
<b>Alias / AKA Given Name</b>	Other given name by which cardholder is known
<b>Alias / AKA Suffix Name</b>	Other suffix by which cardholder is known
<b>Name Suffix</b>	Name Suffix (If jurisdiction participates in systems requiring name suffix (PDPS, CDLIS, etc.), the suffix must be collected and displayed on the DL/ID and in the MRT). Collect full name for record, print as many characters as possible on front of DL/ID.
<b>Physical Description – Weight Range</b>	Indicates the approximate weight range of the cardholder: 0 = up to 31 kg (up to 70 lbs) 1 = 32 – 45 kg (71 – 100 lbs) 2 = 46 - 59 kg (101 – 130 lbs) 3 = 60 - 70 kg (131 – 160 lbs) 4 = 71 - 86 kg (161 – 190 lbs) 5 = 87 - 100 kg (191 – 220 lbs) 6 = 101 - 113 kg (221 – 250 lbs) 7 = 114 - 127 kg (251 – 280 lbs) 8 = 128 – 145 kg (281 – 320 lbs) 9 = 146+ kg (321+ lbs)
<b>Race / ethnicity</b>	Codes for race or ethnicity of the cardholder, as defined in ANSI D20.
<b>Standard vehicle classification</b>	

Standard vehicle classification code(s) for cardholder. This data element is a placeholder for future efforts to standardize vehicle classifications.

**Standard endorsement code**

Standard endorsement code(s) for cardholder. This data element is a placeholder for future efforts to standardize endorsement codes.

**Standard restriction code**

Standard restriction code(s) for cardholder. This data element is a placeholder for future efforts to standardize restriction codes.

**Jurisdiction specific vehicle classification description**

Text that explains the jurisdiction-specific code(s) for types of vehicles cardholder is authorized to drive.

**Jurisdiction specific endorsement code description**

Text that explains the jurisdiction-specific code(s) that indicates additional driving privileges granted to the cardholder beyond the vehicle class.

**Jurisdiction specific restriction code description**

Text describing the jurisdiction-specific restriction code(s) that curtail driving privileges.

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF REFERENCES

- American Association of Motor Vehicle Administrators (AAMVA). "Problem Driver Pointer System (PDPS)." Accessed September 22, 2015. <http://www.aamva.org/PDPS/>.
- American Civil Liberties Union. "5 Problems with National ID Cards." Accessed October 19, 2015. <https://www.aclu.org/5-problems-national-id-cards>.
- Bali, Valentina. "Tinkering Toward a National Identification System: An Experiment on Policy Attitudes." *Policy Studies Journal* 37, no. 2 (May 2009): 233–255.
- BBC News. "Identity Cards Scheme Will Be Axed 'within 100 Days.'" Last updated May 27, 2010. <http://news.bbc.co.uk/2/hi/8707355.stm>.
- Beck, Adrian, and Kate Broadhurst. "National Identity Cards: The Impact on the Relationship between the Police and Ethnic Minority Groups." *Policing and Society* 8, no. 4 (1998): 401–424.
- Beynon-Davies, Paul. "Personal Identity Management and Electronic Government: The Case of the National Identity Card in the UK." *Journal of Enterprise Information Management* 20, no. 3 (2007): 244–270.
- . "The UK National Identity Card." *Journal of Information Technology Teaching Cases* 1, no. 1 (March 2011): 12–21.
- Cabinet Office. *Privacy and Data-Sharing: The Way Forward for Public Services*. London: Cabinet Office, 2002.
- Cameron. "USACM Questions Real ID Act's Security Standards." Association for Computer Machinery U.S. Public Policy Council (USACM). April 5, 2005. <http://techpolicy.acm.org/blog/?p=240>.
- Clarke, Richard. "Human Identification in Information Systems: Management Challenges and Public Policy Issues." *Information Technology & People* 4, no. 7 (December 1994): 6–37. <http://www.rogerclarke.com/DV/HumanID.html>.
- Clement, Andrew, Robert Guerra, Jeff Johnson, and Felix Stalder. "National Identification Schemes (NIDS)." In *Human Choice and Computers: Issues of Choice and Quality of Life in the Information Society*, edited by Klaus Brunnstein and Jacques Berleur. Vol. 98, 195–205. Boston, MA: Springer US, 2002.
- Computer Weekly. "Child Support Agency: A History of IT Failure." July 24, 2006. <http://www.computerweekly.com/news/2240062052/Child-Support-Agency-a-history-of-IT-failure>.

