

- 2 Proving identity
- 3 Licensing standards in other states
- 3 Current proposals
- 4 **Box: Biometric Identifiers**
- 4 Issues in the debate

Standardizing Driver's Licenses: Security, Privacy, and Other Issues

Proposals to standardize state driver's licenses and for states to share data on drivers have fueled debate as to whether these changes would be prudent security measures or an unwise step toward establishing a national identification system. These proposals have received more attention since the September 11 terrorist attacks on the World Trade Center and the Pentagon, as the terrorists had obtained identification documents that they used to obtain credit cards, board the airplanes, and otherwise function in American society.

The proposals, including federal legislation, would set uniform minimum standards for states to follow in issuing driver's licenses and in establishing residency and identity; allow states to share information on drivers and to check that information against federal databases; and require licenses to include biometric identifiers such as fingerprints, eye scans, or facial recognition. In May 2002, a spokesman for Homeland Security Director Tom Ridge said that the Bush administration opposes a national identification system but is working with some groups that propose standardizing licenses. Several states have revised their standards for obtaining driver's licenses, and others — including Texas — are considering similar measures.

Because driver's licenses are used routinely for identification in the United States, some observers argue that standardizing licenses and linking databases with driver information would result in a driver's license becoming a *de facto* national identification card. Some supporters of a national identity card system argue that state-issued driver's licenses are the logical basis of such a system because offices for distributing the licenses already exist, people are accustomed to using the licenses for identification, and authority for issuing the cards would remain dispersed rather than centralized federally. Others

As with other issues in the wake of September 11, the debate over standardizing driver's licenses centers on potential conflicts between security and civil liberties.

argue that a uniform identification system would be a federal responsibility that should not be imposed on the states.

While some supporters of enhancing state driver's licenses are interested only in making the licenses more uniform, others cite the additional potential benefit of making the licenses more secure as identity documents. Supporters of these proposals say that because driver's licenses already amount to identity cards, the government has a responsibility to make them more secure. They say the proposals could help prevent identity theft, make it more difficult to counterfeit licenses, and strengthen national security by making it harder for terrorists to use false names and identities. Supporters say these aims could be accomplished in a manner that respects individual privacy and limits potential abuses.

Opponents of these proposals argue that standardizing the state driver's license system and sharing driver information among states would lead to implementation of a national identification system that would erode individual privacy and would be vulnerable to many potential abuses. They say the proposals would not necessarily make the licenses more secure, prevent fraud, or help combat terrorism.

Proving identity

In the absence of a national identification card, U.S. citizens use various documents to prove their identity. State-issued driver's licenses, the most common form of identification, are used to board airplanes, rent cars, write checks, and more. Other forms of identification include passports, birth certificates, workplace-issued cards, and credit and debit cards that bear pictures of the cardholders.

While Social Security numbers often are used for identification, Social Security cards contain no photograph or other feature to identify the cardholder. Various proposals have arisen to use Social Security numbers as the basis for a national identification system. In 1996, the 104th U.S. Congress incorporated a provision into an immigration bill requiring states to put Social Security numbers, either visible or machine-readable, on all

driver's licenses. Supporters said this measure would strengthen identification procedures and help crack down on illegal immigration. However, the 106th Congress repealed the measure in 1999 because of concerns about privacy abuse and compliance costs.

Each state has its own system and standards for issuing driver's licenses, and each state decides what is necessary to prove identity and state residency when applying for a license. These systems have resulted in more than 200 valid forms of identification, according to the American Association of Motor Vehicle Administrators. Some of the September 11 hijackers reportedly obtained driver's licenses or identity cards from states with less stringent requirements, then used those cards as identification in carrying out their plot.

Texas system. Texas Transportation Code, sec. 521.142 requires applicants for driver's licenses to state their full name and place and date of birth and to verify that information by presenting proof of identity to the Department of Public Safety (DPS). Texas Administrative Code, Title 37, sec. 15.24 lists documents acceptable as proof of identity. Applicants must present one type of document from a list of "stand-alone" identification or one type from a list of "documented" identification, plus one or more types of support materials. Stand-alone identification includes a valid or expired Texas driver's license or identification card, a U.S. passport, and certain U.S. immigration documents. Documented identification — recorded government documents whose authenticity can be verified — includes an original or certified copy of a U.S. or Canadian birth certificate. Supporting materials include public school records, marriage licenses, utility bills, voter registration cards, and Social Security cards.

