Implementation of a Facial Recognition Technology System in the Alaska Division of Motor Vehicles

Carol Beecher

University of Alaska Anchorage
PADM 659
Public Administration Capstone
Spring 2010
Table of Contents

I. Background 3

II. Driver’s License History 4

III. Literature Review 10

IV. Methodology 13

V. Findings 17

VI. Policy Considerations 20

VII. Policy Recommendations 22

VIII. Conclusion 23

References 25

Charts

Chart 1. Licensed Drivers by Year 17

Chart 2. States with Facial Recognition Systems 19

Figures

Figure 1. Policy Analysis Framework 14
Implementation of a Facial Recognition Technology System in the Alaska Division of Motor Vehicles.

I. Background:

A driver’s license has become the ubiquitous form of identification for most Americans. Its use has far exceeded its original purpose as license to operate a vehicle on public roads and now functions as a license for entry, to purchase items, to gain government benefits as well as proving identity. Because of its widespread use as a de facto form of national identification, it has also become a valuable commodity on the black market. Sophisticated methods have been developed for producing fraudulent licenses as well as the proof of identity documents or ‘breeder documents’ that are required. Copiers and printers and software allow easy and accurate forgeries to be printed that are difficult to differentiate from originals. The Internet offers tutorials for aspiring forgers and evolving technologies have made the entire process accessible to the public.

To combat the fraudulent documents, motor vehicle administrators have begun to move toward adopting safeguards and minimum standards and procedures, including the use of biometric data, to ensure document authenticity and deter and detect fraud. Alaska has taken measures similar to other states in implementing procedures to reduce issuance of fraudulent licenses. In a 2004 study Alaska was one of four states that received a grade of ‘F’ in secure driver’s licensing practices and procedures (Etzioni). Since 2004,
Alaska has implemented procedures that would raise that grade to a ‘B’.

This paper will examine the policy question of whether or not the Alaska Division of Motor Vehicles (DMV) should implement a facial recognition system technology as a security measure to deter and detect fraudulent driver’s licenses. A discussion of the literature on the topic, an examination of the issues involved, an analysis of the data collected and a policy recommendation will be presented.

II. Driver License History:

The first state to require a driver’s license was Rhode Island in 1908 (Harberson, 2002) and the remaining states followed suit with South Dakota finally implementing the requirement in 1954 (2002). The original intent of the driver’s licenses, which were initially part of the automobile registration, was to generate revenue by the cities and counties in the state (Watner, 2004). In some states the multiple registration and licensing requirements meant that a driver could end up with nearly $300 in registration fees merely to be able to drive legally in the various jurisdictions across the state (2004).

A bill introduced in the 60th Congress in 1907 to require federal registration of all vehicles failed due to questions about the Constitutionality of the Federal government’s regulatory role in the states (2004). The states resolved the problem by making vehicle registration a state responsibility and by entering into agreements to accept registrations across state borders (2004). The
United States Supreme Court confirmed the authority of states to levy registration fees and for the administration and regulation of motor vehicles in *Kane v. New Jersey*, 242 U.S. 160 (1916).

**American Association of Motor Vehicles:** In 1933 the non-profit, American Association of Motor Vehicles (AAMVA) was founded to “create a forum for the exchange of information among and establishment of standards for motor vehicle driver licensing and law enforcement administrators.” (Maxwell, 2009 p4). Since its inception, the Association has been a proponent for standardization of driver’s licensing (AAMVA, 2010). AAMVA operates the Commercial Driver’s License Information System, which shares information about commercial drivers, including out-of-state convictions.

The association provides support for the Problem Driver Pointer System, which reports serious traffic offenses, such as drunken driving offenses and withdrawals of driver’s licenses, to the National Highway Traffic Safety Administration. AAMVA also maintains National Motor Vehicle Title Information System which verifies automobile titles across the United States to deter theft and fraud (2010).