- Congressional Research Service. “All Bill Information (Except Text) for H.R.1268—Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005.” Accessed June 23, 2015. <https://www.congress.gov/bill/109th-congress/house-bill/1268/all-info>.
- Cotton, James. “Data: The Importance of Accuracy, Integrity and Real-Time Integration.” Information Builders. December 15, 2014. <http://www.informationbuilders.com/blog/james-cotton/19152>.
- Crossman, Gareth. “Nothing to Hide, Nothing to Fear?” *International Review of Law, Computers & Technology* 22, no. 1–2 (2008): 115–118.
- Department of Homeland Security. *Privacy Impact Assessment for the REAL ID Act In Conjunction with the Notice of Proposed Rulemaking, Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*. Washington, DC: Department of Homeland Security, 2007. [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_pia\\_realid.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_realid.pdf).
- . “REAL ID Enforcement in Brief.” Accessed October 25, 2015. <http://www.dhs.gov/real-id-enforcement-brief>. <http://www.dhs.gov/real-id-public-faqs>.
- . “REAL ID Frequently Asked Questions for the Public.” Accessed June 11, 2015. <http://www.dhs.gov/real-id-public-faqs>.
- Dilley, Ryan. “When the British Fought Off ID Cards.” *BBC News*. Last updated September 23, 2003. [http://news.bbc.co.uk/2/hi/uk\\_news/magazine/3129302.stm](http://news.bbc.co.uk/2/hi/uk_news/magazine/3129302.stm).
- Electronic Privacy Information Center (EPIC). *REAL ID Implementation Review: Few Benefits, Staggering Costs*. Washington, DC: Electronic Privacy Information Center, 2008.
- . “Social Security Numbers.” Accessed October 27, 2015. <https://epic.org/privacy/ssn/>.
- Electronic Privacy Information Center (EPIC) and Melissa Ngo. *Comments Re: DOCKET NO. DHS 2006–0030 Notice of Proposed Rulemaking: Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*. Washington, DC: Department of Homeland Security, 2007. <http://www.regulations.gov/#!documentDetail;D=DHS-2006-0030-7239>.
- Eyre, William. “Chapter 4: Technology of the Real ID Act.” In *The Real ID Act: Privacy and Government Surveillance*, 105–126. El Paso, TX: LFB Scholarly Publishing LLC, 2011.
- FindLaw. “Civil Rights Vs. Civil Liberties.” Accessed November 5, 2015. <http://civilrights.findlaw.com/civil-rights-overview/civil-rights-vs-civil-liberties.html>.

- Foundation for Information Policy Research. "ID Card Scheme an Expensive Flop." Accessed October 4, 2015. <http://www.fipr.org/press/040426id.html>.
- Government Technology. "Survey Shows Public Support for Goals Similar to Real ID." Accessed October 25, 2015. <http://www.govtech.com/security/Survey-Shows-Public-Support-for-Goals.html>.
- Halperin, Ruth, and James Backhouse. "A Roadmap for Research on Identity in the Information Society." *Identity in the Information Society* 1, no. 1 (2008): 71–87.
- Harper, Jim. *REAL ID: A State-by-State Update*. Washington, DC: CATO Institute, 2014. [http://object.cato.org/sites/cato.org/files/pubs/pdf/pa749\\_web\\_1.pdf](http://object.cato.org/sites/cato.org/files/pubs/pdf/pa749_web_1.pdf).
- . "Testimony regarding SB 262 and the U.S. Federal REAL ID Act: Committee on Transportation New Hampshire State Senate." CATO Institute. Accessed June 23, 2015. <http://www.cato.org/publications/testimony/testimony-regarding-sb-262-us-federal-real-id-act>.
- "House-Passed 'Real ID Act' Folded into Supplemental Spending Bill," in *CQ Almanac 2005*, 61st ed., 13–3-13-4, Washington, DC: Congressional Quarterly, 2006, <http://library.cqpress.com/cqalmanac/cqal05-766-20098-1042121>.
- Home Office Identity & Passport Service. *Introducing the National Identity Scheme: How the Scheme Will Work and How it Will Benefit You*. London: Home Office Identity & Passport Service, 2008.
- Home Office. *Entitlement Cards and Identity Fraud: A Consultation Paper*. Norwich, England: The Stationary Office, 2002.
- . "Identity Cards: The Next Steps, Cm 6020." November 2003. <http://www.statewatch.org/news/2003/nov/id.pdf>.
- . *Identity Cards Bill Regulatory Impact Assessment*. London: Home Office, 2004.
- . *Identity Cards: A Summary of Findings from the Consultation on Legislation on Identity Cards*. Norwich: The Stationery Office, 2004.
- . *Legislation on Identity Cards: A Consultation*. UK: The Stationery Office Limited, 2004.
- Hornung, Bernd. "Information System." Principia Cybernetica Web. Accessed August 15, 2015. [http://pespmc1.vub.ac.be/ASC/INFORM\\_SYSTE.html](http://pespmc1.vub.ac.be/ASC/INFORM_SYSTE.html).
- House of Commons, Home Affairs Committee. *A Surveillance Society? Fifth Report of Session 2007–08 Volume 1*. London: House of Commons Library, 2008.

