

DMV proposes a major policy shift to biometric systems with significant fiscal and policy implications through an expedited 30-day opt out process

February 3, 2009

Issue:

Should California allow the DMV to make a major policy shift - applying biometric technology to photos and thumbprints received as part of the process for obtaining driver's licenses and identity cards – through an expedited 30-day notice to the Legislature?

Background:

On January 14, 2009, the DMV issued a Section 11 (2008 Budget Act) letter to the Legislature stating its intent to change the terms of its driver license and id card contract – including the use of biometric systems including facial recognition scans and biometric thumbprints on people seeking driver's licenses and ID cards. Unless the Joint Legislative Budget Committee objects within 30 days, the contract with the vendor will take effect.

Biometrics technology is the computerized matching of an individual's personal characteristics against an image or database of images. Initially, the system captures a fingerprint, picture, or some other personal characteristic, and transforms it into a small computer file (often called a template). The next time someone interacts with the system, it creates another computer file (often called a sample), and compares it to the original template or tries to find a match in its database. Because every sample is a little different, biometrics really asks whether the sample is similar enough to the template. The matching of individuals using biometric technology raises serious cost and privacy concerns.

Organizations from across the political spectrum raise concerns with (1) the expedited process the DMV is attempting to use to effectuate major policy and fiscal changes, and (2) the underlying proposal to use biometric technologies without appropriate safeguards.

Procedural Concerns:

- A 30-day expedited opt-out letter to the Legislature is an inappropriate vehicle to move from photographs and thumbprints of millions of Californians to biometric systems that pose a number of privacy and technological concerns if not handled carefully.¹
- The DMV should not be permitted to implement biometric technologies that the Legislature has considered and rejected over the years, without the issues being fully considered and addressed in policy and budget hearings.²
- The DMV does not appear to have statutory authorization to move from thumb and finger prints and photographs to facial recognition technology and other biometric technologies.³

Policy Concerns:

- A government database that contains the facial and thumbprint images of practically every Californian over age 16 raises serious privacy and cost concerns. Where a biometric identifier is used as a unique identifier to catalogue personal information about an individual, it would enable the surveillance, monitoring and tracking of individuals. Law enforcement currently has access to DMV's database of more than 25 million people.⁴ It appears that the biometric thumbprints and facial scans from the DMV will be used in criminal investigations, and as public and private surveillance cameras become more ubiquitous, the likelihood rises of using facial recognition to surveil innocent people.⁵
- The security of the database is critical. For example, because people cannot change their fingerprints (unlike a password or other security measures), if someone compromises the database (i.e., an identity thief substitutes his or her fingerprints or facial scan in someone else's file), it could be a nightmare to resolve. It

does not appear that the DMV has met the basic question: does California "need" these biometric databases? Biometric imaging is in large **not** required by the Real ID Act. While the Department of Homeland Security is pushing for biometric facial image capture, it does not require biometric finger printing. Furthermore, the new Administration has already committed to revisiting Real ID. Therefore, it is not clear what will eventually be required by that law.⁶ Essentially there is no federal impetus behind this move. Further, 11 states have passed legislation against adopting Real ID, while 10 other states have passed resolutions against the Act.

- What is the "bang for the buck" that California would get from the use of these biometric databases? How much is the whole system going to cost? How much would be borne by the state, how much would be borne by individuals? While we do not have access to the access to the contract between the DMV and L-1 Identity Solutions⁷; we do know that creating biometric database systems (facial image and thumbprint) will be very costly, and even more costly to do correctly (in addition to the technology, staff needs be trained, and there must be technical and due process protections in place to ensure that people's licenses are not wrongly denied or taken away because of an error).
- The DMV has also stated that the current cards are not in compliance with the security standards "such as those specified by the American Association of Motor Vehicles [AAMVA]."⁸ It is unclear whether the DMV is referencing the biometric technology or other standards. If the DMV is referencing biometric standards, this seems to be incorrect. The most recent information on the AAMVA website states that the current biometric technologies available are not adequate to do the one-to-many match that AAMVA believes are required.⁹

During this budget crisis, California needs to be absolutely sure that it is not wasting time and money and endangering privacy.

