CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Working for Civil Liberties on the Internet

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

DEPARTMENT OF HOMELAND SECURITY
DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE
March 21, 2007
[Docket No. DHS-2007-0008]

Written Testimony of Sophia Cope
Staff Attorney/Ron Plesser Fellow
Center for Democracy & Technology

REAL ID Act

Thank you for inviting CDT to speak on the REAL ID Act and the Department of Homeland Security's proposed implementing regulations.

I. SUMMARY

A. THE REAL ID ACT IS FUNDAMENTALLY FLAWED

CDT supports the goal of making driver's license and ID card issuance more secure and thereby making the cards more reliable identity credentials. However, DHS's proposed regulations confirm our fears that the REAL ID Act is fundamentally flawed. Both the Act itself and the proposed implementing regulations fail to protect privacy while creating serious security gaps.

CDT urges this Committee to recommend to the Secretary that he ask Congress to adopt a statutory framework for driver's license and ID card issuance that expressly protects privacy and security. Congress must repeal or substantially rewrite the Act if driver's license and ID card reform is to be effective. The privacy and security shortfalls found in the proposed regulations stem directly from those in the Act itself: the statutory language provides no guidance on privacy and little guidance on security. DHS states in the Preamble to the draft regulations that it has addressed privacy "within the limits of its authority under the Act."[1] The Department explains that the REAL ID Act "does not include statutory language authorizing DHS to prescribe privacy requirements," which "is in sharp contrast with the express

[1] Notice of Proposed Rulemaking (NPRM), Preamble at 10824-25.

authorization provided in section 7212 of IRTPA [Intelligence Reform and Terrorism Prevention Act of 2004], which was the prior state licensing provision repealed by the REAL ID Act."[2] Given these limitations of the Act, the Secretary should request from Congress the power to adequately protect privacy and security.

At the same time, CDT urges the Committee to recommend substantial changes to DHS's proposed REAL ID regulations. We believe that the Department does have some authority to address privacy and security under the Act as it currently stands. Even given the limitations of the REAL ID Act, the Department could have done a much better job of creating a regulatory framework that does not increase the risk of identity theft nor enable widespread governmental and commercial tracking of U.S. residents. Since Congress might not pass explicit privacy and security mandates in a timely manner, it is exceedingly important for the final regulations to protect privacy and ensure security to the maximum extent possible.

B. THE ACT AND DRAFT REGULATIONS CREATE SERIOUS PRIVACY AND SECURITY RISKS

Risks to privacy and security flow from three key provisions in the REAL ID Act:

- Each state must "provide electronic access to all other States to information contained in the motor vehicle database of the State,"[3]
- Each state must "employ technology to capture digital images of identity source documents so that the images can be retained in electronic storage in a transferable format,"[4] and
- Each driver's license and ID card must contain a Machine Readable Zone (MRZ), which enables fast and easy collection of personal information by digital means.[5]

CDT's privacy and security concerns – based on the REAL ID Act as well as the proposed regulations – can be summarized as follows:

- **The Act's Requirement for "Electronic Access" Is Overbroad** – The Act mandates that each state give every other state "electronic access" to information contained in its DMV database. A nationally accessible network of government databases that contain highly sensitive personal information creates increased potential for abuse by government and identity thieves. The "electronic access" mandated by the Act is far broader than what

[2] NPRM, Preamble at 10825 n.3.

[3] REAL ID Act of 2005, Title II [H.R. 1268] Public Law 109-13, §202(d)(12).

[4] §202(d)(1). Subsection (d)(2) also requires states to "retain paper copies of source documents for a minimum of 7 years or images of source documents presented for a minimum of 10 years." The Conference Report on the REAL ID Act [H.R. 1268], House Report 109-72, explains with respect to §202(d)(2) that "The goal is to move all the state's records into electronic format, with each state consolidating electronic records otherwise maintained at the County level at the State level."

