SUBJECT: Image verification system for issuance of driver licenses

COMMITTEE: Defense Affairs and State-Federal Relations — committee substitute recommended

VOTE: 7 ayes — Corte, Campbell, Berman, Herrero, Hodge, Leibowitz, P. Moreno

0 nays

2 absent — Merritt, Noriega

WITNESSES: For — Mike Nuemann, AXALTO Inc.; (*Registered, but did not testify*: Michael Craig, Houston Police Dept.; Barry Macha; Mike Smith, Texas Department of Public Safety Officers Assn.)

Against — Scott Henson, ACLU

On — Judy Brown, Tommy Davis, Texas Department of Public Safety; (*Registered, but did not testify*: Kim Smith, Texas Department of Public Safety; Margaret Spinks, Texas Department of Public Safety/Driver License Division)

BACKGROUND: Biometric identification includes any automated method of identifying a person based on a physiological characteristic, including facial recognition, thumbprinting, and fingerprinting.

Under Transportation Code, sec. 521.142, an application for a Texas driver's license or identification card must include the thumbprint and a brief description of the applicant. Transportation Code, sec. 730.010 allows the Department of Public Safety (DPS) to use the image only in connection with the issuance of the license and to disclose the image only if expressly authorized by law. The prints are not embedded in the licenses but are stored in a DPS database.

In 2001, the 77th Legislature enacted HB 678 by McCall, which limits the use of biometric identification. People and governmental bodies who possess biometric identifiers may not sell or otherwise disclose them unless the person consents to the disclosure, the disclosure completes a

financial transaction requested or authorized by the person, 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.

DIGEST: CSHB 2337 would require DPS to establish an image verification system for driver's license applicants using biometric identification. DPS would authenticate the applicant's facial image and thumbprint or fingerprint using image comparison technology before issuing an identification certificate, driver's license, or commercial driver's license or permit. The technology would be used to ensure that an applicant was issued only one original license, permit, or certificate; did not fraudulently obtain a duplicate of any of these documents; and did not commit other fraud in connection with an application for any of these documents.

The bill would authorize DPS to use the image verification system to aid other law enforcement agencies in investigating criminal conduct or establishing the identity of a victim of a disaster or crime if a local law enforcement agency were unable to do so.

DPS would require an application for a license to include, in addition to a thumbprint and a brief description of the applicant, a photograph and signature. Under the bill, DPS could use the image of an applicant's thumb or finger to verify the identity of the individual as needed by law enforcement agencies.

CSHB 2337 also would extend the use of a $1 fee required at the time of application of registration or renewal of registration of a motor vehicle to finance the state highway fund until August 31, 2007. The purpose of the state highway fund would be expanded to include the use of image comparison technology in the reengineering of the driver's license system.

The bill would take effect September 1, 2005, and would apply only to a driver's license or permit, personal identification certificate, or the renewal of one of these documents, applied for on or after that date.

SUPPORTERS
SAY: Image verification technology would enable DPS to compare all of the photographs on licenses and identification cards in its system to verify that each person held a license or identification card in only one name. This would combat identity theft and driver's license fraud. The technology would alert DPS to any instance when a person tried to establish a false identity and would ensure that DPS did not issue licenses or identification

cards to those persons. The information collected would be stored on DPS's secure computer system and would be available to other agencies only with DPS approval and supervision.

An image verification system not only would help protect against terrorism but against identity theft. Recent advances in technology have shown facial recognition technology to be effective in identifying and verifying applicants. The system works from a standard digitized facial image stored on a dedicated server, ensuring restricted access and privacy. When an applicant requests a driver license or ID card, DPS operators are able to take a picture, just as they currently do. The image would be run immediately through a facial recognition software database and compared to the previous images stored on file. This technology would prevent people illegally from obtaining valid driver's licenses under false pretenses and from obtaining other "valid" documents to establish a "legitimate" identity.

The system should have the capability to compare "one to many faceprints," which would help investigators identify a number of factors, including an individual holding two or more licenses under different names, different individuals holding a common identity and license number, operator error (such as assigning a new license to a person who already held a license), patterns of error that might indicate collusion, known offenders returning for a new and fraudulent licenses, and perpetrators "shopping" for multiple licenses on a single day.