- . *Identity Cards: Fourth Report of Session 2003–04, Volume I*. London: The Stationery Office Limited, 2004.
- . “Select Committee on Home Affairs Written Evidence Session 2003–04, Memorandum submitted by the Association of Chief Police Officers.” April 2004. <http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/130we02.htm>.
- Institute of Electrical and Electronics Engineers, The. *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*. IEEE Std 610. New York: The Institute of Electrical and Electronics Engineers, 1991.
- Ipsos MORI. “British ‘Favour ID Cards.’” Accessed October 24, 2015. <https://www.ipsos-mori.com/researchpublications/researcharchive/622/British-Favour-ID-Cards.aspx>.
- Joinson, Adam N. “Privacy Concerns, Trust in Government and Attitudes to Identity Cards in the United Kingdom.” In *42nd Hawaii International Conference on System Sciences, 2009. HICSS '09.*, edited by Sprague, Ralph H., 1–10. Piscataway, NJ: IEEE, 2009.
- Joinson, Adam N., Carina Paine, Tom Buchanan, and Ulf-Dietrich Reips. “Watching Me, Watching You: Privacy Attitudes and Reactions to Identity Card Implementation Scenarios in the United Kingdom.” *Journal of Information Science* 32, no. 4 (August 1, 2006): 334–343.
- Kent, Stephen T., and Millett, Lynette I. *IDs—Not that Easy: Questions about Nationwide Identity Systems*. Washington, DC: National Academy Press, 2002.
- Kephart, Janice. *Repealing REAL ID? Rolling Back Driver’s License Security*. Washington, DC: Center for Immigration Studies, 2009.
- Kubicek, Herbert, and Torsten Noack. “Different Countries-Different Paths Extended Comparison of the Introduction of eIDs in Eight European Countries.” *Identity in the Information Society* 3, no. 1 (2010): 235–245.
- Liberty. “The Case Against ID Cards.” Accessed September 16, 2015. <https://www.liberty-human-rights.org.uk/human-rights/privacy/id-cards/case-against-id-cards>.
- Lips, Miriam. “The Quest for Managing Identity Management.” *Online Information Review* 33, no. 3 (2009).
- Lyon, David. “National ID Cards: Crime-Control, Citizenship and Social Sorting.” *Policing: A Journal of Policy and Practice* 1, no. 1 (January 1, 2007): 111–118.

- Marit Hansen, Peter Berlich, Jan Camenisch, Sebastian Clauß, Andreas Pfitzmann, and Michael Waidner, "Privacy-Enhancing Identity Management." *Information Security Technical Report* 9, no. 1 (2004): 35–44.
- Martin, Aaron K. "National Identity Infrastructures: Lessons from the United Kingdom." In *ICT Critical Infrastructures and Society*, edited by Magda David Hercheui, Diane Whitehouse, William Jr. McIver, and Jackie Phahlamohlaka. Vol. 386. 44–55. Berlin: Springer, 2012.
- Mathieson, S. A. "Extract: A Speeding Liberal Knocks Down ID Cards." Accessed October 28, 2015. <http://samathieson.com/card-declined/extracts-and-articles/extract-a-speeding-liberal-knocks-down-id-cards-clarence-willcock/>.
- Milberg, Debra. "National Security Surveillance and National Authentication System: The National Identification Debate: "REAL ID "and Voter Identification." *I/S: A Journal of Law & Policy for the Information Society* 3, no. 3 (Winter 2007): 443–472.
- National Association of Teachers of Travellers + Other Professionals. "Gypsy, Roma and Traveller Communities." Accessed October 13, 2015. <http://www.natt.org.uk/gypsy-roma-and-traveller-communities>.
- National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. Washington, DC: National Commission on Terrorist Attacks upon the United States, 2004.
- National Science & Technology Council's (NSTC) Subcommittee on Biometrics and Identity Management. "Biometrics Glossary." National Science & Technology Council's (NSTC). Accessed January 12, 2015. <http://www.biometrics.gov/Documents/Glossary.pdf>.
- Pew Research Center. "Free Trade Agreements Get a Mixed Review." Accessed December 26, 2015. <http://www.people-press.org/2006/12/19/free-trade-agreements-get-a-mixed-review/>.
- Politics.co.uk. "Civil Liberties." Accessed November 5, 2015. <http://www.politics.co.uk/reference/civil-liberties>.
- Posner, Richard A. *Not a Suicide Pact: The Constitution in a Time of National Emergency*. New York; Oxford: Oxford University Press, 2006.
- Privacy International. "Mistaken Identity; Exploring the Relationship between National Identity Cards & the Prevention of Terrorism." April 2004. <http://www.privacyinternational.org/issues/idcard/uk/id-terrorism.pdf>.

