

Biometrics

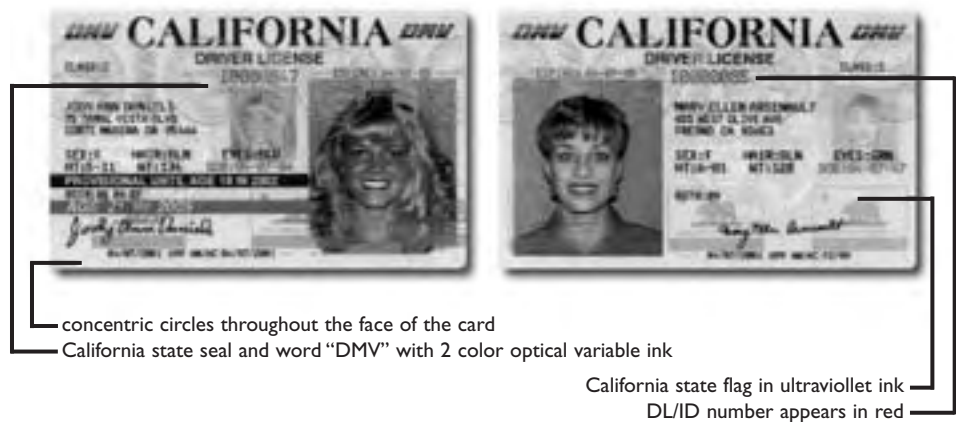
The future of identification

BY CHAD S. FOSTER

Are you who you say you are? This simple question is the source of many difficult decisions that states are facing in response to the Sept. 11 attacks. Four out of the five hijackers on American Airlines Flight 77 that crashed into the Pentagon used Virginia driver's licenses. How did the terrorists, who were not Virginia residents, acquire valid driver's licenses? Investigators revealed two main reasons for the false identifications. First, a woman was convicted in August 2001 of providing false forms for licenses to thousands of illegal immigrants. Second, the Virginia Department of Motor Vehicles' requirements for driver's licenses were insufficient and contained loopholes that the terrorists exploited.

These events have caused states to examine their license and identification systems. Does a photo and brief description of physical characteristics identify a person? Does the license identify all legal residents properly? Does it prevent outsiders from easily forging documents? State officials, departments of motor vehicles and identification experts are seeking ways to improve the accuracy of information found on driver's licenses and are using state legislation and biometrics as a means to accomplish this.

Biometrics is the science of applying statistical techniques and methods to biological data. State DMVs currently use sex, height, weight, eye and hair color to identify licensed drivers. This system lacks many critical features that include exact and unique identifiers as well as innovative



Security features added to the California driver's license in 2001. A state leader in biometric gathering, California plans to further develop its fingerprint capabilities to ensure, "one individual, one license, one record." Photo sent by Steve Fong, Department of Motor Vehicles, Systems Development Unit, Sacramento, CA.

measures to prevent forgery. According to a Jan. 18, policy brief by the Progressive Policy Institute, "People can falsely identify themselves by simply borrowing a driver's license from someone with a similar appearance...false identification leads to billions of dollars in fraud every year...and it allows terrorists to plot attacks on the United States from within."

States were aware of problems with their identification procedures before Sept. 11, but a lack of funding and support prevented them from taking the necessary steps to improve the systems. Many states did not believe that improved biometrics was the answer to the country's identification problems. This was the case despite credible advances in the field of biometrics including the use of thumbprints, hand geometry and iris scans for identification. Following Sept. 11, convincing argu-

ments can be made for biometrics in support of both short-term national security and long-term financial benefit, and as a result, states are making driver license and identification reform a top priority.

State leadership

Many states are looking at California as a model for legislative and biometric reform. In addition to stringent license requirements, California has been collecting thumbprints for more than 25 years. Under existing law, every application for an original drivers license or renewal is required to contain a legible print of the thumb or finger of the applicant. According to the California DMV, the state maintained central database includes a fingerprint copy of every licensed driver. These records are accessible from any of the 170

continued on page 22

continued from page 19

state motor vehicle centers, but authorized access outside of the DMV is restricted to state and local law enforcement for traffic safety cases only.

