epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

**WATCHING THE WATCHERS – Policy Report #1 (February 2002)**

# "YOUR PAPERS, PLEASE: FROM THE STATE DRIVERS LICENSE TO A NATIONAL IDENTIFICATION SYSTEM"

**An Assessment of the Proposal of the American Association of Motor Vehicle Administrators (AAMVA) to Transform the State Drivers License into a De Facto National ID Card**


## SUMMARY

The American Association of Motor Vehicle Administrators (AAMVA) Special Task Force on Identification Security has issued recommendations that would turn the state driver license into a de facto national ID card. The proposed scheme, analyzed in detail below, seeks federal legislation to require all states and other jurisdictions to conform to uniform standards for driver license eligibility, proof of identity, license content and document security. It would facilitate greater information sharing between jurisdictions and with state and federal agencies. It seeks to reduce fraud by encoding unique biometric identifiers on licenses and strictly enforcing prohibitions on credential fraud. But the biometric identifier would also enable new systems of identification in the private sector, and will contribute to greater profiling and surveillance of American citizens.

EPIC supports efforts to detect and prevent fraud occurring by means of the state driver's license. New technologies can reduce the risk of counterfeiting and fraud. It is also appropriate for the state Departments of Motor Vehicles (DMVs) to implement improved document security measures to prevent forgery. However, EPIC opposes AAMVA's move to standardize driver's licenses, to collect more and more invasive personal information, and to expand the information sharing capacities of DMVs.

This proposal has all the elements, risks and dangers of a national identification card system. The only distinctions between the AAMVA proposal and other National ID proposals rejected in the past are that (a) the card will not be issued by the federal government but by state motor vehicle agencies under mandatory federal regulations, and (b) the driver's license and DMV issued identity cards, held by 228 million individuals, are not (yet) mandatory. These distinctions are illusory rather than substantive, do not diminish the harm to individuals' privacy, and should not dissuade public opposition to the scheme.

The AAMVA proposal will have far-reaching and profound impacts on individual privacy. It significantly transforms the legitimate purpose of the driver's license: to certify that an individual is competent to drive a motor vehicle. It does not accomplish its stated aims of increased safety and security, but merely shifts the potential for fraud and identity theft to a higher plane, where the intrinsic privacy invasion is greater, and the means of remedying inevitable flaws in the system is more complex and difficult.

> ⇒ ***There must be wider public debate about the details and the consequences of AAMVA's national identification card and driver's license system.***

AAMVA and its industry advisors[1] have not given adequate consideration to either the details of their proposed system or its consequences. They have failed to define the scope of proper access to and use of personal information, failed to consider mechanisms to prevent internal breaches or misuse by third parties, and failed to provide a means to correct abuses when they inevitably occur.

There must be wider public debate about the details and the consequences of AAMVA's national identification card and driver's license system.

EPIC favors legislative proposals that would reduce the risks of counterfeiting and tampering, that would enable greater accuracy and reliability, and that would give individual license holders greater control over the subsequent use of their personal information. EPIC opposes provisions that would facilitate linkage of personal data among federal and state agencies, that would expand profiling of licensed drivers, and that would turn the state drivers license into an open-ended system of identification that could be routinely requested for purposes unrelated to the administration of motor vehicles and the safety of public roads.

**Background of Driver's License Privacy**

For more than a decade, state legislatures, the Congress, and even federal courts have worked to safeguard the privacy of driver record information. Aware that the widespread availability of the personal information obtained by state agencies for the purpose of licensing drivers has contributed to identity theft, financial loss, and even death, efforts to limit the use of driver's record information has been a high priority in the United States beginning with passage of the Drivers Privacy Protection Act of 1994, which limited the ability of state DMVs to circulate information obtained from individuals who applied for drivers licenses. The law, which was challenged by several states on federalism grounds, was upheld by the United States Supreme Court in one of the few recent opinions where the Court has held that the federal government has the authority to regulate state practices.[2]

Other steps taken to limit or reduce the risks of disclosure of personal information include efforts to allow non-commercial drivers to designate an identification number other than the Social Security Number. This change came about in part because of the awareness that the

[1] See http://www.aamva.org/links/mnu_lnkAssociate Members.asp for a list of AAMVA Associate Members & Industry Advisory Board Members and http://www.aamva.org/drivers/drvIDSecurityDocume nts.asp for a list of identification technology companies submitting reports to AAMVA's Special Task Force on Identification Security.

[2] *Condon v. Reno*, 528 U.S. 141 (2000) http://supct.law.cornell.edu/supct/html/98-1464.ZO.html. See also EPIC's Amicus Brief at http://www.epic.org/privacy/drivers/epic_dppa_brief.pdf

use of a single identifier, such as the SSN, was contributing to identity theft and white-collar crime.

States have also passed laws restricting the circumstances when a person can be required to provide a drivers license. And a federal appeals court ruled recently that it is unconstitutional for police to arrest someone for failure to provide identity documents.[3]

All of these developments in the United States over the past decade indicate widespread efforts at all levels of government to protect privacy and to reduce the risk that could result from the use of the state drivers license as a de facto national identifier.

**Analysis of AAMVA recommendations[4]**

Set out below is an assessment of the eight principles contained in the initial AAMVA report. The first three principles put forward by AAMVA are:

*AAMVA(1) Improve and standardize initial driver's license and ID card processes*
*AAMVA(2) Standardize the definition of residency in all states and provinces*
*AAMVA(3) Establish uniform procedures for serving non-citizens*

AAMVA seeks to "improve and standardize initial driver's license and ID card processes." This would include standardizing the definition of residency and imposing uniform procedures for non-citizens[5]. Such a proposal raises serious questions about the appropriate scope of state DMV authority and infringes on a state's right to develop systems and processes to serve the particular needs of its citizens.