[5] §202(b)(9).

is necessary to achieve the goal of "only one license for one driver." ***CDT recommends that the "electronic access" provision of the REAL ID Act be repealed.***

- **The Act and Regulations Are Leading to a Centralized ID Database** – To implement the "electronic access" provision of the Act, DHS proposes to build upon the system used for commercial drivers: the Commercial Driver's License Information System (CDLIS), which is managed by the non-profit American Association of Motor Vehicle Administrators (AAMVA). Even though proponents of REAL ID have repeatedly stated that the Act would not produce a centralized database, that is precisely what CDLIS is: a central database that houses a small but very significant amount of personal information (including name and Social Security Number)[6] and that links to other information contained in state databases. Applying this system to all non-commercial drivers and ID card holders (i.e., virtually all U.S. residents) opens the door to the national linking of many other state and federal government databases; once a centralized identification database is established, there are no limits on what information it could point to. Both the Act and the proposed regulations fail to place any limits on the use of a centralized database. ***CDT recommends that a central database not be created, and instead that a system be designed that gives a simple "yes" or "no" answer regarding whether a person already holds a driver's license or ID card issued by another jurisdiction, and where that information comes directly from each state and not via a central repository.***

- **The Act and Regulations Fail to Protect the Privacy and Security of Personal Data in State DMV Databases** – The Act requires states to digitally copy and store for several years all source documents, which contain highly sensitive personal information. But neither the Act nor the proposed regulations contain limitations on what personal information (including source documents) in a DMV database can be accessed, by whom, and for what purposes. ***CDT recommends that source documents and other personal data in the state databases be accessible only by DMV officials for legitimate administrative purposes, and only by law enforcement officials for legitimate law enforcement purposes consistent with existing law. CDT recommends that the regulations include specific minimum security mandates for personal data stored in DMV databases.***

- **The Act and the Regulations Fail to Build Security into the Machine Readable Zone Technology** – The Act mandates that each driver's license and ID card have a machine-readable zone (MRZ) containing personal information, but the Act does not state what security and privacy standards the technology must meet. The lack of statutory guidance enables DHS to endorse technology with weak security. In fact, the Preamble to the proposed regulations contemplates that some driver's licenses and ID cards could contain an RFID chip so that they can be used in place of a passport book or PASS card at U.S. land and sea borders under the Western Hemisphere Travel Initiative (WHTI),[7] yet the RFID technology chosen for the PASS card is insecure. ***CDT recommends that privacy and security criteria be mandated for the MRZ technology***.

[6] *See* AAMVA's webpage on CDLIS <http://www.aamva.org/TechServices/AppServ/CDLIS/>.

[7] NPRM, Preamble at 10841-42.

- **The Act and the Regulations Set No Limits on the Amount and Nature of Data in the MRZ** – The Act does not limit the type or amount of personal information that can be digitally stored in the MRZ, and it appears from the Preamble to the proposed regulations that DHS gave little attention to the tradeoff of putting items of personal information, such as name, in the MRZ. There is a significant risk that any data in the MRZ will be inappropriately "skimmed." ***CDT recommends that the contents of the MRZ be limited to the information necessary for law enforcement purposes, and, as we explain below, that all information be protected against unauthorized skimming.***

- **The Act and the Regulations Fail to Limit the Compilation of Travel and Activity Information by Government Agencies** – Neither the Act nor the proposed regulations prohibit REAL ID cards from being read by innumerable state and federal government agencies, which would create a vast and efficient surveillance system that enables widespread tracking of the movements and activities of virtually all U.S. residents. ***CDT recommends that the MRZ be encrypted or otherwise designed so it can be read and/or personal data can be "skimmed" (as opposed to the card being visually inspected) only by DMV officials for legitimate administrative purposes, and by law enforcement officials for legitimate law enforcement purposes consistent with existing law.***

- **The Act and the Regulations Contain No Protections Against Skimming by Third Parties** – Neither the Act nor the proposed regulations prohibit the cards from being read and personal data "skimmed" by businesses or other non-governmental third parties to create profiles and fill databases with information about the activities and preferences of millions of U.S. residents. ***CDT recommends that the MRZ be encrypted or otherwise designed so it can be read and/or personal data "skimmed" (as opposed to the card being visually inspected) only by DMV officials for legitimate administrative purposes and by law enforcement officials for legitimate law enforcement purposes consistent with existing law.***

- **The Nationally "Unique" Identifier Can Become the New Social Security Number, With All the Risks of the SSN** – The proposed regulations refer to a "unique" card number and require that it be included in the MRZ. It is unclear whether this number would be unique nationally or state-by-state. A nationally unique number could be abused as happened with the Social Security Number. ***CDT recommends that the driver's license or ID card number not be standardized and unique across states, and that its use be expressly limited.***

All of these issues relate to those parts of the REAL ID Act and the proposed implementing regulations that go far beyond what is needed to make driver's license and ID card issuance more secure. These provisions create a *national identification system* by mandating "one person – one license/ID card – one record" supported by greater collection, centralization and sharing of highly sensitive personal information. The key point is that the more personal information is collected, centralized (even if in a technically "decentralized" system) and shared, the greater the potential for abuse not only by government and businesses, but also by terrorists, identity thieves and other criminals.