Six other states recently have begun collecting fingerprints for new or renewal driver's licenses. Colorado, Georgia, Hawaii and Texas require fingerprints while Arkansas and West Virginia offer fingerprint collection on a voluntary basis only. Among these states, Arkansas, Colorado and Georgia are able to compare an individual fingerprint record against an entire database. A check called the "one-to-many," compares the applicant's fingerprint to the entire database of fingerprints to prevent residents from obtaining multiple licenses in different names by using fraudulent documents. Second, a check called the "one-to-one," is designed to prevent identity theft by ensuring applicants are who they say they are. Illinois and West Virginia are able to do similar database comparisons using facial recognition. As other states develop similar programs and systems, the need for interstate database sharing becomes critical. States need to work collectively on information security measures, standards and procedures.

Data collection and security

Proposed legislation around the country would give state DMVs the option of collecting additional biometrics. Nebraska's LB 924, introduced on Jan. 9, would allow the department of motor vehicles to capture and store biometric identifiers. Likewise, Virginia's SB62 would allow the state DMV to take thumbprints or other types of biological identification – eye scans, pictures or DNA samples – and place the information on all applications for driver's licenses. In Georgia, HB1008 would allow the department to require applicants to submit fingerprints by means of an inkless fingerprint scanning device.

Many people for privacy reasons are reluctant to provide agencies with personal identification. In the past, criminals have used social security numbers to tap into private financial accounts. Criminals also have retrieved credit card information off the Internet without being traced.

Criminals will make every effort to exploit personal information for financial and personal gain. To assure the public, legislators have included language to control the disclosure of personal information. Nebraska LB924 proscribes: "No officer, employee, agent, or contractor of the department of a law enforcement officer shall release a digital image, a digital signature, or biometric identifiers except to a federal, state, or local law enforcement agency for the purpose of carrying out the functions of the agency upon verification of identity of the person requesting the release of the information and the verification of the purpose of the requestor in requesting the release." Furthermore, the bill charges any violator of the above disclosure with a Class IV felony.

Virginia's SB62 dictates that any personal information collected by the DMV "is confidential and will not be divulged to any person, association, corporation, or organization, public or private, except to the legal guardian or the attorney of the applicant or to a person." Other states are

following suit with similar restrictive language to ensure controlled access and protect personal information.

Legislation will enable states to quickly adapt and implement new and improved security measures, and states see biometric gathering as one such tool. What will be the impact of this technology on the states? The smart card is one example of such technology. Smart cards are identification cards with an implanted microchip that can support multiple applications such as encrypted identity storage and financial services. How would you like to use your smart card for everything and not have to show another form of identification? The Federal Computer Acquisition Center and General Services Administration are working on smart cards for the federal government that, in time, may develop into the standard identification for every American citizen. ★

Chad S. Foster is a policy analyst in the Public Safety and Justice Group at The Council of State Governments.

The Future of Biometrics

Fingerprint Scan. The fingerprint is one of the most widely used biometrics in the world today. Even though it is a convenient and low-cost biometric, it may be considered intrusive because of its association with law enforcement usage.

Hand Geometry. Hand-geometry systems use optical systems to map key geometrical features of the topography of a hand to verify an individual's identity. Hand-geometry technology uses a number of different measurements such as finger length, skin translucency, hand thickness and palm shape. It is highly accurate and nonintrusive.

Facial Recognition. Several state motor vehicle departments are currently using facial recognition software to provide identity authentication for drivers' licenses. Facial recognition is based upon comparison of the characteristics of a live scan of a face against a stored template of facial characteristics. This biometric is captured through the use of a video/digital camera and is

relatively easy to implement.

Iris Scan. This biometric uses a video/digital camera to take a picture of the eye and iris. It is then compared against the live iris scan image obtained by having the user look into a reader. This biometric is far less invasive than a retinal scan.

Voice Recognition. Voice verification extracts specific and unique features from a person's speech, such as pitch, tone, cadence, harmonic level and vibrations and stores and uses them to differentiate that person's voice from other voices. Voice is a convenient verification system for use in telephonic transactions. Voice verification can greatly enhance security for dial-up computer links and terminal access so it is particularly popular for logical access control applications.

Source: Smartcard Policy and Administrative Guidelines, General Services Administration, Feb. 8, 2002