AAMVA states its aim to "develop/capture citizenship/residence on document and/or database" within the next year.[6] It is not clear what role establishing citizenship and uniform residency status plays in the core function of a driver's license: ensuring that there are trained, safe drivers on the roads. In fact, the proposed requirements would undermine the public safety rationale of a driver's license by discouraging undocumented aliens from getting licenses, leading to more uninsured and untrained drivers on the roads and contributing to the national road toll of 40,000 deaths per year.[7] Different states have formulated specific responses to this issue based on their individual circumstances, and there is no overriding federal need to establish uniform procedures.

> ⇒ ***Centralizing authority over personal identity necessarily increases both the risk of ID theft as well as the scope of harm when ID theft occurs.***

Establishing citizenship and residency status shifts the role of the state DMVs from licensing drivers to verifying the identity of all Americans. AAMVA relies on faulty reasoning to make its argument: driver's licenses are used as identity cards for purposes unrelated to the operation of a motor vehicle, such purposes

[3] *Carey v. Nevada Gaming Control Board*, No. 00-16649 (9th Cir. 2002) http://caselaw.lp.findlaw.com/data2/circs/9th/001664 9p.pdf

[4] AAMVA Press Release, January 14 2002 [http://www.aamva.org/news/nwsPressReleaseAAM VAHelpsSecureSaferAmerica.asp].

[5] Other consequences of standardization are discussed below in the context of AAMVA's proposal for a "uniform" national driver's license.

[6] AAMVA Special Task Force on Identification Security Report to the AAMVA Board at 4 [Hereinafter "AAMVA Task Force Report"].

[7] The National Institute of Health reports 41,717 traffic fatalities in 1999. [http://www.niaaa.nih.gov/databases/crash01.txt].

include verifying employment status, opening bank accounts, and renting apartments. Since there are people who mistakenly rely on a driver's license to prove lawful status, and there are those who might seek to exploit this weakness, the appropriate solution is to change the driver license into a document that does, in fact, verify lawful presence. This is a dramatic and unwarranted expansion of function for a state *motor vehicle* department. Privacy and security interests are best protected by documents serving limited purposes and by relying on multiple and decentralized systems of identification in cases where there is a genuine need to establish identity. Centralizing authority over personal identity necessarily increases both the risk of ID theft as well as the scope of harm when ID theft occurs.

> ⇒ ***Privacy and security interests are best protected by documents serving limited purposes and by relying on multiple and decentralized systems of identification.***

---

*AAMVA(4) Implement processes to produce a uniform, secure, and interoperable driver's license/ID card to uniquely identify an individual.*

Strategy 4 is the core of AAMVA's driver license reform proposal, and contains several distinct elements that are yet to be adequately explored, developed, or discussed with the public. This strategy incorporates the following distinct ideas: uniformity (of both issuing standards and documents); security (of the identity of the applicant, and of the integrity of the document itself); interoperability (requiring uniformity, and mandating data sharing between states and with other parties); and a unique identifier.

**Uniformity**

AAMVA proposes that the issuing processes and requirements, as well as the information collected and maintained by the DMV, should be uniform across all states.

**Uniformity of Issuing Standards**

The AAMVA proposal relies upon the imposition of a national uniform standard for driver's license issuing processes.[8] AAMVA is also lobbying for Congress to delegate "the criteria and implementation of the uniform standard" to AAMVA itself.[9]

However, AAMVA have not demonstrated that uniformity is necessary to address any specified problem with the current system. They claim that "Unscrupulous individuals shop for the easiest and fastest way to get a license. They find the loopholes and they put you and me at risk."[10] There has been no substantiation from AAMVA of their claim that such "weak" licensing requirements have allowed dangerous individuals to obtain licenses, and no analysis of any security threat posed.

> ⇒ ***As yet, none of the parties involved in the proposal have announced what the new uniform processes should be.***

Further, if such a problem does exist, it can be addressed equally effectively, and without the disadvantages of a national ID system, by strengthening the issuance standards in those

---

[8] AAMVA Task Force Report at 2, Press Release, January 14, 2002, available at http://www.aamva.org/news/nwsPressReleaseAAMVAHelpsSecureSaferAmerica.asp

[9] Statement of Senator Durbin, Congressional Record -- Senate, S13776-13778, December 20 2001

[10] Press Release, January 14, 2002, available at http://www.aamva.org/news/nwsPressReleaseAAMVAHelpsSecureSaferAmerica.asp

states that are the "weakest links" in the system. In fact, in recent months several states have changed their application procedures to address perceived loopholes[11]. The proposal does not even demonstrate the advantages of a national uniform system over a national minimum standard, or of state-specific actions to close existing loopholes. Thus it is not narrowly tailored to the perceived problem and infringes on individual privacy for no justifiable ends.

As yet, none of the parties involved in the proposal have announced what the new uniform processes should be. It is therefore impossible to evaluate whether uniform standards would be effective in meeting perceived problems in the system, to what extent privacy interests would be compromised, and whether the proposal appropriately balances the interests of identification security and privacy.

AAMVA is not the appropriate body to be determining the balance between identification and privacy. AAMVA is a trade association that "represents the state and provincial officials in the United States and Canada who administer and enforce motor vehicle laws."[12] with a large industry advisory board including insurance, identification technology and information management companies.[13] The determination of uniform national standards and procedures is not appropriate for a bureaucracy with no direct accountability to the public, and a vested interest in the proposed system.[14] These decisions properly belongs to the state legislatures and the Congress, after a period of public debate and consultation.

**Uniformity of License Documents**

Just as there is no proven need for uniform application procedures and standards, there is no demonstrated need for uniformity of state driver's licenses. There are already mutual recognition programs and database pointer systems in place to address the needs AAMVA has identified. The primary reason for uniformity would be to enable information sharing with both government and private sector organizations as discussed below. In this context, uniformity intrinsically facilitates tracking, monitoring, profiling and other privacy invasive practices.