Neither the Act nor the proposed regulations control what information may be collected or accessed, by whom (i.e., state and government agencies, business, and other third-parties), and for what purposes. The Act does not mandate privacy and it barely addresses security, and DHS has failed to fill the gaps left by the statute despite an extensive discussion in the Preamble. Thus CDT concludes that the Act must be repealed or substantially rewritten to include mandates that protect privacy and ensure security. If Congress fails to act, DHS must do everything in its power to minimize the privacy and security impacts of the statute.

C. A MUCH DIFFERENT APPROACH IS NEEDED TO MAKE DRIVER'S LICENSE AND ID CARD ISSUANCE MORE SECURE

All of the privacy and security concerns raised above stem from elements of the Act and the proposed regulations that are not necessary to make the issuance of driver's licenses and ID cards more secure, thereby making the cards themselves a more reliable means of identifying individuals in special contexts. CDT supports the goal of making driver's license and ID card issuance more secure. Indeed, for years CDT has urged attention to the security flaws in the issuance of driver's licenses due to theft from DMV offices and insider DMV fraud.[8] And security in the issuance of driver's licenses and ID cards was the focus of the recommendation of the 9/11 Commission.[9]

Driver's license and ID card issuance can be made more secure without significantly compromising privacy, or weakening security in other ways. Measures to improve the security of the issuance process include verifying that a person is who he says he is, and that he is providing accurate and current information. Such measures also include ensuring that access to information and supplies used to create driver's licenses and ID cards are strictly controlled, and that the cards themselves are resistant to tampering and counterfeiting. Additionally, as already occurs under the Problem Driver Pointer System (PDPS)/National Driver Register (NDR), states should be able to be sure that they are not issuing a driver's license to someone whose license has been revoked in another jurisdiction. While such measures may raise questions about cost or practical implementation, they are reasonable reform measures that are likely to be effective and pose no risk to privacy or security.

Congress must revisit the REAL ID Act and create a statutory framework that addresses both privacy and security. CDT supports the bills introduced by Senator Akaka (S. 4117) and Representative Allen (H.R. 1117). These bills would repeal the REAL ID Act, but they also recognize the need for driver's license/ID card reform and aim to create a framework to do it right.

---

[8] *See* "Unlicensed Fraud: How bribery and lax security at state motor vehicle offices nationwide lead to identity theft and illegal driver's licenses" (January 2004) <http://www.cdt.org/privacy/20040200dmv.pdf>.

[9] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, Authorized Edition, at 390.

II. KEY PRIVACY AND SECURITY ISSUES

Privacy and security are fundamental to any system that deals with vast amounts of personal information. Privacy and security are interrelated: threats to privacy can create security risks, and vice versa.

A. "ELECTRONIC ACCESS" IS RISKY AND IS UNNECESSARY TO ENSURE "ONLY ONE LICENSE FOR ONE DRIVER"

1. The Statutory Language is Overbroad and Should be Repealed

According to the legislative history, the purpose of the "electronic access" provision of the REAL ID Act is to ensure that there is "only one license for one driver."[10] While this is a legitimate goal, mandating that each state give every other state "electronic access" to "information" contained in its "motor vehicle database" goes far beyond what would be appropriate to achieve only one driver's license or ID card per person, and instead creates enormous privacy and security risks.

This provision contemplates a national network of government databases that contain highly sensitive personal information. The greater centralization of personal data mandated by the Act creates increased potential for abuse by government and by identity thieves, especially given that the Act and the proposed regulations fail to place limits on authorized access and fail to mandate specific security measures to guard against unauthorized access. If one point in the network is compromised, the entire network will be compromised. And even if DHS were to amend the proposed regulations to interpret this provision narrowly now, the Department would be free to interpret it broadly in the future.