CSHB 2337 would help combat fraudulent driver's licenses, bolster homeland security, and give DPS the funds to update its aging driver's license computer system, while continuing to protect the privacy of licensees and safeguard Texans' private information. Using biometric identification as part of the license process would increase confidence in the accuracy of the cards and make them more difficult to forge.

Current law requires license applicants to state their full names and places and dates of birth and to verify that information by presenting proof of identity to DPS. DPS has no way to verify many of these documents, such as birth certificates, that are used as proof of identity. This can allow people to obtain licenses under false names or multiple licenses by presenting to DPS fraudulent identity documents. CSHB 2337 would solve this problem by allowing DPS to capture a biometric identifier when a person applied for a license or ID card and to use that identifier to ensure

that the person did not obtain licenses under false names. This would help prevent identity theft and would help ensure the accurate identification of drivers by DPS and others, such as merchants who use the cards to verify identity.

The benefits of the state having a reliable, accurate database that law enforcement could use to authenticate identity in combating terrorism far outweigh unfounded concerns about privacy. CSHB 2337 would not expand current law broadly. DPS already collects applicants' thumbprints, which are biometric identifiers. The bill simply would direct DPS to set up its identification system based on biometrics, provide funding to do so, and allow DPS to use other biometric identifiers, such as facial recognition. The bill would make Texas poised to use the most up-to-date, effective technology.

Other states use biometric identifiers in connection with driver's licenses without violating drivers' privacy or creating serious technical problems. Businesses and the military use identification cards with biometric identifiers and have reported no abuse or privacy problems.

The bill would allow thumbprints to be used only to authenticate identity. Other safeguards would prevent abuse or sharing of biometric information. Transportation Code, sec. 730.007, limits the disclosure of personal information collected in connection with motor vehicle records to disclosure for use by government agencies carrying out their functions. This means that biometrics would be disclosed only when the thumbprints and photographs now collected could be disclosed – for example, for legitimate law enforcement purposes. Concerns about the use of biometrics for some type of mass identification program using cameras in public places are unfounded because these situations would not meet the requirements for disclosure.

OPPONENTS SAY:

The technology provided by CSHB 2337 effectively would allow the government to create a colossal database of its citizens' faces, facilitating the intrusion of the government into the lives of average citizens while doing little to target or thwart criminals. Using biometric identifiers for the driver's license program would erode Texans' individual privacy and unwisely would expand the government's reach and power. This would be another step in government's efforts to gather more and more information on private citizens.

The image verification system greatly would expand DPS's ability to use personal information. The law currently restricts use of thumbprints to, for example, license issuance, child support collection, and the U.S. selective service. However, DPS intends to share image information with other government agencies, and computer hackers or other criminals also could gain access to this information.

Biometric identifiers can contain a greater amount of personal information than the photographs used on current licenses. Analysis of biometric information can go beyond identifying a person and can reveal highly sensitive information, such as a person's genetic makeup or medical history, that could be shared with government or private entities. CSHB 2337 would allow DPS to collect facial images and fingerprints, vastly expanding the agency's current authority to collect thumbprints. Also, the thumbprints now collected are not in a searchable database like the one this bill would establish.

This bill would expand the government's power by allowing biometric information on law-abiding people to be compiled into a massive database of all licensed drivers. If this database were connected with the expanding network of cameras watching people's everyday movements, the government could invade Texans' privacy by tracking their everyday movements.

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, using biometric identifiers on Texas driver's licenses could be problematic because this technology is untested for a large population and often fails properly to identify people. Law enforcement use of the DPS biometric database could lead to increasing harassment of innocent people.

NOTES: The substitute would modify the original bill by limiting the ability of DPS to use the image verification system to aid other law enforcement agencies in establishing a person's identity to situations where the identity of a victim of a disaster or crime could not be established.

The fiscal note for CSHB 2337 estimates that DPS would require $4,450,782 in fiscal year 2006 for hardware and other system components necessary to implement the database system. In fiscal year 2006.

$2,996,555 also would be needed for a one-time image file comparison to enroll, search, and compare existing driver's license and identification card images in the database.