AAMVA's 90-day action plan includes efforts to "encourage voluntary short-term use of AAMVA standards in all jurisdictions," and "work with Congress to introduce DRIVerS legislation,"[15] before introducing model legislation in each AAMVA jurisdiction within one year.[16]

The adoption of the AAMVA standard by states would allow the use of driver's licenses as an identification and information gathering mechanism not only for government, law enforcement and security purposes, but also in the private sector. Products are already available that scan the AAMVA-compatible magnetic strip on a driver's license, and download 16 data fields captured on the license.[17] The information can then be compiled

[11] For example, Virginia no longer allows online renewal of driver's licenses, and has changed the identification documents required for a driver's license or identification card application: http://www.dmv.state.va.us/webdoc/citizen/drivers/applying.asp.

[12] AAMVA website http://www.aamva.org/about/

[13] AAMVA website http://www.aamva.org/links/mnu_lnkAssociateMembers.asp.

[14] AAMVAnet currently administers, and charges DMVs for access to driver and vehicle databases, and online verification networks: http://www.aamva.org/products/mnu_proAAMVANetApp.asp.

[15] AAMVA Task Force Report at 5.

[16] Id. at 3.

[17] The fields include: Last Name, First Name, Middle Name, Address1, Address2, City, State, Zip Code, Birthday, Drivers License Number, Drivers License

with data entered by the company, including a date/time stamp to track the individual's presence and information on their purchases. It may also be retained by the company, producing a database of detailed customer information that could not economically be compiled in the absence of such technology. These products are being marketed to companies that routinely check driver's licenses as identification or proof of age, including auto dealerships, clubs, bars, restaurants, and convenience stores. They are also suggested for use by health clubs and personal trainers "for use as a billing aid" and in the general retail market "to expedite adding customers to your monthly mailer."[18] AAMVA has also publicly stated that it seeks to share its model with retailers, car rental companies, insurers and banks.[19]

**Security**

AAMVA presents driver's license security as a single problem, but it can be distinguished into two different issues - document security and identification. EPIC supports the use of creative technology to improve document security if it is aimed at making it more difficult to counterfeit driver's licenses.[20] There is no demonstrated need, however, to establish uniform document security features across the 50 states. Each state DMV is capable of determining the needs of its customers and can incorporate features best situated to them.

Identity security concerns stem from the "one-driver, one-license, one-record" concept touted by AAMVA. In the AAMVA Special Task Force on Identification Security Report to the AAMVA Board, any pretense of a system concerned primarily with drivers is eliminated: the revised motto is "one card, one person, one record."[21] There are two main problems with such a concept. First, serving as the nation's main identity authenticators will distract a state DMV from its core function of licensing competent drivers and registering safe vehicles. Second, attempting and claiming to establish proof-positive identity is a very complex and error-prone task that creates more problems that it might solve.

Increasing reliance on the driver's license as an internal passport dramatically raises the incentives to forge or steal such credentials. If DMVs limited the use of the document for driver's licensing purposes the fraud incentives would drop significantly, particularly if the cost of fraud were raised by better document security features and stringent enforcement of identity theft laws.

> ⇒ ***As the importance of the card increases, the incentives to create fraudulent documents will also rise.***

Expiration Date, Sex, Height, Weight, Hair Color, Eye Color. See http://www.intellicheck.com/What_is_IDCheck.htm for the Intelli-Check IDCheck system, which operates not only on mag stripe cards but also 1D and 2D barcodes, and allows downloads for permanent archiving of customer identification and transaction information. See also http://www.dgahouston.com/dlsplit1.htm for product information on DLSPLIT "software to separate, format and display driver's license data," available online for US$169.60, including mag stripe reader.

[18] http://www.dgahouston.com/dlsplit1.htm for examples of "DLSPLIT Uses"

[19] "Task G: Promote the use of the Uniform Identification Practices model program developed by this Working Group to various potential customers, such as: all AAMVA jurisdictions; insurance companies, banks; travel industry; car rental agencies; retailers; others." AAMVA Uniform Identification Practices Working Group available at http://www.aamva.org/drivers/drvDL&CuniformIdentificationWG.asp

[20] Examples of such physical security features can be found listed in Appendix H of AAMVA's DL/ID Standard. Available at http://www.aamva.org/documents/stdAAMVADLIDStandrd0006630.pdf

[21] AAMVA Task Force Report at10.

DMVs must necessarily continue to rely on "breeder" documents such as birth certificates and Social Security card to establish identity. These documents are easily forged or obtained and are the main sources of identity fraud. There are currently 14,000 different versions of birth certificates in circulation.[22] A major source of fraudulent drivers licenses is DMV employees.[23] As the importance of the card increases, the incentives to create fraudulent documents will also rise. Moreover, the technology to uniquely identify individuals is untested for a large population, and previous applications of similar technology reveal significant technical error rates.[24] The enrollment process -- how we move from our current system to a unique identifier system -- will also present a number of difficult problems, including an anticipated rise in identity theft by criminals seeking to take advantage of the new procedures to establish "hardened" identities. The combination of technical concerns and prevalent American constitutional values protecting freedom of movement, privacy, and anonymity strongly suggests that any national identification scheme must be rejected.

**Interoperability**

For licenses to be "interoperable," they must be (a) in a compatible format across the nation, and (b) supported by a network allowing different parties to access the information linked to the individual license holder.

If AAMVA succeeded in making driver's licenses uniform across the nation (as discussed above), it would automatically satisfy the first criteria of interoperability: because there would be no relevant differences between licenses from Connecticut and Colorado, they would be interoperable.