Furthermore, in the short-term, states are not at the same level (and will not be for some time) in terms of implementing highly secure issuance procedures and ensuring data accuracy within their own statewide systems. Until individual state databases are accurate and complete, it will be difficult to reliably check whether someone already holds a driver's license or ID from another jurisdiction. Granting electronic access to incomplete and inaccurate data will not improve security.

> **Recommendation to Congress:** Repeal the language of the REAL ID Act that requires each state to "provide electronic access to all other States to information contained in the motor vehicle database of the State."

2. The Proposed Regulations Favor a Centralized ID Database, Which Could Facilitate Nationwide Linking of Multiple Databases

The proposed regulations do not specify what "electronic access" means. Instead, the rules simply state, "States must provide to all other States electronic access to information

[10] Conference Report on H.R. 1268, House Report 109-72, at 184.

contained in the motor vehicle database of the State, in a manner approved by DHS pursuant to this regulation."[11] As a matter of transparency and accountability, this is inappropriate. It is incumbent upon DHS to be specific and transparent regarding how the multi-jurisdictional check will take place.

The Preamble, however, states that DHS is contemplating a system similar to (if not exactly like) that already in place for commercial driver's licenses: the Commercial Driver's License Information System (CDLIS).[12] CDLIS includes a central database with "pointers" or links to state databases. Therefore, DHS is *blatantly misleading* when it asserts that "the recommended architecture for implementing these data exchanges does not create a national database, because it leaves the decision of how to conduct the exchanges in the hands of the states."[13]

CDLIS, moreover, is not simply a " one license for one driver" system.[14] Rather, it is a "one person – one license (or ID card) – one *record*" system. In the REAL ID context, this is even more of a concern given that there are no statutory or regulatory limitations on what information may be in a person's "record," who can access the information, and for what purposes. Because this system would also include ID card holders, the "record" might not simply contain driving history. And, as the Privacy Impact Assessment for REAL ID explains, "CDLIS maybe subject to more limited privacy protections" because CDLIS – which is managed by the non-profit AAMVA – is not a federal "system of records" under the Privacy Act.[15]

---

[11] NPRM, Proposed Rules §37.33(b).

[12] The American Association of Motor Vehicle Administrators (AAMVA) manages a central database that includes basic identification information for holders of commercial driver's licenses. A person's "pointer" record within the central database includes the individual's name, alias information, date of birth, Social Security Number (mandatory), and current State of Record (the issuing state). The State of Record, after issuing a person's first CDL, must report the person's basic identification information to CDLIS, which becomes the individual's "pointer" record. AAMVA's central database does not contain a person's commercial driving history; this information is housed in the database of the State of Record.

If person applies for a CDL is another state, the new state will check CDLIS (by inputting basic identification information), which will then "point" to the person's commercial driving history in the State of Record's database. If the person's commercial driving history is good, the new state will issue a new CDL, become the new State of Record, and transfer the person's commercial driving history over to its own database. A person cannot have more than one commercial driver's license (nor can a person have a non-commercial driver's license at the same time) and his commercial driving history follows him from jurisdiction to jurisdiction.

[13] NPRM, Preamble at 10825. *See also* Renee Boucher Ferguson, "DHS Issues Proposed Regulations for Real ID Act," *eWeek* (March 2, 2007) (DHS Secretary Chertoff said, "We at the Department of Homeland Security in the federal government will not build, will not own, and will not operate any central database containing personal information. The data will continue to be held at the state level as it has traditionally been since they began to issue driver's licenses.") <http://www.eweek.com/article2/0,1895,2100036,00.asp>.

[14] Ensuring one-card-per-person, possibly using a CDLIS-type system, should be distinguished from states linking to federal databases to verify source document information (e.g., birth certificates, Social Security Numbers, passports, etc.).

[15] Privacy Impact Assessment, DHS Privacy Office, at 11 <http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_realid.pdf>

The Act and the proposed regulations place no limits on the number and type of state databases that could be nationally searchable via the "pointer system" once it is created. Under the centralized pointer system apparently contemplated by DHS, the risk for "mission creep" – linking new databases to the pointer – is enormous. Such centralization of personal data would also create a greater security risk, especially since the proposed regulations fail to include any specific security mandates for a CDLIS-type system.