The 77th Legislature in 2001 enacted, but Gov. Rick Perry vetoed, HB 396 by Wise, et al., which would have defined in statute the types of proof of identity necessary to receive a driver's license. Debate centered on whether the bill would have made it easier for illegal immigrants to obtain driver's licenses by requiring DPS to accept a foreign birth certificate as proof of identity.

Each state has its own system and standards for issuing driver's licenses, and each state decides what is necessary to prove identity and residency.

In April 2002, DPS proposed amending the Administrative Code to revise the list of documents acceptable for proving identity, including requiring that passports and U.S. Immigration and Naturalization Service (INS) documents be current and eliminating several immigration documents from the approved list. DPS commissioners may vote on the proposed rule this summer.

Each Texas driver's license contains a magnetic strip that carries the information printed on the front of the license. This practice also is common in other states. Transportation Code, sec. 521.126 prohibits DPS from including on the magnetic strip any information except what is printed on the license and a physical description of the licensee. DPS must ensure that the information is used only for law enforcement or governmental purposes.

During the 77th Legislature, the Senate passed SB 293 by West, which would have created criminal penalties for accessing or using electronically readable driver's license information and for compiling or maintaining a database of such information, with exceptions for official or law enforcement uses and for merchants transcribing information onto or verifying a check or computing a purchaser's age. However, the House rejected the measure.

Since the late 1960s, applicants for Texas driver's licenses and identification cards have had to submit a thumbprint when receiving or renewing their cards. The prints are not embedded in the licenses but are stored in a DPS database. In 1995, DPS began storing the prints digitally, instead of using ink on paper. So far, according to DPS, the prints have been used only for identification — for example, to identify victims of airplane crashes or natural disasters.

Licensing standards in other states

Several states have tightened standards for obtaining driver's licenses since September 11, according to a January 2002 report by the National Conference of State Legislatures (NCSL). For example, notarized affidavits no longer are acceptable to prove residency and identity in Virginia, where several of the hijackers obtained licenses by using a notarized form attesting that the applicant was a state resident.

At least three states now verify immigration status with an INS database, according to NCSL. At least eight states do not issue driver's licenses to people who are not in the United States lawfully, but at least four states issue licenses to any resident, without regard to immigration status.

Six states in addition to Texas collect fingerprints when people apply for or renew driver's licenses. Of these states, only Georgia uses the prints to verify identity when issuing replacement licenses. West Virginia uses facial recognition technology, a type of biometric identifier. (See box, page 4.)

Texas is among 29 states that use digital images on licenses, allowing computer storage of drivers' pictures. In Texas, these digital images are retrieved only if a question arises when a person applies for a license, and the images generally cannot be retrieved at local DPS offices.

Biometric identifiers. New technology that allows biometric identifiers such as fingerprints, retina or iris scans, and hand and face geometry to be included on identification cards also has become controversial. Some propose requiring driver's licenses or other identity cards to carry biometric information unique to the cardholder in a magnetic strip or computer chip. A card presented at airports and other places could be scanned and the biometric information checked against a database to identify the cardholder.

The 77th Texas Legislature enacted HB 678 by McCall, which prohibits the capture of a biometric identifier for a commercial purpose unless the person giving the identifier consents. People and governmental bodies who possess biometric identifiers may not sell or otherwise disclose them unless the individual consents to the disclosure; the disclosure completes a financial transaction requested or authorized by the individual; the disclosure is required or permitted by a state or federal law; or the disclosure is made by or to a law enforcement agency for a law enforcement purpose.

Current proposals

The debate about enhancing state driver's licenses intensified in early 2002 when a task force of the American Association of Motor Vehicle Administrators (AAMVA) proposed that Congress set uniform minimum

Biometric Identifiers

Some current proposals would require driver's licenses or other identity cards to carry biometric data unique to the cardholder in a magnetic strip or computer chip. The most common biometric identifiers in use are:

Fingerprint scan. A person places one or more fingers onto a fingerprint scanner, and the system stores unique characteristics of the fingerprint (such as the endpoints and junctions of ridges, whorls, loops, and tilts) for later comparisons.

Hand geometry. These optical systems map key geometric features of the topography of a hand from measurements such as finger length, skin translucency, hand thickness, and palm shape. Live hand scans are compared against stored scans.

Facial recognition. These systems compare the characteristics of a live scan of a face against a stored template of facial characteristics by means of video or digital cameras. They can use either spatial measurements, such as distances between the eyes and ears, or a method that evaluates the entire face.