> ⇒ ***The combination of cost, technical obstacles, and American constitutional values argue against a national identification system in the United States.***

To achieve functional interoperability, AAMVA plans to link information systems. This would enable a DMV or other authorized person to obtain the same information about a license holder regardless where the license was issued. It would also enable other entities, including government agencies and the private sector to access the information on the card. Both means of information sharing would compromise the privacy of driver's license holders.

**Information sharing between states**

There is already information sharing between states with regard to problem drivers in the Problem Driver Pointer System (POPS) and Commercial Drivers License System (CDLIS). There has been no demonstrated need to expand interstate information sharing beyond the existing capacity, which addresses the problems articulated thus far by AAMVA such as multiple licenses and avoidance of penalties. To the extent that AAMVA claims that PDPS does not capture problem drivers adequately, then that system should be improved, rather than creating a new system covering all drivers, including those with unblemished records.

[22] Birth Certificate Fraud (OEI-07-99-00570;9/00), September 2000, Office of Inspector General, Department of Health and Human Services, http://oig.hhs.gov/oei/reports/a492.pdf

[23] 127 California DMV employees were disciplined over the past 5 years for facilitating ID fraud. "Legislators Order DMV Audit", *Orange County Register*, February 27, 2001

[24] James L. Wayman, *Biometric Identification Standards Research, Final Report Volume I* (revision 2), San Jose State University, December, 1997 http://www.engr.sjsu.edu/biometrics/publications_fhwa.html

AAMVA's proposal for information sharing between states includes a complete feasibility study for photo exchange and specifications within 90 days.[25] But apparently regardless of the outcome of the study, AAMVA also plans to "obtain commitments for photo exchange as feasible" within the year, and begin to "implement standard image exchange" in 2003.[26]

AAMVA has set no limits on future information sharing between DMV administrators in different jurisdictions. It includes as stated goals to "coordinate effort to verify out-of-jurisdiction licenses electronically" and "continue efforts in North America *and internationally* regarding driver license/ID standards" (emphasis added).[27]

**Information sharing with other entities**

AAMVA has announced that it would like to link the state DMV databases with, and provide mutual access rights to, various government agencies, including SSA, INS, FBI, and some commercial organizations.

AAMVA wants its members in state DMV offices to have access to the records held by SSA, INS and Vital Statistics to assist in verifying the identity of license applicants.[28] Despite the history of abuse of personal information by DMV employees, and the privacy harm in releasing other government-held information for the unrelated purpose of driver's license ID verification, AAMVA has proposed no new safeguards to protect individuals' privacy under this practice. The AAMVA proposal to allow DMV employees to access information in state and federal agencies may require amendments to current law that protects the privacy of these records.

AAMVA has not specified the agencies that will be provided with access to driver's license information, or provided any suggested regulations to guard against a future expansion of its availability.

There is a long history of opposition by the DMVs themselves to increased information sharing, and an expansion of their information gathering function. One example of AAMVA's proposed information sharing schemes is to "improve social security number on-line verification" within one year. A similar proposal was widely rejected in 1998 under the NHTSA's Notice of Proposed Rulemaking Docket No. NHTSA-98-3945, pursuant to the (now repealed) §656(b) of the Immigration Reform Act of 1996. In a letter dated July 31 1998, opposing the NHTSA proposal, Betty Serian, Deputy Secretary of the Pennsylvania Department of Transportation, later Chair of the AAMVA Task Force on Identification Security, highlighted many of the concerns of states.[29]

Ms. Serian wrote that "the proposed requirement that states must, in all cases, verify social security numbers exceeds the statutory authority of the law" by "usurp[ing] each state's discretionary authority . . . creating a national driver's license." States require flexibility to determine what identification documents they find acceptable, based on their particular local or historical factors. Ms. Serian argued, "states

[25] AAMVA Task Force Report at 5.
[26] Id. at 3 and 5.
[27] Id. at 5.
[28] "AAMVA supports and encourages the access by its members (government entities) to other databases, such as SSA, INS and Vital Statistics to confirm identify, residency, citizenship and address verification" AAMVA Task Force Report at 8. They also plan to "improve jurisdiction access to SSA, INS and others" within a year (p. 5), "implement on-line address verification" after one year (p. 4), "continue to improve verification with the INS" within the year (p. 4)

[29] Letter on file with EPIC and available at http://www.epic.org/privacy/id_cards/penndot_letter_to_dot_ref.html.

must have the flexibility to provide for exceptions without draconian federal intervention."

Ms. Serian also cautioned of the administrative burden of the proposal, estimating that "the social security check will not match the SSA's records in approximately 20% of the cases because of the use of nicknames . . . unmarried names, data entry errors, etc. on the social security record." The SSA provides only a "Not Valid" message when the name and number do not match, forcing DMV administrators to interact with customers repeatedly. Additionally, the burden required to change data formats to achieve uniformity would be untenable. Ms. Serian stated that adding a full middle name to driver license records "would require 28 data entry clerks four years to complete the conversion" just for Pennsylvania's records. Ms. Serian concluded that the requirements were "very costly, ineffective, and customer hostile, once again adopting a theoretical approach while ignoring basic service needs of law abiding customers… Government at the state level . . . would be harmed." The additional burden in the AAMVA proposal of extra fields, including complex encoded biometric data, and altered formats to accommodate information sharing would constitute an unjustified and extravagant burden on state DMVs.

**Existing Legislative Limitations on Information Sharing**

Existing legislation limits the ability of DMVs and other agencies to share information. AAMVA's proposal would require substantial amendment to these laws, removing significant privacy protections that have been in place for many years.

The **Driver's Privacy Protection Act** presently contains no provisions governing the use of biometric identifiers. Before a system such as that proposed by AAMVA could come into effect, an amendment would be required incorporating biometric identifiers into the definition of "personal information" in 18 USC 2725(3),[30] and providing greater protection for the privacy of such information.