When balancing the potential security benefits of a "one person – one license/ID card – one record" system (e.g., keeping track of driving "points")[16] against the privacy risks (i.e., a nation-wide identification system used to track people for purposes other than administering driver's licenses), it becomes evident that such a system should not be implemented. In any case, a CDLIS-type system for all U.S. drivers is largely unnecessary to ensure driver safety across states given the existence of the Problem Driver Pointer System (PDPS)/National Driver Register (NDR).[17]

To enable states to determine whether an applicant already holds a driver's license or ID card in another jurisdiction to achieve the goal of one-card-per-person, CDT recommends against creating either a central database or central identification records. Instead, a truly decentralized system should be architected that simply gives a "yes" or "no" answer regarding whether a person holds a driver's license or ID card issued by another state.

Recommendation to Congress: Prohibit the creation of a central database.

Recommendation to DHS: Architect a system that does not have a central database and that, instead, simply gives a "yes" or "no" answer regarding whether an applicant already holds a driver's license or ID card in another jurisdiction.

[16] *See* NPRM, Preamble at 10834 ("the primary purpose of State-to-State data exchange is driver safety – to ensure that drivers are not holding multiple licenses in multiple jurisdictions to avoid points from dangerous driving").

[17] When a driver in a state has his license revoked or suspended, or when he is convicted of a serious traffic violation such as a DUI, the state DMV is supposed to report this to the NDR. The NDR is a central database managed by the Department of Transportation, but it does not contain driver history information. Rather, what a state adds to the NDR is basic identification information including name, date of birth, gender , driver's license number, and reporting state. Social Security Number is optional; the state need not submit it to the NDR.

If the person tries to get a driver's license in another state, the new state will check the NDR (by inputting basic identification information), which will then "point" to the person's driving history housed in the original state's DMV database. The new state will decide whether to issue a new license based on this information. If a person is licensed in more than one state and has had those licenses suspended, for example, he will have more than one "pointer" record in the NDR. The purpose of the PDPS/NDR is to prevent a bad driver from evading his punishment or putting others at risk by getting a new license in another state.

B. PRIVACY AND SECURITY OF PERSONAL INFORMATION IN STATE DMV DATABASES

The Act and the proposed regulations have left unanswered key privacy and security questions related to the collection and use of personal information: What information may be collected and accessed, by whom, and for what purposes? How is personal information contained in the DMV databases going to be protected from unauthorized access?

Neither the Act nor the proposed regulations limit what information may go into a "motor vehicle database" (i.e., be part of a person's record). The Act merely requires states to include at a minimum "all data fields printed on drivers' licenses and identification cards issued by the State," and "motor vehicle drivers' histories, including motor vehicle violations, suspensions, and points on a license."[18] The Act also requires states to digitally copy and store for several years all source documents, which contain highly sensitive personal information (birth certificate, passport, Social Security card, utility bill).[19]

Yet neither the Act nor the proposed regulations contain limitations on what personal information in a DMV database (including source documents) can be accessed, by whom (i.e., state or federal agencies, businesses or other third parties), and for what purposes. The Privacy Impact Assessment frankly states that "DHS cannot rely on the DPPA [Driver's Privacy Protection Act] to protect the privacy of the personal information required under the REAL ID Act."[20] This is especially relevant if a DMV databases are linked or a CDLIS-type system is created, as greater electronic collection and centralization of personal information would facilitate government access to such information, as well as create a "target rich environment" for identity thieves.

> **Recommendation to Congress:** CDT believes that Congress must pass statutory limitations on the use of personal data stored in DMV databases, including source documents. Specifically, Congress should limit access to personal information to DMV officials for legitimate administrative purposes, and to law enforcement officials for legitimate law enforcement purposes consistent with existing law. Congress should also write legislation to secure personal data held in DMV databases against unauthorized access.

Even without clear privacy and security mandates from Congress, DHS should craft meaningful regulations to protect the privacy and security of personal data held in government databases. The Preamble includes various assurances that the REAL ID system will not afford the federal government any greater access to information than it already has,[21] but there are no

---

[18] §202(d)(13).

[19] §202(d)(1)-(2).

[20] PIA at 12.