**State Compacts:** In an effort to protect the public from drivers with convictions for serious traffic violations, and to prevent them from obtaining a driver’s license in a different state, the states formed the Driver’s License Compact, in 1961 as a formal agreement between participating states to report dangerous driver’s traffic
violations. The Driver’s License Compact has 45 member states who share information in a database administered by the AAMVA.

In 1965, the Traffic Violations Compact was formed to provide information to participating states about driver’s with outstanding traffic citations in different jurisdictions. The Compact was revised and renamed the Non-Resident Violator Compact (NRVC) in 1977. The Compact has 44 participating states. Alaska is a participating member of both compacts (2010).

**Commercial Driver’s Licenses:** The Federal government enacted the Commercial Motor Vehicle Safety Act in 1986. The Act set national standards for commercial driver’s licenses and reporting requirements for the states. The AAMVA maintains the Commercial Driver’s License Information System (CDLIS), a repository for information reported by the states as mandated by the Act. CDLIS contains information about each commercial driver including:

- Name
- Date of birth
- Social Security Number
- State driver license number
- AKA information
- Current “State of Record” (SOR)

The system database maintains the history of each commercial driver’s convictions and license withdrawals. As of March 2009 it held 13.9 million records and it continues to expand.
**Real ID Act of 2005:** The Real ID Act of 2005 was signed into law several years after the terrorist attack on the World Trade Center Twin Towers in New York City on September 11, 2001 (9/11). A commission was formed and a report was prepared and presented to Congress to investigate the weaknesses in the various agencies that may have contributed to or allowed the perpetrators to carry out their attack. One of the 9/11 Commission recommendations to “Protect Against and Prepare for Terrorist Attacks” included:

- Set Standards for the issuance of birth certificates and sources of identification, such as driver’s licenses.

The Real ID Act of 2005 was passed by Congress as a result of this recommendation. The Act sets out requirements for Real ID compliant identification cards that will be required by the federal government for entry into nuclear facilities, federal facilities (including Social Security offices, courts and national parks) and federally controlled airlines.

Many states reacted to the Real ID Act by introducing or passing legislation that prohibited expending funds for implementation of the Real ID requirements. Some states also passed resolutions calling for the repeal of Real ID (Harberson, 2002). The Act was seen as an unfunded mandate and a move toward a national ID system (EPIC, 2002) (Perlman, 2007). The federal Department of Homeland Security initially estimated that Real ID implementation would cost states approximately $14.6 billion (DHS, 2008). The
estimated expense was reduced to $4 billion in 2008, largely as a result of measures taken by states in the interim between passage of the Real ID Act and the promulgation of the regulations to secure their driver’s licensing and identification practices and procedures (2008).

The release of the Real ID regulations in 2008 allayed the concerns of many states. Additionally, compliance deadlines were extended to May 2011 to, “give states more time to consider the issue.” (AFSA, 2009, p2).

Alaska Driver’s License Laws

Alaska was one of the states that responded negatively to the passage of the Real ID Act of 2005. In testimony before the legislature for Senate Bill 202, which prohibits the expenditure of funds, “solely for the purpose of implementing or aiding in the implementation of the federal Real ID Act of 2005, (AS 44.99.040), the Director of the Division of Motor Vehicles stated that the cost to implement Real ID was estimated to be $2 million (SB 202 Minutes, 2008). The bill sponsor stated that Real ID was “The federal government commandeering the DMV and not paying for it. If the government is creating big brother, they need to pay for it.” The bill passed in 2008 along with HJR 19, which called for the repeal of Real ID. A law to require driver’s licenses to expire when a legal alien’s visa expires was introduced and failed in a vote in the House in 2010. The sponsor plans to introduce the bill again in the next session (Eschleman, 2010).
III. Literature Review:

Privacy Issues: Maintaining a balance between individual privacy and the government’s ability to collect information about the citizenry has always been an issue. Our founding fathers, recognizing the tendency and potentially abusive power of government to intrude upon the individual, passed the Bill of Rights to specifically address and protect the citizen against its government. George Orwell in his dystopian classic, “1984” envisioned a future in which the government would watch our every move, using technology to control the minds and actions of the people (1961). The notion of advanced technologies that would make such a world possible was inconceivable to the readers of his book for many decades. However, advances in technology in the last twenty years have made Orwell’s vision a potential reality.