Biometric identifiers should also be incorporated in the definition of "highly restricted personal information," as defined in section 2725(4). This category currently includes "an individual's photograph or image, social security number, medical or disability information."

The prohibition on the use and disclosure of personal information in section 2721 is subject to many exceptions. The initial portion of sub-section 2721(b) requires that personal information (including highly restricted personal information) shall be disclosed in connection with the administration of a wide variety of motor vehicle related laws,[31] including

[30] 18 USC 2725(3) currently provides that "personal information" means information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and the driver's status.

[31] 18 USC §2721(b): "Personal information referred to in subsection (a) shall be disclosed for use in connection with matters of motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle product alterations, recalls, or advisories, performance monitoring of motor vehicles and dealers by motor vehicle manufacturers, and removal of non-owner records from the original owner records of motor vehicle manufacturers to carry out the purposes of titles I and IV of the Anti Car Theft Act of 1992, the Automobile Information Disclosure Act (15 USC 1231 et seq.), the Clean Air Act (42 USC 7401 et seq.), and chapters 301, 305, and 321-331 of title 49 [49 USC §§30101 et seq., 30501 et seq., 32101-33101 et seq."

environmental standards and investigation by motor vehicle manufacturers.

The prohibition on information sharing is also subject to the "permissible uses" listed in sub-section 2721(b). The permissible uses of highly restricted personal information are a subcategory of these uses, and comprise:

> (1) For use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions.
>
> (4) For use in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court.
>
> (6) For use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities, rating or underwriting.
>
> (9) For use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under chapter 313 of title 49 [49 USCS §§ 31301 et seq.].

Highly restricted personal information may be disclosed to any party for any with the express consent of the person to whom the information applies.[32]

There are several currently permitted uses of highly restricted personal information which would constitute further privacy violations if a biometric identifier was included on the driver's license and in the information collected by the DMVs.

The required disclosure of biometric identifiers in connection with motor vehicle laws under sub-section 2721(b) allows access to personal information by a wide variety of organizations for many purposes, where there is no demonstrated need to use such information.

The exceptions under sub-section 2721(b)(1) for sharing information with other government agencies could allow AAMVA to go even further. The provision is not limited to the SSA, INS, FBI or other agencies concerned with national security, but extends to any function of any government agency, including State and local governments and those acting on their behalf. DMV administrators thus already have the authority to share information (including biometric identifiers), and thus make provision of a driver's license a prerequisite of any interaction with government agencies.

The sensitivity of biometric information, and its use by motor vehicle administrators, was not considered by Congress at the time the Driver's Privacy Protection Act was passed in 1994.[33] The Act would require substantial amendment to take account of changes in technology, and to protect the privacy interests of driver's license holders.

[32] 18 USC §2721(a)(2).

[33] See also the discussion of biometric unique identifiers below.

There is as yet no proposal for auditing requests for access made to the DMV, or any avenue for appeal or review of decisions to grant disclosure based on the factors in the DPPA. AAMVA's proposal should include a provision requiring all DMVs to keep a record of all disclosures of personal information, and make those requests accessible to the individual to whom the information pertains.[34] If the Canadian members of AAMVA decide to join the scheme, amendments would likely be required to Canadian Provincial privacy laws, which are generally more stringent than either state or federal regulation in the United States.

**Technological feasibility of information sharing**

Creating a national database on 228 million Americans creates myriad problems[35]. Such a database would probably use a pointer or index system to link distinct state databases -- this is precisely how most large databases are constructed. The key issue is determining the data elements that would be used to create the index. AAMVA is lobbying for the use of the Social Security number along with name and date of birth to link the records. This is in spite of the fact that §656(b) of the Immigration Reform Act of 1996, which would have mandated the display of SSNs on state driver's license, was repealed because it would have facilitated precisely the sort of information sharing AAMVA is currently contemplating.[36]

Aside from the important policy arguments against creating such a database, these databases are notoriously mistake-prone, difficult to secure, open to abuse, and expensive to compile and operate. Reconciling different databases such as those of the Social Security Administration is expected to generate 20% error rates.[37] Linking with INS and FBI databases will likely present similar issues.

> ⇒ ***The difficulty in fixing a credit report might prove trivial in comparison to correcting one's record in the national database.***

Actually connecting the different databases is also a significant problem -- the FBI and INS have been trying to link their databases for over a decade. Moreover, large databases do not present any solution to the problem of bad data: once in a database of any sort, data -- errors and all -- tend to be authoritative, pervasive and persistent. A U.S. PIRG study found 30% of credit reports contain serious errors and 70% contain some errors.[38] The difficulty in fixing a credit report might prove trivial in comparison to correcting one's record in the national database. Instead of solving public safety problems, the government will create a bureaucratic headache that will take resources away from performing the functions that specific agencies are meant to

[34] Such a requirement exists in many state jurisdictions, often with an exception that the request information need not be provided where it relates to an ongoing criminal investigation of the person to whom the information pertains and the release would prejudice the investigation.

[35] AAMVA states that 228 million US and Canadian citizens have either a driver's license or a DMV issued identity card, representing 75 percent of the total population: AAMVA Task Force Report at 8.

[36] Report to Congress, Evaluation of Driver Licensing Information Programs and Assessment of Technologies, National Highway Traffic Safety Administration, Federal Motor Carrier Safety Administration and AAMVA, July 2001,, section 3.4.4 p. 41

[37] See Letter from Betty Serian, Deputy Secretary, Pennsylvania Department of Transportation to NHTSA, July 31, 1998 http://www.epic.org/privacy/id_cards/penndot_letter_to_dot_ref.html. See also the problems faced in California last year when the DMV began to verify social security numbers. "Glitch in DMV crackdown leaves some drivers unable to renew licenses", San Jose Mercury News, June 23, 2001

[38] Available at http://www.pirg.org/reports/consumer/mistakes/

carry out. State DMVs already operate with over-stretched resources and there is no reason why they ought to take on the burden of administering a national database.

