CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Keeping the Internet Open, Innovative and Free

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

September 22, 2008

To: AAMVA REAL ID Verifications Systems Working Group
Re: State-to-State Verification System Alternatives
Via: state2stateREALIDstudy@AAMVA.org

CDT appreciates the opportunity to submit these brief comments on the various architectural alternatives for the system that will enable states, pursuant to the REAL ID Act, to ensure that a driver's license (or ID card) applicant is not already licensed in another jurisdiction. While CDT has consistently questioned the wisdom of the REAL ID Act and supports its repeal or significant amendment, we recognize that it is important to make wise implementation decisions should the law stand.

Thus we write to encourage the states to create a **fully distributed system that avoids the privacy and security risks associated with a state-to-state verification system that relies on a central database of personal information.** CDT is pleased that AAMVA recognizes that different architectural options have different implications, especially with regard to personal privacy. We look forward to reviewing the white paper that objectively analyzes the various architectural alternatives for the state-to-state verification system. CDT makes the following six points:

1. States Should Not Expand CDLIS or Otherwise Develop a Verification System that Centrally Stores Personal Information

CDT has consistently argued against expanding CDLIS to include all drivers and ID card holders, or otherwise developing a centralized identification system that stores highly sensitive personal information on virtually all Americans. **While we appreciate the desire to combine the CDLIS modernization and REAL ID directives into one initiative in order to be more efficient, we strongly suggest moving each forward on their own timeframe in light of the significant privacy and security risks.**

A central database that stores personal information such as name, Social Security Number, date of birth, and physical characteristics on hundreds of millions of Americans would become a treasure trove of extremely valuable data for identity thieves, terrorists and other determined hackers. A central ID database would also increase the temptation for internal abuse by unscrupulous government employees, which is a leading cause of driver's license fraud and identity theft. It is not clear that the risk of unauthorized access to personal information by both external and internal actors would be greatly reduced by developing a "reduced pointer file" where some smaller amount of personal information is stored centrally, or where personal information is "un-correlated" (e.g., Social Security Number and state of record are in one database, and state of record, name and date of birth are in another database).

Most importantly, building a centralized system – whether fully centralized or where the central record "points" to additional information in state motor vehicle databases (e.g., driving histories) as CDLIS does – would also set the stage for future "mission creep." The temptation would be too great to further develop a nation-wide identification system that could be used by the government and others to track people for purposes other than administering driver's licenses, to download or mine the entire database, and to link new state and federal databases to the central record. Not only will such mission creep be unavoidable – it will create the very "national ID" system the public fears.

Moreover, it is not clear that federal privacy laws such as the Privacy Act and the Driver's Privacy Protection Act, or even state privacy laws, would provide adequate protection of personal information stored in a central database managed by a private entity like AAMVA. In short, no robust legal framework exists to protect the personal information that would be held in a centralized ID system from misuse by government agencies and employees, businesses and others.

CDT urges the states and AAMVA *not* to design a system that can be easily expanded and abused in the future. Rather, a state-to-state verification system should be designed that gets the "one REAL ID card per person" job done without putting the security of the system and Americans' privacy at grave risk – now or in the future.

2. States Should Develop a Fully Distributed Verification System ("Multi-Search")

As we suggested to the Department of Homeland Security in response to the proposed REAL ID regulations,[1] states should develop a fully distributed system that enables each state to directly communicate with all other states to check whether a driver's license applicant is already licensed in another jurisdiction, thereby ensuring "one REAL ID card per person." (The Working Group is calling this the "Multi-Search" alternative.) A classic distributed system – where relevant personal information is securely stored in disparate locations (i.e., state motor vehicle databases) – can be built by using a common protocol for formatting data and sending and receiving messages (i.e., requests and responses).

CDT has advocated for this design alternative because it avoids storing highly sensitive personal information on virtually all Americans in a central database not clearly protected by

[1] See CDT's comments to DHS on the proposed REAL ID regulations (May 8, 2007), pages 11-12, http://www.cdt.org/security/20070508realid-comments.pdf.

federal and state privacy laws, which is incredibly risky as discussed above. The Working Group noted that privacy risks are also associated with the distributed model because 55 copies of personal information would be sent out each time a "state of inquiry" processed a new driver's license applicant, rather than the one copy that would be sent out using the CDLIS model.

Although we recognize that privacy risks are associated with a distributed system, we believe that they are much less significant than the privacy risks associated with a centralized system. Moreover, we believe that encrypting the state-to-state communications and having receiving states delete personal data immediately after they do the "look up" can mitigate such risks. (We understand that the CDLIS system currently is not encrypted – which raises serious concerns – but that encryption of both static and dynamic personal information is part of the CDLIS modernization plan.)

Additionally, CDT is in favor of a distributed model for the state-to-state verification system because the Driver's Privacy Protection Act (although it should be strengthened) would clearly apply to citizen's personal information stored in state motor vehicle databases, as would state privacy laws.

Finally, CDT understands that some feasibility concerns have been expressed about a distributed system – specifically, whether states (and small states in particular) would be able to handle the high query volume. As we suggested to DHS,[2] a detailed analysis evaluating what would be needed to scale up state systems to handle the traffic generated by a distributed state-to-state verification system should be conducted; specifically, what are the performance objectives and requirements of such a system, where are state systems today, and what would be needed (and how much would it cost) to upgrade state systems to meet the performance objectives and requirements of the distributed system? The bottom line is that this can be done; the deciding factor is whether the states and AAMVA have the will to make it happen.[3]

3. The "Enhanced Multi-Search" System Should Not Record Transactional Data

The Working Group presented a slight variation on the fully distributed system whereby AAMVAnet's Central Site would coordinate the queries and responses between the "state of inquiry" and the other 55 jurisdictions. (The Working Group is calling this the "Enhanced Multi-Search" alternative). CDT believes that this alternative is preferable to the other centralized, CDLIS-based models for the reasons stated above.