In this post 9/11 world, being observed has become commonplace (Desmond, 2002). Cameras are now used to observe public places across the country and people scarcely notice (Avexander, 2007). Cities have installed cameras at intersections, campuses and parks and the images they produce have become increasingly detailed as technology has continued to improve (2007).

Reality shows are a television staple, with people recording every moment of their lives, or in some cases, acting it out in real time before an audience of thousands. Cell phones are equipped with digital cameras and video recorders that allow the user to quickly record and send the
information to number of individuals or sites. Photographs and video images are posted on social networking sites, providing public access to family reunions and private celebrations.

The lines between what is considered public and private are continuing to blur. Current technology allows users to collect and identify faces in photographs that have been posted on the web using facial recognition technology (McClurg, 2007). In a Harvard Law Review article titled, “In the Face of Danger: Facial Recognition and the Limits of Privacy Law” the author states that, “the sales of digital cameras have exploded in recent years, with new camera phones alone generating an additional twenty-nine billion images in 2004.” (McClurg, 2007, p1870). Software programs are now able to sort images and the ever expanding collection is easily accessible (2007).

Privacy advocates have raised concerns that the current laws are not adequate to address the resulting privacy protection issues (2007). The sheer volume and accessibility of images was never contemplated by the laws that are in place to protect individual privacy. The 1967 landmark ruling in Katz v. U.S. 389 U.S. 347, refined the Fourth Amendment’s protection of the individual against unreasonable search and seizure to include protection against electronic search if there was an ‘expectation’ of privacy, and the expectation was ‘reasonable’. In Katz, the issue was whether or not a phone call using a public phone (the individual was engaged in illegal gambling) was a
protected activity. Justice Harlan, in his concurring opinion stated that, “an enclosed telephone booth is an area where, like a home, and unlike a field, a person has a constitutionally protected reasonable expectation of privacy.” (Katz) (Woodward, 2003).

Courts have followed the Katz ruling since it was released. Thus, the privacy protections of the Fourth Amendment do not apply to open public areas where an individual could not reasonably expect his actions to be kept private. This same reasoning has been applied to cameras and surveillance in the public arena. It is not reasonable to expect that a person’s face is protected under the Fourth Amendment if the individual knowingly appears in a public place (Blitz).

In her article titled, “The Observer and the Observed: Re-imagining Privacy Dichotomies in Information Privacy Law”, Marcy Peek discusses the changing role of the individual from being ‘watched’ to becoming active participant in being ‘observed’ (2009). She notes that the lines between privacy expectations are becoming increasingly blurry as technology advances and as societal norms are changing to allow greater levels of observation of individual activities to occur, while individuals are also becoming more used to being observed, and are often not only actively participating, but enjoying the idea of being watched (Peer p 59).

The public seems to have generally accepted the increased security measures that have been put in place
since 9/11. What initially stirred outrage, is now viewed as a mere irritation. The trade-off between privacy and security has reached a sort of equilibrium.

IV: Methodology.

The first step in researching the question of whether or not the Alaska Division of Motor Vehicles should implement a Facial Recognition Technology System to deter and detect fraud was to identify the aspects surrounding the issue. Although the current status of a driver’s license as a national form of identification was the result of a linear progression through history, the aspects identified through investigation of available data revealed that a policy recommendation must consider certain events as distinct and relevant issues that must inform the policy making process.

Figure 1: Policy Recommendation Framework

Data Collection: The limited time allowed for the project made it impractical to pursue any primary research methods for collecting information. Thus, the majority of the information collected consisted of legal law reviews,
individual state web sites, news articles, government web sites and journal articles.