**Unique Identifier**

> ⇒ ***The very attraction of biometrics for identification purposes is intrinsically linked to the infringement of individual privacy.***

AAMVA has not determined the mechanism will be used to uniquely identify individual license holders, although it has acknowledged that it contemplates the use of biometric technology. [To uniquely identify an individual, an identifier must be verifiable against the person's actual identity, that is, their permanent physical characteristics. Any alphanumeric identifier can only be verified by the possession of corresponding documents; a biometric can be used to verify the information held by the agency or on a card by reference to the actual physical characteristic it refers to. Thus it appears that AAMVA intends to implement some kind of biometric identifier.]

The very attraction of biometrics for identification purposes is intrinsically linked to the infringement of individual privacy. Whereas a license number or a PIN number can be randomly assigned, and is not in itself personally identifiable information, a biometric is inextricably linked to the particular individual it codes for. A recent opinion of the Eastern District of Pennsylvania noted that analysis of fingerprints may yield other personal information, such as the individual's environmental conditions, disease history and genetics.[39]

Notwithstanding the close link between biometrics and identity, biometrics are not fraud-proof. For example, licenses may currently be fraudulently obtained with mismatched details, such as the name, address, SSN and date of birth of one person and the photograph of another person who holds the card and may impersonate the named person. The photograph is a biometric, although not usually a digitized biometric such as AAMVA proposes, and it can be falsified. Other biometrics, such as fingerprints and retinal scans, may thus also be fraudulently placed on licenses. Their inclusion would make it extremely difficult for victims of identity theft to prove their identity, once a biometric other than theirs is associated with their driver's license.

> ⇒ ***Biometric technology is not yet sufficiently advanced to accurately identify all members of the large population of licensed drivers.***

To remedy the fact that biometric identifiers can be compromised in much the same way as the Social Security number or a photograph. AAMVA is contemplating the inclusion of multiple biometric identifiers on the license. Of course, this proposal does not make the license fraud-proof, nor change the nature of biometrics. Instead it compromises privacy and further hampers victims of identity theft with no commensurate security benefits.

Finally, biometric technology is not yet sufficiently advanced to accurately identify all members of the large population of licensed drivers. Even fingerprinting, a common technique used in law enforcement, has not been subjected to such large-scale use and there are important limitations emerging about the

[39] *USA v Llera Plaza et al*, Nos. CR 98-362-10 to 98-362-12, at 2 (E.D.P.A. filed Jan. 7, 2002) [http://www.paed.uscourts.gov/documents/opinions/02D0046P.HTM].

reliance on the technique.[40] Automated fingerprint examination is not foolproof -- a 3% error rate (a conservative guess assuming the technology and databases are used following precise directions) will mean that over 6 million Americans might be incorrectly identified in the database.[41]

For these reasons, EPIC opposes the inclusion of biometric identifiers on driver's licenses and identification cards.

---

*AAMVA(5) Establish methods for the prevention and detection of fraud and for auditing of the driver's license/ID processes.*

*AAMVA(6) Ensure greater enforcement priority and enhanced penalties for credential fraud.*

EPIC supports internal reform at the DMVs to remedy their record of fraud and abuse of personal information. The Driver's Privacy Protection Act provides that violations of its provisions may be addressed by individual criminal fines, per diem penalties against the DMV, and civil actions resulting in actual damages of not less than $2,500, punitive damages and costs.[42]

AAMVA have not demonstrated a need for additional laws or penalties regarding driver license fraud and unauthorized use of data. The existing laws provide strict penalties and prohibitions but AAMVA's member jurisdictions have failed to implement successful investigation and enforcement strategies. In a previous effort to combat terrorism through reducing ID fraud, the specially formulated Federal Advisory Committee on False Identification rejected the idea of a unique identifier and instead recommended better enforcement and higher penalties. These recommendations were codified in 18 USC §1028. The Internet False Identification Prevention Act of 2000 amended §1028 to address changes in technology. That Act also established a multi-agency Coordinating Committee on False Identification, which is due to report on the efficacy of current ID fraud laws in March 2002 and again in March 2003.

---

*AAMVA(7) Seek U.S. federal and other national requirements for legislation, rule making and funding in support of AAMVA's identification and security strategies.*

AAMVA proposes to "seek mandatory US federal and Canadian legislation to impose and fund national and uniform driver license/ID standards."[43] AAMVA states that such legislation would be required before any significant progress is made on its strategy. While legislative support is needed for certain key elements in the strategy, state DMVs can still move ahead on other parts without Congressional mandate. For instance, AAMVA is encouraging the voluntary use of its DL/ID standard, which facilitates information sharing among the states, enforcement authorities, and private industry.[44] AAMVA is also encouraging states to adopt uniform citizenship and residency standards as well as Social Security number verification. The problem for AAMVA is that as long as all states are not on board, the system continues to be limited. Its proposed national strategy is a way of compelling states to adopt uniform standards.

---

[40] Pankanti et al., *On the Individuality of Fingerprints* (Michigan State University 2001) http://biometrics.cse.msu.edu/cvpr230.pdf.

[41] James L. Wayman, *Biometric Identification Standards Research, Final Report Volume I* (San Jose State University December, 1997).

[42] 18 USC sects. 2721, 2723(a), 2723(b).

[43] AAMVA Task Force Report at 6.

[44] See http://www.intellicheck.com/Jurisdictions.htm for the states that have machine-readable licenses.