[21] The Preamble asserts that "neither the REAL ID Act nor these proposed regulations gives the Federal Government any greater access to information than it had before. Moreover, there is no information about a

limits in the regulations themselves. Moreover, the proposed regulations simply require that each state, as part of its certification process, develop a "privacy policy regarding personal information collected and maintained by the DMV."[22] This is entirely insufficient. DHS should at the very least specify in the regulations criteria against which DHS will evaluate a state's privacy policy.

The Preamble states that the state privacy policies should follow Fair Information Principles (FIPs): openness, individual participation (access, correction, redress), purpose specification, data minimization, use and disclosure limitation, data quality and integrity, security safeguards, and accountability and auditing. DHS should write these into the regulations, along with more specific criteria for certification, consistent with the FIPs. Failure to do so will result in states having no guidance as to what is acceptable to DHS, and there will be 56 different privacy policies with different levels of protection.

CDT commends DHS for interpreting the "physical security" provision of the Act[23] as also contemplating database security.[24] The proposed regulations themselves require that states, as part of the certification process, develop "standards and procedures for safeguarding information collected, stored, or disseminated for purposes of complying with the REAL ID Act, including procedures to prevent unauthorized access, use, or dissemination of applicant information and images of source documents . . . ."[25] However, DHS must be more specific. Arguably, the only specific database security requirement in the proposed rules is internal audit controls.[26]

> **Recommendation to DHS:** By regulation, limit access to personal information, including source documents, to DMV officials for legitimate purposes related to the administration of driver's licenses and ID cards, and to law enforcement officials for legitimate law enforcement purposes consistent with existing law. Write specific privacy criteria – consistent with FIPs – against which the state privacy policies will be evaluated. Write specific security criteria against which the state security plans will be evaluated.

---

licensee that the Federal Government will store that it is not already required to store." NPRM, Preamble at 10824.

[22] NPRM, Proposed Rules §37.41(b)(5).

[23] §202(d)(7).

[24] NPRM, Preamble at 10826.

[25] NPRM, Proposed Rules §37.419(b)(8).

[26] NPRM, Proposed Rules §37.419(b)(7).

C. PRIVACY AND SECURITY OF DATA IN THE MACHINE READABLE ZONE (MRZ)

The Act requires that each driver's license and ID card have "a common machine-readable technology, with defined minimum data elements."[27] It is not clear why it is necessary to federally mandate a machine-readable zone in state driver's licenses and ID cards. Neither Congress nor DHS have clearly explained what the benefits are or whether they outweigh the privacy and security risks. It seems that the choice of whether to include an MRZ on each card could be left up to the states.

However, the main issue with regard to the MRZ is the collection and use of personal information digitally contained on the card. The Act falls short in four specific ways related to this issue:

- Not requiring privacy and security criteria for the chosen MRZ technology;
- Not requiring technological security features such as encryption;
- Not limiting the amount and type of personal information contained in the MRZ; and
- Not limiting who can "skim" data from the MRZ and for what purposes.

Failing to explicitly address skimming opens the door to using the REAL ID card as a key component of a vast and efficient surveillance system that enables widespread tracking of the movements and activities of virtually all U.S. residents. Similarly, businesses and other non-governmental third parties could create profiles and fill databases with the activities and preferences of millions of U.S. residents.

1. Privacy and Security Criteria for the MRZ Technology

The Act mandates that each driver's license and ID card have a machine-readable zone, but the Act does not state what privacy and security standards the technology must meet. The lack of statutory guidance enables DHS to endorse a technology with weak security. In fact, the Preamble contemplates that some driver's licenses and ID cards could contain an RFID chip so that they can be used in place of a passport book or PASS card at U.S. land and sea borders under the Western Hemisphere Travel Initiative (WHTI),[28] yet the RFID technology chosen for the PASS Card is insecure.

Recommendation to Congress: Establish minimum privacy and security criteria for the MRZ technology.

Recommendation to DHS: Prohibit the use of long-range or "vicinity read" RFID technology in driver's licenses and ID cards at this time.

[27] §202(b)(9).

[28] NPRM, Preamble at 10841-42.

2. Technological Security Features for the MRZ

A technological security feature such as encryption would help prohibit unauthorized "skimming" of personal information from the MRZ, both by government agencies and businesses compiling databases of movements and activities, and by identity thieves. Only state DMVs and law enforcement officials should have the ability to read the contents of the MRZ in clear text.