Eye scan. An iris scan uses a video or digital camera to take a picture of the structure and pattern of the eye's iris, which then is compared to a live iris-scan image obtained by looking into a reader. A retina scan measures the pattern of blood vessels along the retina (a nerve on the back of the eye), which is unique from person to person.

Voice recognition. These systems extract specific, unique features from a person's speech, such as pitch, tone, cadence, and harmonic level and vibrations, and stores the features for later comparison with a live voice.

Source: U.S. General Services Administration.

standards for states to meet in issuing licenses. These standards could include acceptable types of identification and a uniform definition of residency. AAMVA also proposed establishing minimum security features such as holograms and biometric identifiers on licenses;

stiffer penalties for fraud related to licenses; and federal funding for technology to enable states to check each other's motor-vehicle databases to find out if an applicant holds a license from another state and to check the applicant's driving history. Other proposals include allowing states to check federal databases, such as those of the INS and the Federal Bureau of Investigation, for immigration status and criminal records.

In May 2002, U.S. Reps. James P. Moran (D-Va.) and Thomas M. Davis III (R-Va.) filed H.R. 4633, which would establish uniform standards for state driver's licenses, including requiring states to embed in each license a computer chip containing biometric data of the license holder. The bill also would require states to participate in a program to link their motor-vehicle databases and would require the federal government to issue guidelines for the states, including standards for the biometric data, security features, documenting identity and residency of license applicants, and numbering driver's licenses. H.R. 4633 would appropriate \$300 million for grants to help states implement the bill's requirements.

U.S. Sen. Richard Durbin (D-Ill.) has said he plans to introduce legislation to improve the reliability and security of state driver's licenses. He said the legislation will call for uniform minimum standards for issuance and administration of licenses, federal-state sharing of information to verify data, and enhancing penalties for fraud and for making or using false identification cards.

In early May, a U.S. House Judiciary subcommittee approved H.R. 4043 by Rep. Jeff Flake (R-Ariz.), which would require states to coordinate expiration dates on driver's licenses or other identification documents with expiration dates on nonimmigrant visas. Federal agencies could not accept identification documents from states that failed to comply.

Issues in the debate

The debate over these proposals — linked with the debate over the creation of a national identification card — centers on issues of security, privacy, potential abuses, use of biometric identifiers, and combating terrorism.

Both supporters and critics of these proposals point to public opinion polls to bolster their positions.

Proponents cite public support for increasing the security of driver's licenses and creating a national identification system. In an April 2002 poll commissioned by AAMVA, 77 percent of those surveyed said they would favor a proposal to require states to develop similar procedures for issuing driver's licenses and identification cards and to allow states to search other states' records to verify the accuracy of information provided by applicants and to enable law enforcement officials to confirm licenses' validity.

Supporters also cite a poll by the Pew Research Center soon after September 11, in which 70 percent of those surveyed said they favored establishing a national identity card. Almost 60 percent of those surveyed in November 2001 by National Public Radio, the Kaiser Family Foundation, and Harvard University's Kennedy School of Government said they favored requiring everyone in the United States to carry an identity card issued by the federal government.

Critics counter that as people become more familiar with the concept of a national identification system, support falls. According to a Gartner poll released in March 2002, only 26 percent of those surveyed supported a national identification system, while 41 percent opposed the idea. Gartner said its poll showed that people would support a national ID card only for very specific, limited purposes.

Issue 1: Security of driver's licenses

Supporters of the proposals say:

Making state driver's licenses more uniform and sharing data on drivers would help make licenses more secure and accurate. Varying state standards have resulted in easily exploitable systems under which people can obtain licenses fraudulently or without adequate documentation. If requirements for issuing licenses were uniform, anyone looking at a license would know what minimum standards the licensee had met to obtain the license and would know how reliable the license was for establishing identity.

Driver's licenses would become more secure if the types of documents used to prove identity were standardized across states and if information on the cards could be verified and cross-checked with other sources of information, such as a state agency responsible for birth certificates or federal agencies such as the INS and Social Security Administration. These steps would help prevent people from obtaining licenses under false names.

These proposals would not undermine the core function of state driver's license agencies but would standardize and enhance their duties. These agencies already verify identity and residency and issue identification cards to people who are not drivers.