AAMVA must also make transparent the detailed financial structure of its program. It has asked the federal government for $100 million, however, a report from last July to Congress in which AAMVA was a co-author stated that $24 to $35 million would be required to implement an Integrated Driver License Identification System (IDLIS), with an annual operating cost of $17-$21 million.[45] The report notes that there are "substantial costs involved in developing and converting to a system encompassing all drivers" but that "once such a system would be operational, states could recover costs of operating by assessing driver license fees and related fees."[46]

---

*AAMVA(8) Establish public and stakeholder awareness and support*

It is clear that such a wide-ranging proposal requires public debate and thorough scrutiny. AAMVA's legislative schedule, as currently formulated, does not accommodate the time that would be needed for Americans to examine the appropriateness of introducing a national ID system through the state DMVs. Moreover, the technical and procedural consequences if such a scheme is implemented have not been adequately explored. At the very least, there must be a full assessment of the risks and consequences of a system of national identification in the United States. Appropriate legal and technical safeguards should be established before should a project goes forward.

[45] Report to Congress, Evaluation of Driver Licensing Information Programs and Assessment of Technologies, National Highway Traffic Safety Administration, Federal Motor Carrier Safety Administration and AAMVA, July 2001, Section 3.6 at 43

[46] Id. at 3

⇒ ***There must be a full assessment of the risks and consequences of a system of national identification in the United States. Appropriate legal and technical safeguards should be established before should a project goes forward.***

**UNEXPECTED RESULTS**

AAMVA states that it expects it national ID strategy to result in a safer America through:

a) increased security,
b) increased highway safety,
c) reduced fraud and system abuse,
d) increased efficiency and effectiveness,
e) uniformity of processes and practices.

AAMVA's scheme in fact diverts resources away from current priorities and fails to resolve any of the perceived problems. Each of its expected results is briefly refuted below:

⇒ ***A national ID would create a false sense of security because it would enable individuals with an ID -- who may in fact be terrorists -- to avoid heightened security measures.***

*Increased Security*

An identity card is only as good as the information that establishes identity in the first place. Terrorists and criminals will continue to be able to obtain -- by legal and illegal means -- the documents needed to obtain a government ID, such as birth certificates and social security numbers. A national ID would create a false sense of security because it would enable individuals with an ID -- who may in fact pose security threats -- to avoid heightened security measures.

A national ID program should be evaluated in the same way we might evaluate other security countermeasures. First, what problem are IDs

trying to solve? Second, how can an ID system fail to achieve its goals in practice? Third, given the failures and the loopholes in the system, how well do IDs solve the security problem? Fourth, what are the costs associated with IDs? And finally, given the effectiveness and costs, are IDs worth it?

*Increased Highway Safety*
Information on problem drivers is already shared between states under the Problem Driver Pointer System, administered by AAMVA. Any deficiencies in this system can be remedied by amending its scope and operation: a new system for law-abiding motorists is unnecessary. Establishing uniform residency and citizenship standards and cross-checking applications with criminal records would discourage many people from getting licenses and therefore increase the number of untrained and unlicensed drivers on the roads.

> ⇒ ***Ordinary citizens will get caught in the cracks of the new bureaucratic machinery and will have a more difficult task in remedying identity fraud and protecting privacy.***

*Reduced Fraud & System Abuse / Increased Efficiency & Effectiveness*
If the driver license acquires more importance in society as a "gateway" or internal passport document, the incentives for fraud will greatly increase. The unprecedented infrastructure required for creating a national ID scheme would make it difficult to differentiate abuses from technical errors and glitches. Ordinary citizens will get caught in the cracks of the new bureaucratic machinery and will have a more difficult task in remedying identity fraud and protecting privacy. The error rates alone will reduce system-wide efficiency and make the process of obtaining a driver's license a nightmare. There is no precedent for such a large database being effectively compiled and securely managed. If prior experience is any guide, the technological, privacy and security problems will be formidable.

*Uniformity in Processes & Practices*
There is no reason to impose uniform processes and practices, and override each state's right to develop its own practices. It will take significant resources to ensure that processes and practices are truly uniform across the country. California, for instance has been collecting fingerprints for over 20 years but most of the 60 million prints in its database are useless because of poor operating practices in collecting the data. [47] Such errors will only be magnified in a national program. Finally, AAMVA does not demonstrate how "uniformity in process and practices" is either necessary or effective in creating a "safer America."

> ⇒ ***There are several less expensive, less invasive and better-crafted alternatives***

**Alternatives**

There are several less expensive, less invasive and better-crafted alternatives which would not lead to the creation of a national ID card yet would address AAMVA's perceived problems of poor document security. For instance, AAMVA might develop training programs to improve the ability of DMV staff to detect fraudulent documents. Technology can be used creatively to enhance document security using features such as holograms and ultra fine lines. AAMVA can also help develop model audit and verification systems that states can choose to implement if they feel their procedures are inadequate.

[47] "Failure to finger fraud: DMV's thumbprint database is insufficient -- and costly to fix." Orange County Register, December 31, 2000

**Recommendations**

AAMVA's proposal to implement a national ID scheme through the driver's license system is a backward step for individual privacy with no substantial countervailing safety or security benefits. At present, the case against adoption of a national ID card in the United States is compelling.

- Efforts to detect and prevent fraud occurring within DMVs, or with the assistance of DMVs and their employees, should be pursued.

- Improved document security measures to prevent counterfeiting and tampering are overdue and should be pursued, but measures that enable profiling and tracking of licensed drivers in the United States raise far-reaching policy concerns.