The REAL ID Conference Report explicitly contemplates that personal data would be "stored securely and only able to be read by law enforcement officials."[29] However, the Act itself fails to address privacy and security of personal data stored in the MRZ. Thus Congress should make technical protection, through encryption or other means, a clear statutory requirement.

DHS has stated in the Preamble that it "leans toward recommending that States protect the personally identifiable information stored in this 2D bar code by requiring encryption."[30] DHS has asked for public comments on the cost and feasibility of encrypting the MRZ: "DHS leans toward an encryption requirement if the practical concerns identified above [key infrastructure] can be overcome in a cost-effective manner."[31] CDT plans to offer more technical advice in the comments submitted to DHS prior to the May 8 deadline, but it seems that DHS has shirked its responsibility here. It is the Department's obligation to provide the public with a detailed analysis of the cost and feasibility of an encryption scheme, especially given Congress' clear intent that the MRZ be secure and that only law enforcement officials have access to the personal data contained in it.

> **Recommendation to Congress:** Statutorily require that the contents of the MRZ be protected by encryption or other technical means.
>
> **Recommendation to DHS:** Require by regulation that the contents of the MRZ be protected by encryption or other technical means. Conduct an analysis of the cost and feasibility of implementing an encryption scheme.

3. Limiting the Contents of the MRZ

In CDT's view, encryption or other technological means are clearly the best way to protect information on the MRZ. If Congress and DHS do not require encryption or other technological means of protecting MRZ data, this information can also be protected by policy and law. That may include narrowly limiting the information in the MRZ.

In the Preamble to the proposed regulations, DHS suggests that states should store "only the *minimum* data elements necessary for the purpose for which the REAL IDs will be used.

---

[29] Conference Report on H.R. 1268, House Report 109-72, at 179.

[30] NPRM, Preamble at 10826.

[31] NPRM, Preamble at 10838.

DHS requests comments on what data elements should be included . . . ."[32] However, the proposed rules themselves currently require nine data elements: 1) expiration date, 2) full legal name and all name changes ("name history"), 3) issue date, 4) date of birth, 5) gender, 6) principal address, 7) unique driver's license or identification number, 8) revision date, (9) inventory control number of the physical document.[33]

The Privacy Impact Assessment also discusses data minimization, a Fair Information Principle: "Good privacy policy supports limiting the data in the MRZ to the minimum personal data elements necessary for the intended purposes of providing access to law enforcement personnel."[34] Consistent with data minimization and because law enforcement officers are to be the intended beneficiaries of the MRZ, CDT believes that the only personally identifiable information that should be included in the MRZ is the number associated with a driver's license or ID card – especially if the MRZ is not encrypted or otherwise secured. The PIA recognizes that less information in the MRZ would make "skimming less attractive to third parties."[35]

CDT believes that Congress should make this a statutory limitation so that the required contents of the MRZ cannot be easily changed by regulatory action. But CDT believes that it is within the Department's present authority under the Act to further limit the contents of the MRZ.

> **Recommendation to Congress:** If there are no technological protection requirements for the MRZ such as encryption, Congress should statutorily limit the contents of the MRZ, and in particular should consider the risks of including name in the MRZ.
>
> **Recommendation to DHS:** If there are no technological protection requirements for the MRZ such as encryption, DHS should limit by regulation the contents of the MRZ, and in particular should consider the risks of including name in the MRZ.

4. Prohibiting by Law the Unauthorized Skimming of MRZ Data

The Conference Report on the REAL ID Act explicitly contemplates that the MRZ should "only be able to be read by law enforcement officials."[36] However, neither the Act itself nor the proposed regulations include this specific limitation. The PIA states, "the REAL ID Act does not contain any statutory language to address the downloading, access and storage by third parties of the information in the MRZ."[37] In the Preamble to the draft regulations, DHS recognizes that downloading from the MRZ is a serious concern, but it claims that it is powerless to address the problem:

---

[32] NPRM, Preamble at 10838 (emphasis added).

[33] NPRM, Proposed Rules §37.19.

[34] PIA at 17. *See also* NPRM, Preamble at 10826.

[35] PIA at 17.

[36] Conference Report on H.R. 1268, House Report 109-72, at 179.