The current system under which states check for "problem" drivers allows states to identify only drivers who have had their licenses suspended or revoked. If state motor-vehicle databases were linked and agencies routinely could inspect the driving records of all people applying for licenses, an agency could determine whether a potential driver held a license from another state and whether the driver had a record of traffic violations or drunk driving without having had his or her license suspended or revoked. Also, the current system makes it difficult to distinguish among drivers with similar names, while the proposed system could enable this by using biometrics to identify individuals accurately.

If identity cards were uniform in appearance and the technology for placing information on a magnetic strip or computer chip were the same in all states, then law enforcement officials, financial institutions, and bar and restaurant workers in all states could read licenses easily and accurately. Correcting mistakes on licenses would be no more difficult than it is now.

States would not find it costly or burdensome to adopt uniform minimum license standards. These proposals typically would involve simple, inexpensive changes, such as revising the list of acceptable documents to prove identity and revamping the information required on the card. Nor would the proposals infringe on states'

Both supporters and critics of a national identification system point to public opinion polls to bolster their positions.

autonomy. States would retain the authority to issue and rescind licenses under their own rules and through their own agencies.

Critics of the proposals say:

Standardizing which documents states could accept as proof of identity would not ensure the security or accuracy of driver's licenses. Licenses are only as good as the supporting documents, such as birth certificates and Social Security cards, which could be forged or obtained fraudulently even if states had uniform standards for what documents to accept. In May 2002, a Social Security Administration official stated that noncitizens wrongly received about 100,000 Social Security numbers in 2000. Even if these proposals were enacted, hundreds of different types of birth certificates and other supporting documents still would exist, making it difficult to identify fraudulent documents.

Uniform nationwide requirements would not enhance the primary function of a driver's license — to ensure the safety of drivers. Rather, these proposals would undermine the core function of driver's license agencies and would expand their duties unwisely to include authenticating people's identities for purposes other than driving.

States do not need to share information on all drivers. State agencies already can check with other states to see if a person applying for or renewing a license has a suspended or revoked license or holds a commercial license in another state. If problems exist with these systems, they should be fixed rather than expanding the systems to include law-abiding drivers.

Making driver's licenses more important in people's daily activities would increase the incentive to produce fraudulent licenses. Identity theft would become more difficult to remedy if people had to deal with the bureaucratic machinery necessary for such a large, uniform system. This bureaucracy also would make it very difficult to correct simple errors, just as correcting a credit report can be difficult now.

A uniform licensing system with linked databases would be costly and difficult to implement, amounting to an unfunded mandate on the states.

Monitoring to ensure that states met the uniform standards also would be expensive.

Uniform requirements would infringe on states' authority to set their own standards. States need flexibility in setting standards and issuing licenses to allow for exceptions when warranted. States with weak standards or problems in issuing their licenses can address those problems themselves.

Issue 2: Protecting privacy

Supporters of the proposals say:

These proposals could make state driver's licenses more secure without compromising citizens' privacy. For example, strict criteria could be established for the circumstances under which information stored on the cards or in linked databases could be retrieved. The use of linked state databases could be reserved for state driver's license agencies to verify names, birth dates, addresses, and Social Security numbers.

Anyone living in the mainstream U.S. society already is the subject of a trove of information in various databases maintained by government agencies, banks, insurance companies, health-care providers, credit card companies, Internet vendors, and grocery and retail stores. Linked databases are not necessarily to be feared because they can provide more complete information about people. Some databases with personal information already are linked, and governmental agencies already share this information. For example, Texas uses databases of newly hired employees to identify people who owe child support.

Critics of the proposals say:

Linking databases with driver information would erode personal privacy and increase governmental power dramatically by increasing government access to personal information. The American tradition of restricting government access to this information except for good, justifiable reasons should not be altered.

While many databases now hold information about individuals, the databases are not linked.

Linked databases make it easier to track and monitor people, further eroding privacy. Eventually, promises of restricting access to driver information would be ignored just as prohibitions against using Social Security numbers for purposes outside of the Social Security Administration have been ignored. Americans' privacy would be eroded even more if nationwide identity databases were linked to private databases, such as those with people's credit history, spending habits, voting records, medical history, and employment records.

Issue 3: Potential abuses

Supporters of the proposals say:

State driver's licenses already function as *de facto* identification cards without the widespread abuses anticipated by critics of these proposals. Penalties could be increased for abuse of driver information by government workers and others, and voters' elected representatives could address any problems that arose if governmental or private entities inappropriately demanded to see licenses.

People are accustomed to using driver's licenses to conduct all kinds of business, and this practice could continue easily with standardized licenses. A person who objected to producing a driver's license as identification could use another document such as a passport or workplace identification card. Driver's licenses are optional documents, and anyone concerned about potential abuses may refrain from obtaining one.