- AAMVA's move to standardize driver's licenses nationally, to collect more and more invasive personal information, and to expand the information sharing capacity of DMVs raises substantial privacy concerns that have not been adequately addressed

- AAMVA's proposal has all the elements and problems of a National ID Card. Although the card would not be mandated by federal law or issued by a federal agency, in many respects it reaches further than a simple ID card and might be better understood as the creation of a National Identification System. AAMVA recognizes this, citing as a "major implication" of their proposal that "the continued evolution and improvements of the driver license/ID card precludes the need for a new, separate national identification card."[48]

- AAMVA's proposal significantly changes the purpose of the driver's license: to certify that an individual is competent to drive a motor vehicle. In diluting this central function, the AAMVA proposal may reduce public safety.

- The increasing reliance on a single centralized form of identification makes ID theft simpler, and more difficult for victims to remedy.

- AAMVA must define the scope of proper access to and use of personal information, consider mechanisms to prevent internal breaches or misuse by third parties, and provide a means to correct abuses when they inevitably occur, before its proposal can be thoroughly analyzed.

- There must be wider public debate about the details and the consequences of AAMVA's national identification card and driver's license system. This proposal is moving too quickly, with too little consideration of the long-term impact on privacy and the risk of new forms of identity theft and fraud.

**CONCLUSION**

The combination of technical concerns and prevalent American constitutional values protecting freedom of movement, privacy, and anonymity strongly suggests that any national identification scheme must be rejected.

**REFERENCES**

AAMVA website: http://www.aamva.org

AAMVA Driver's License / Identification Card Standard
http://www.aamva.org/standards/stdAAMVADLIdStandard2000.asp (summary)

[48] AAMVA Task Force Report at10.

http://www.aamva.org/Documents/stdAAMVADLIDStandrd000630.pdf (full report)

AAMVA Executive Committee Resolution establishing the Special Task Force on Identification Security
http://www.aamva.org/Documents/hmExecResolution.pdf

AAMVA Special Task Force on Identification Security information
http://www.aamva.org/drivers/drvIDSecurityindex.asp

AAMVA Special Task Force on Identification Security Report to the AAMVA Board, Executive Summary
http://www.aamva.org/drivers/drvIDSecurityExecutiveSummary.asp. (Full report on file with EPIC).

Commercial Applications of AAMVA Standard Driver's Licenses:
http://www.dgahouston.com/dlsplit1.htm
http://www.intellicheck.com/

Driver's Privacy Protection Act 18 USC §2721 et seq.

Statement of Senator Richard Durbin, Congressional Record -- Senate, S13776-13778, December 20 2001

Letter from Betty Serian, Deputy Secretary, Pennsylvania Department of Transportation to NHTSA dated July 31 1998
http://www.epic.org/privacy/id_cards/penndot_letter_to_dot_ref.html

*USA v Llera Plaza et al*, Nos. CR 98-362-10 to 98-362-12 (E.D.P.A. filed Jan. 7, 2002) (motion to preclude the US from introducing latent fingerprint identification evidence)
http://www.paed.uscourts.gov/documents/opinions/02D0046P.HTM

*Condon v. Reno,* 528 U.S. 141 (2000).
http://supct.law.cornell.edu/supct/html/98-1464.ZO.html

*Carey v. Nevada Gaming Control Board*, No. 00-16649 (9th Cir. 2002)
http://caselaw.lp.findlaw.com/data2/circs/9th/0016649p.pdf.

**Reports**

James L. Wayman, *Biometric Identification Standards Research, Final Report Volume* I, San Jose State University December, 1997
http://www.engr.sjsu.edu/biometrics/publicatios_fhwa.html

Office of Inspector General, Department of Health and Human Services. *Birth Certificate Fraud,* September 2000
http://oig.hhs.gov/oei/reports/a492.pdf

John J. Miller and Stephen Moore, *A National Id System: Big Brother's Solution to Illegal Immigration*, September 7, 1995
http://www.cato.org/pubs/pas/pa237es.html

Sharath Pankanti, Salil Prabhakar & Anil K. Jain, *On the Individuality of Fingerprints,* Michigan State University, 2001
http://biometrics.cse.msu.edu/cvpr230.pdf

Public Interest Research Group (PIRG), *Mistakes Do Happen: Credit Report Errors Mean Consumers Lose,* March 1998
http://www.pirg.org/reports/consumer/mistakes/

National Highway Traffic Safety Administration, Federal Motor Carrier Safety Administration and AAMVA, *Report to Congress, Evaluation of Driver Licensing Information Programs and Assessment of Technologies,* July 2001

http://www.aamva.org/Documents/Library/libNHTSAReportToCongress.pdf

Robert Ellis Smith, *A National ID Card: A License to Live, Privacy Journal*, December 2000.

Shane Ham and Robert D. Atkinson, *Modernizing the State Identification System: An Action Agenda*, February 2, 2002 http://www.ppionline.org/documents/Smart_Ids_Feb_02.pdf

Charlotte Twight, *Why Not Implant a Microchip?*, February 7, 2002 http://www.cato.org/dailys/02-07-02.html

Adam Thierer, *National ID Cards: New Technologies, Same Bad Idea*, TechKnowledge No. 21, September 28, 2001 http://www.cato.org/tech/tk/010928-tk.html

Lucas Mast, *Biometrics: Hold On, Chicken Little*, TechKnowledge No. 31, January 18, 2002 http://www.cato.org/tech/tk/020118-tk.html

Simon G. Davies, "Touching Big Brother: How biometric technology will fuse flesh and machine," *Information Technology & People*, Vol 7, No. 4 1994. http://www.privacy.org/pi/reports/biometric.htl

EPIC ID Card Resource Page http://www.epic.org/privacy/id_cards/

**ABOUT EPIC**

The Electronic Privacy Information Center is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, freedom of expression and constitutional values in the information age. EPIC pursues a wide range of activities, including policy research, public education, conferences, litigation, publications, and advocacy. The Watching the Watchers Project was undertaken by EPIC in 2001 to assess the impact of proposals for public surveillance put forward after September 11.