[37] PIA at 14.

> The ability of commercial entities and other non-law enforcement third parties to collect the personal information encoded on driver's licenses or identification cards raises serious privacy concerns. However, while cognizant of this problem DHS believes that it would be outside its authority to address this issue within this rulemaking.[38]

CDT believes that Congress should explicitly prohibit non-DMV or non-law enforcement third parties – including state and federal government agencies, and private businesses and other entities – from "skimming" personal data from the MRZ. Moreover, Congress should mandate that the MRZ be designed to prevent skimming.

Additionally, CDT disagrees with the Department's assertion that it is powerless to address the skimming problem. DHS could require security features in the MRZ to prevent "skimming" for non-DMV or non-law enforcement purposes and also require states to outlaw unauthorized skimming as a condition of certification.

While collection of personal data off the MRZ is already possible in a number of states, CDT believes that it is the responsibility of both Congress and DHS – given the REAL ID federal mandate – to address this serious national problem in the next generation of driver's licenses that will emerge as a result of REAL ID.

> **Recommendation to Congress:** Statutorily limit the collection of personal data from the MRZ to DMV officials for legitimate purposes related to the administration of driver's licenses and ID cards, and to law enforcement officials for legitimate law enforcement purposes consistent with existing law.

> **Recommendation to DHS:** Require states, as part of the certification process, to pass laws that limit the collection of personal data from the MRZ to DMV officials for legitimate purposes related to the administration of driver's licenses and ID cards, and to law enforcement officials for legitimate law enforcement purposes consistent with existing law.

D. CONCERNS WITH A "UNIQUE" IDENTIFIER

The Act requires that the face of the driver's license or ID card show "the person's driver's license or identification card number."[39] While the Preamble echoes this language, the proposed regulations themselves refer to a "unique" number and require that it be included in the machine-readable zone. It is not clear whether the draft regulations require a number that would be unique state-by-state or nationally.

Significant privacy and security risks – most notably, the enhanced ability for tracking – would exist if the driver's license or ID card number were unique nationally, rather than within a state. The Privacy Impact Assessment assumes that "unlike a SSN, a person's driver's license

[38] NPRM, Preamble at 10837. *See also* PIA at 14.

[39] §202(b)(4).

number may change over time if the person moves from one state to another."[40] But neither the Preamble nor the proposed regulations say so.

> **Recommendation to Congress:** Mandate that the driver's license or ID card number not be standardized and unique across states.
>
> **Recommendation to DHS:** Mandate by regulation that the driver's license or ID card number not be standardized and unique across states.

Additionally, even though the PIA assumes that a REAL ID number will not be nationally unique, the document rightly notes that "if retailers, healthcare providers, financial institutions, insurers, and other private or government entities were to collect the credential and record the ID number whenever individuals engaged in a transaction, the REAL ID's unique number could pose the same, if not greater, risks as experienced in the use of the SSN."[41] Thus, "The only way to prevent misuse of any identifier is to establish enforceable restrictions at the time any REAL ID identifier is introduced."[42]

> **Recommendation to Congress:** Carefully consider how use of the REAL ID identifier can be limited.
>
> **Recommendation:** Carefully consider how states, as part of the "privacy" certification process, could limit the use of the REAL ID identifier.

III. CONCLUSION

CDT supports driver's license/ID card reform by making the issuance process more secure, thereby making the cards a more reliable means of identifying an individual in a given context. However, the privacy and security shortfalls of both the REAL ID Act and the Department of Homeland Security's proposed regulations are many. Moreover, deficiencies in the regulations stem directly from fundamental flaws in the Act.

CDT urges this Committee to recommend that the Secretary seek from Congress clear statutory authority to protect privacy and security. Because Congress may fail to pass corrective legislation in a timely manner, CDT urges this Committee to recommend to DHS that is make substantial changes to the regulations to address the serious privacy and security concerns created by the Act.

Again, thank you for the opportunity to testify before the Committee. We welcome additional questions you might have.

---

[40] PIA at 6.

[41] PIA at 6.

[42] PIA at 7. The issue of using the card identifier as an anchor to access lots of other personal information is distinguishable from using the REAL ID card as a physical credential that verifies a person's identity for "official purposes" such as entering a nuclear power plant. *See* §201(3).

###