- . “Privacy International’s FAQ on the UK Government’s Proposed National Identity Card.” Accessed October 28, 2015. <https://web.archive.org/web/20120207124540/https://www.privacyinternational.org/issues/idcard/uk/uk-idcard-faq.html>.
- Ridge, Tom. “Transcript of Secretary of Homeland Security Tom Ridge at the Center for Transatlantic Relations at Johns Hopkins University ‘Transatlantic Homeland Security Conference.’” Department of Homeland Security. Accessed August 10, 2015. <https://www.hsdl.org/?view&did=475404>.
- Schneier, Bruce. “Security and Function Creep.” *IEEE Security & Privacy* 8, no. 1 (January/February 2010): 88.
- Solove, Daniel J. *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven, CT: Yale University Press, 2011.
- Steinbock, Daniel J. “Fourth Amendment Limits on National Identity Cards.” In *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*, edited by Strandburg, Katherine J. and Daniela Stan Raicu, 295–312. New York: Springer US, 2006.
- Stringfellow, Angela. “What is Data Integrity? Data Protection 101.” Digital Guardian. Accessed October 5, 2015. <https://digitalguardian.com/blog/what-data-integrity-data-protection-101>.
- Surveillance Studies Network, The. *A Report on the Surveillance Society: Summary Report for the Information Commissioner*, 2006.
- Tackett, Michael. “Health Card Potentially A Miracle and A Menace.” *Chicago Tribune*, October 28, 1993. [http://articles.chicagotribune.com/1993-10-28/news/9310280372\\_1\\_smart-cards-health-security-card-medical-records](http://articles.chicagotribune.com/1993-10-28/news/9310280372_1_smart-cards-health-security-card-medical-records).
- U.S. Privacy Protection Study Commission. “Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission, Chapter 16: The Social Security Number.” Accessed October 28, 2015. <https://epic.org/privacy/ppsc1977report/c16.htm>.
- U.S. Senate Committee on Homeland Security and Governmental Affairs. “Twelve Senators Urge Frist to Keep REAL ID Act Off Supplemental Appropriations Bill.” April 12, 2005. <https://www.hsgac.senate.gov/media/majority-media/twelve-senators-urge-frist-to-keep-real-id-act-off-supplemental-appropriations-bill>.
- United States Department of Justice. “Overview of the Privacy Act of 1974: Social Security Number Usage.” Accessed October 27, 2015. <http://www.justice.gov/opcl/social-security-number-usage>.

- University of Glasgow. "War and National Registration." Accessed June 3, 2015. <http://www.gla.ac.uk/schools/socialpolitical/research/economicsocialhistory/historymedicine/scottishwayofbirthanddeath/warandnationalregistration/>.
- Ward, Phillip. *The Identity Cards Bill (Bill 9 of 2005–06) House of Commons Research Paper 05/43*. London: House of Commons Library, 2005.
- White House, The. *National Strategy for Homeland Security*. Washington, DC: Office of Homeland Security, 2002.
- Whitley, Edgar A. *The Identity Project: An Assessment of the UK Identity Cards Bill and its Implications*. London, UK: Department of Information Systems, London School of Economics and Political Science, 2005.
- Whitley, Edgar A., Ian R. Hosein, Ian O. Angell, and Simon Davies. "Reflections on the Academic Policy Analysis Process and the UK Identity Cards Scheme." *Information Society* 23, no. 1 (January 2007): 51–58.
- Ya Ni, Anna, and Alfred Tat-Kei Ho. "A Quiet Revolution or a Flashy Blip? The Real ID Act and U.S. National Identification System Reform." *Public Administration Review* 68, no. 6 (2008): 1063–1078.
- Yale Journal of Medicine and Law: An Undergraduate Publication. "Clinton's Failure: Lessons from the National Health Security Plan." Accessed October 28, 2015. <http://www.yalemedlaw.com/clinton's-failure-lessons-from-the-national-health-security-plan/>.
- Zetter, Kim. "National ID Battle Continues." *Wired*. Accessed October 25, 2015. <http://archive.wired.com/politics/security/news/2005/05/67498?currentPage=all>.

THIS PAGE INTENTIONALLY LEFT BLANK

## **INITIAL DISTRIBUTION LIST**

1. Defense Technical Information Center  
Ft. Belvoir, Virginia
2. Dudley Knox Library  
Naval Postgraduate School  
Monterey, California