Many other countries, including western democracies such as France, Germany, Belgium, and Denmark, use national identity cards without serious abuses. These proposals fall far short of such comprehensive identity checks.

Critics of the proposals say:

If these proposals became law, unscrupulous bureaucrats could use the information on driver's licenses inappropriately, and the government could begin to compel people to produce the cards on demand whether or not a person was suspected of wrongdoing. The government could begin to demand the identification when the nation was perceived

to be experiencing a "crisis" in an area such as illegal immigration, gun ownership, illegal drugs, or welfare fraud; when someone bought "suspicious" items like fertilizer that can be used to make bombs; or when someone used cash to buy a bus ticket.

A uniform driver's license could become a type of "internal passport" required for routine activities such as obtaining a job, renting a hotel room, entering a public building, cashing a check, opening a bank account, or receiving federal benefits. This would increase the incentive to produce forged licenses and to commit identity theft.

These proposals actually could discourage some people from trying to obtain driver's licenses, resulting in an increase in unlicensed, untrained, and uninsured drivers. Practically speaking, a driver's license is almost mandatory to work or attend school in many parts of the United States.

Issue 4: Use of biometric identifiers

Supporters of the proposals say:

Including biometric identifiers on driver's licenses would increase confidence in the accuracy of the cards and make them more difficult to forge. If a license contained a person's unique fingerprint or retina scan, these identifiers could be matched with the person presenting the license to ensure accurate identification. Safeguards can be put into place to ensure that biometric information is not abused or shared. Some businesses and the military use identification cards with biometric identifiers and have reported no abuse or privacy problems.

Critics of the proposals say:

Using biometric identifiers on driver's licenses would be a further invasion of individual privacy by the government. Biometric identifiers can contain more personal information than the photographs used on current licenses. Analysis of biometric information could go beyond identifying a person and could reveal highly sensitive information, such as a person's genetic makeup or medical history, which could be shared with government or private entities.

Using biometrics on driver's licenses would not make the licenses fraud-proof. A different person's biometric identifier could be placed on a license just as a photograph of one person can be placed on a license with another person's name and address. Also, requiring all states to use biometric identifiers could be problematic because the technology for using biometric identifiers is untested for a large population.

Issue 5: Combating terrorism

Supporters of the proposals say:

The recent terrorist attacks on the United States show the need for an accurate, verifiable system of identification. These proposals could help identify people who are in the country illegally and who might pose a threat. For example, if states could cross-check information on potential drivers with federal and state law enforcement agencies, they could find out whether an applicant was on a government terrorist watch list. Agencies also could check with immigration authorities to find out whether a potential driver had overstayed his or her visa authorization.

Critics of the proposals say:

Enhanced state driver's licenses might confirm that people are who they say they are but would not prevent anyone from committing terrorism. Most of the September 11 terrorists were in the United States legally, and most obtained their driver's licenses legally. Standardizing state driver's licenses would not prevent foreign nationals who obtain licenses from overstaying their immigration authorization or from using fraudulent documents to obtain driver's licenses. Also, these proposals would do nothing to combat U.S.-born terrorists like Oklahoma City bomber Timothy McVeigh. Other, less intrusive ways exist to identify and monitor potential foreign terrorists. Immigration laws could be enforced better; agencies could share information on aliens and monitor foreign students better; or foreign nationals and visitors could be issued special identification cards.

— by ***Kellie Dworaczyk***

HOUSE RESEARCH ORGANIZATION



Steering Committee:

Peggy Hamric, *Chairman*
 Roberto Gutierrez, *Vice Chairman*
 Dianne White Delisi
 Harold Dutton
 Bob Hunter
 Carl Isett
 Mike Krusee
 Jim McReynolds
 Elliott Naishtat
 Joe Pickett
 Robert Puente
 Bob Turner
 Steve Wolens

Capitol Extension
 Room E2.180
 P.O. Box 2910
 Austin, Texas 78768-2910

(512) 463-0752
 FAX (512) 463-1962

www.capitol.state.tx.us/hrofr/hrofr.htm

Staff:

Tom Whatley, *Director*; Greg Martin, *Editor*;
 Rita Barr, *Office Manager/Analyst*; Kellie Dworaczyk,
 Patrick K. Graves, Dana Jepson, Travis Phillips,
 Kelli Soika, *Research Analysts*