The initial search for related literature on the subject of driver’s licenses, Real ID and biometrics began with the Google search engine. Individual state motor vehicle sites were also accessed via the internet for information on driver’s licensing policies and requirements. The Consortium library was the first site accessed to search for journal articles that discussed the history of driver’s licensing in the United States. The reference sections from the journal articles and the law reviews provided further leads to related information.

To ensure that information from the internet was accurate, the data was cross-checked with information provided in government generated documents and news articles. Additionally, questions specific to the Division of Motor Vehicles were checked against the DMV website and the Director of the Division of Motor Vehicles was available to answer questions and provide information and guidance.

Data Analysis: The collected data was then sorted by theme. These included: Historical information, legal analysis of privacy considerations, Alaska information (legislative archives, minutes, statutes, Alaska DMV site), government sources (state DMV information, National Highway Safety, etc.) and biometric information.

Alaska legislative information was limited to the minutes and bills that were presented or passed after the passage of Real ID in 2005. Biometric information was
limited to the time frame of implementation of the technology by the states, beginning in 1998 to present. Real ID data was collected from information generated in 2005 to present.

Information collected from the state web sites regarding security policies for driver’s licensing and identification cards was put into a chart which listed each state along the vertical and used separate columns which were horizontally labeled with security measures, such as biometric data collected, centralized licensing, legal presence check, and social security online verification implementation and the dates the policies and procedures were implemented. The chart provided a visual indicator of trends in security procedures by state. Information from the comprehensive state-by-state spread sheet was consolidated by date into the smaller tables presented in the findings below.

The National Highway Safety Transportation Administration site and the Alaska Division of Motor vehicles site provided information on national and state numbers of driver’s licenses and other statistical data. This information was used to produce the chart on state driver’s licenses.

V. Findings:

States are continuing to implement security measures and standardize documents as part their efforts to combat issuance and use of fraudulent driver’s licenses. The scope of the problem is evident when the volume of
licenses issued in the United States is examined. In 2010 there are approximately 210 million licensed drivers in the United States. The challenge for motor vehicles administrations to verify authenticity of the documentation used by applicants to establish identity is enormous.

**Chart 1: Licensed Drivers by Year**

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of Driver's Licenses (million)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1920</td>
<td>60</td>
</tr>
<tr>
<td>1930</td>
<td>70</td>
</tr>
<tr>
<td>1940</td>
<td>90</td>
</tr>
<tr>
<td>1950</td>
<td>100</td>
</tr>
<tr>
<td>1960</td>
<td>170</td>
</tr>
<tr>
<td>1970</td>
<td>190</td>
</tr>
<tr>
<td>1980</td>
<td>210</td>
</tr>
</tbody>
</table>

**Biometrics:** As part of the effort to keep personal information secure and to ensure that an individual’s identification is specific to that individual, identifiers are increasingly being deployed using biometric technologies to produce a numerical signature based on a unique physical characteristic. Driver’s licenses already contain biometric data including weight, height, hair and eye color as well as a photograph of the card holder. However, these identifiers are easily altered, (e.g. hair dye, weight loss or gain, contact lenses) (Woodward, 2003).

Of the five biometric methods currently in use today for identification purposes, only two are in use by
motor vehicle divisions. Voice Recognition, Hand Geometry, and Iris Scans are often used for entry into secure facilities, but have not been employed in driver’s license processes. Some states require applicants to submit a fingerprint when they apply for a driver’s license including, Arkansas, California, Georgia, Hawaii, Texas and West Virginia. Some of these states include the fingerprint on the card and some store the print in a database (Harris, 2008).

Facial recognition systems are currently in use in 38 states. The following chart reflects the implementation since systems began to be deployed in 1998.

Following implementation of facial recognition systems states have reported immediate results in detecting fraud and duplicate licenses soon after installation. Illinois reports that between 1998 and 2007 over 5,000 cases of
identity fraud were detected (Harris). Indiana’s system flagged 463 identity related cases in the first six months of implementation (Notary, 2010). In less than two months, the Nebraska Department of Motor Vehicles was able to detect 41 cases of fraud.