However, privacy concerns would exist if the Central Site recorded transactional data that included personal information or could otherwise be tied to an individual (e.g., "on this date and

[2] See CDT's analysis of the final REAL ID regulations (Feb. 1, 2008), pages 4-6, http://www.cdt.org/security/identity/20080201_REAL ID_hillbrief.pdf.

[3] A minor suggestion regarding query volume: The move toward central issuance of driver's licenses and ID cards – where the cards are made at a central location and not in DMV branch offices – means that the issuance of driver's licenses and ID cards can take several days. States could take advantage of this time delay and stagger their queries so as to not overload the systems of smaller states that are part of the distributed system.

at this time, this state issued an inquiry on this applicant with this identifying information"). If this sort of data is collected and stored by the central database, it could also be subject to unplanned secondary uses, which would be problematic even if the central database did not contain a comprehensive central record. CDT urges AAMVA to clarify the specific role of the Central Site in the "Enhanced Multi-Search" alternative.

4. AAMVA Should Consider a Centralized Hash Index

One alternative for the state-to-state verification system that AAMVA apparently has not considered is a centralized hash index. Although *CDT strongly advocates for the Multi-Search (or at least Enhanced Multi-Search) alternative*, if the states strongly feel that a centralized system of some sort would be preferable to sending out 55 individual inquiries, a centralized hash index might be a feasible alternative.

The Central Site could store a "hash index" rather than personal information in clear text. The personal information of REAL ID cardholders would be encoded using a one-way cryptographic "hash" function that produces a short representation of the information. It is easy to compute the hash value from the personal information, but it is difficult to reverse the process from the hash value back to the information. When an applicant applies for a REAL ID card in a new jurisdiction, that jurisdiction would check if the hash value of the applicant's personal information exists in the central hash index.

A match would indicate that the applicant is not eligible for a new REAL ID card until he or she terminates the old one. The hash index would ensure that the centralized data is meaningless if accessed without authorization. However, CDT strongly recommends that if a hash index is used as the anchor for a national state-to-state verification system, policies must be in place to prohibit the use of the hash value as a national identification number.

5. AAMVA Should Clarify How the Fair Information Principles (FIPs) Will Inform the Privacy Ranking for Each System Alternative

The Working Group explained that each state-to-state verification system alternative will be evaluated using a set of seven top-level criteria, including privacy and security. Each of these criteria will be ranked using certain standards selected for each criterion; for example, it was explained that the Fair information Principles (FIPs) will be used to determine whether each system alternative poses low, reasonable, moderate or significant risks to personal privacy. CDT notes that there is no widely accepted single articulation of the FIPs. However, the Organization for Economic Cooperation and Development (OECD) developed a set of principles for the protection of personal data[4] that has inspired other permutations of the FIPs, such as those outlined by the Department of Homeland Security's Privacy Office.[5]

[4] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

[5] See, e.g., the Privacy Impact Assessment for the proposed REAL ID regulations (March 1, 2007): http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_realid.pdf.

We suggest that the Working Group clarify how these privacy principles will accurately distinguish the privacy risks of a centralized system from those of a distributed system. Principles such as Transparency, Individual Access, Correction & Redress, and Data Quality & Integrity are virtually meaningless for this kind of evaluation. A CDLIS-based verification system can meet other privacy principles such as Purpose Specification and Use & Disclosure Limitation, and include technological security safeguards and accountability and auditing mechanisms, but still pose grave risks to personal privacy as compared to a distributed system.

Perhaps the Data Minimization principle will be the most useful FIP for purposes of giving each system alternative a privacy ranking. For example, a distributed system has low associated privacy risks because it epitomizes data minimization: no personal data is stored centrally; whereas a centralized model has high associated privacy risks because a significant amount of highly sensitive personal information is stored centrally (even if a "Reduced Pointer File" is used). CDT urges AAMVA to clearly and specifically articulate the basis for each privacy ranking.

6. AAMVA Should Clarify How Each System Alternative Will be Ranked Overall to Enable Transparent Recommendations of Preferred System Alternatives

The Working Group explained that the goal of the white paper, which will detail the various architectural alternatives for the state-to-state verification system, will be to offer recommendations to the decision-makers (presumably state DMV directors, AAMVA as a whole and DHS). However, in order to make recommendations – such as, "Alternative A is preferable to Alternative B" – the system alternatives must be holistically ranked. This means that each criterion (and its corresponding ranking) must be given a certain weight that informs the overall ranking of a given alternative.

The Working Group did not explain how the seven top-level criteria will be collectively considered for each system alternative, how each system alternative will be assigned an overall ranking, and therefore how recommendations will be made regarding preferred system models. CDT is concerned that the privacy criterion will not be given adequate weight when the Working Group makes its recommendations. If a given system alternative ranks low on privacy but high on the other six criteria, what overall assessment will be given to the alternative? In other words, how will each criterion inform the *overall ranking* of the particular alternative? In our view, even if a system has high or positive scores for cost (i.e., low), adaptability (i.e., easy) and time to implement (i.e., fast), for example, if it scores badly on privacy (i.e., high risk), it should not be implemented.

CDT urges AAMVA to clearly and specifically articulate how overall recommendations will be made (i.e., how each system alternative will be ranked overall), and to give the privacy and security criteria adequate weight when making recommendations regarding whether certain alternatives are more preferable than others.

For further information, please contact:

Sophia Cope
Staff Attorney/Ron Plesser Fellow
scope@cdt.org
202-637-9800 x104