Recommendation:

California organizations listed below strongly urge the Legislature to reject the DMV's proposal to adopt biometric technologies through the use of this expedited process and instead urge the Legislature to consider these important proposals through the normal legislative process which would allow for careful consideration of the important policy and fiscal issues raised.

America Civil Liberties Union
Electronic Frontier Foundation
California Eagle Forum
Consumer Federation of California
Consumers Union
Privacy Activism
Privacy Rights Clearinghouse
World Privacy Forum

¹ Biometrics: Who's watching you? Electronic Frontier Foundation (September 2003), <http://www.eff.org/wp/biometrics-whos-watching-you>, and Biometric Identifiers, Electronic Privacy Information Center, <http://epic.org/privacy/biometrics/default.html>

² For example, see AB 1474 (Koretz) 2002, http://www.leginfo.ca.gov/cgi-bin/postquery?bill_number=ab_1474&sess=0102&house=B&author=koretz, and SB 661 (Dunn) 2001 http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_0651-0700/sb_661_bill_20010223_introduced.pdf.

³ The relevant Vehicle Code sections specify that the print or picture must appear on the application or on the driver's license itself. There is no authorization to convert those images using biometric technology or to create databases. See Vehicle Code sections 12800 and 12800.5.

⁴ Vehicle Code section 1810.5 permits access to the DMV database by law enforcement agencies, and they currently enjoy access to DMV photo and thumbprint data. However, it appears that law enforcement access may be limited by the provisions of the Federal Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.),

⁵ California voters added the personal right of privacy to the state Constitution's inalienable rights (Article I, Section 1). The voter pamphlet specifically stated that this People's Initiative was intended to "prevent government and business interests from stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve another purpose or to embarrass us." (Prop. 11 Ballot Argument, Proposed Stats. And Amends to Cal. Const. with arguments to voters, Gen. Elec. (Nov. 7 1972.)). See also a general discussion of the need to address legal, privacy and efficiency issues with biometrics system, Legislative Analyst's Office, Analysis of the 2001-02 Budget Bill, Department of Motor Vehicles (2740) http://www.lao.ca.gov/analysis_2001/transportation/tran_07_2740_anl01.htm and GAO Testimony, Information Security, Challenges in Using Biometrics, (September 9, 2003) <http://www.gao.gov/new.items/d031137t.pdf>.

⁶ "Feds to 'rethink' license mandate," USA Today, January 22, 2009, http://www.usatoday.com/news/washington/2009-01-22-securelicense_N.htm

⁷ In its analysis of the 2001-02 budget, the Legislative Analysts Office, stated that "estimates for the expanded [facial and thumb and facial print biometrics] system range up to \$50 million, and the time required to fully implement such a system and obtain necessary data files could exceed a decade. Legislative Analyst's Office, Analysis of the 2001-02 Budget Bill, Department of Motor Vehicles (2740) http://www.lao.ca.gov/analysis_2001/transportation/tran_07_2740_anl01.htm

⁸ Section 11.00/11.10 Driver License/Identification/Salesperson Contract Project, APPLICATION, January 14, 2009.

⁹ The possibility of using physiological biometric identifiers to satisfy at least some of the requirements of a unique identifier has been considered. Ultimately, using biometric identifiers holds the promise of a real solution to the problems of identity theft and multiple identities by the same person. However, for a biometric technology to be selected and to be interoperable in North America, it must perform a one-to-many (1-N) record matching or identification function. To date, there have not been any large scale uses of biometric technologies that have performed one to many record matching for populations the size MVAs need to address (300 million records). ...**The current methods of measuring biometric technologies are not adequate for the type of system that AAMVA proposes.** The majority of the research, reports and findings for biometric technologies are related to systems that perform the one-to-one matching. AAMVA suggests that more information is needed to reach a decision. *AAMVA DL/ID Security Framework*, pg 26. (February 2004) (emphasis added) <http://www.aamva.org/aamva/DocumentDisplay.aspx?id={25BBD457-FC4F-4852-A392-B91046252194}>