**Cost of Fraud:** The cost of fraud to the American public cannot be ignored in a discussion of implementation of security measures. The Department of Homeland Security reports that:

“Between 2000 and 2006 there was a 791% increase identity theft in the U.S. In 2005 alone, identity theft cost U.S. households $64 billion of which 28% involved a driver’s license.” (DHS, 2008).

Because driver’s licenses are currently accepted throughout the United States as legitimate identification, it is important that all states take measures to verify and authenticate documents to the greatest extent possible.

**VI. Policy Considerations:**

Under current Alaska Statute the law will not allow the expenditure of funds to implement Real ID provisions. This leads to policy question number one:

**Q:** Would implementation of a facial recognition system be legal under AS 44.99.040?

**A:** Yes. AS 44.99.040 prohibits expenditure of funds “solely for the purpose of implementing or aiding in the implementation of the requirements of the federal Real ID Act of 2005.” Real ID does not require any
biometrics beyond the photograph and signature already required by Alaska.

Alaska’s population is much smaller than most other states.

Q: Would the expenditure be worth it?

A: Current information indicates that Facial Recognition Systems can be implemented for about $450K. The final cost is dependent on many other factors including the level of system required.

From the standpoint of fraudulent activity, it is impossible to know how many fraudulent licenses currently exist in Alaska. As of 2009, there were 524,158 licensed drivers in Alaska. It is anticipated that the bulk of duplicate licenses would be detected in the first two months, based on information from other states (KETV, 2009; McKay, 2009), and would then go down to a very small number. At that point the system would act as a deterrent.

An additional consideration is the ability to share the system with law enforcement to aide in the apprehension of criminals who may be using driver’s licenses in carrying out their illegal activities. Florida police partnered with their DMV by phasing in facial recognition technology in their patrol cars. “by 2009 deputies had made 496 arrests that could be directly attributed to facial recognition technology and confirmed another 485 that did not require arrest.” (Main, 2010).

Another reason to implement the technology is for
public safety. Although some individuals will choose to drive regardless of whether or not they have a valid driver’s license, it may work to prevent some from getting behind the wheel. "In 2000 alone, drivers with invalid licenses killed more than 6,200 people. The total economic impact of those invalid divers in that year is estimated to have exceeded $25 billion, according to the National Highway Traffic Safety Administration." (Harberson, 2002).

VII. Recommendations:

The Alaska Division of Motor Vehicles should move forward with the process of implementing a facial recognition system to detect and deter fraudulent licenses. The vast majority of other states are already using the technology and report that they are very pleased with the results. The system will enhance the security measures already in place and will potentially help to reduce fraud in other agencies that depend on driver’s licenses for identification of clients for services and the law enforcement agencies on the state and federal level. Implementation will help to ensure that Alaska driver’s licenses are secure and will identify frauds or duplicates.

Alaska is already a member of the Driver’s License Compact, and thus already works with other states to identify dangerous drivers. The database of driver’s license photos is under the control of the Alaska DMV which is required by state law (HB 65) and federal law (Driver’s License Privacy Act) to protect information collected and stored by the agency.
Implementation of the technology does not run afoul of Alaska Statutes because the Real ID Act does not require biometrics for driver’s licenses or identity cards.

**VIII. Conclusion:**

No technology or method is foolproof or will ever be completely secure. However, implementing facial recognition technology at the Alaska DMV will provide another level of security for driver’s licenses. The fact that it will not be able to prevent all fraud should not be an argument against its implementation, in the same way that arguing that a determined thief can come through the window should deter a person from purchasing a lock for their door. Security can be measured in degrees and it is by taking all the various measure available to it that the greatest amount of security can be gained.

Alaska may not have any fraudulent driver’s licenses in circulation, but even if that is the case, implementing the technology will serve as a deterrent to those who may contemplate fraud in the future. The Division of Motor Vehicles in Alaska has continued to move forward in implementing the available tools to provide secure and verifiable licenses for its customers and should continue to do so by implementing facial recognition technology.
References


Etzioni, Amitai (2004) License to hide: Security implications of


