epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

DEPARTMENT OF HOMELAND SECURITY

Agency Information Collection Activities: REAL ID: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Office Purposes

[Docket No. DHS-2019-0018]

June 17, 2019

By notice published April 16, 2019, the Department of Homeland Security ("DHS") extended the data collection implemented under the REAL ID Act.[1] Specifically, the notice describes the materials states must submit to certify or recertify their compliance with REAL ID.

The Electronic Privacy Information Center ("EPIC") submits these comments to 1) Call on DHS to publicly release all the certification/recertification documents submitted by each state; and 2) minimize the data collection and recordkeeping requirements under REAL ID.

I. Introduction

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues, and to protect

[1] *Agency Information Collection Activities: REAL ID: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Office Purposes*, 84 Fed. Reg. 15624(Apr. 16, 2019), https://www.govinfo.gov/content/pkg/FR-2019-04-16/pdf/2019-07565.pdf.

privacy, the First Amendment, and constitutional values. EPIC has considerable expertise analyzing the privacy and security risks attendant to the design and implementation of REAL ID.

In 2007, EPIC filed comments on behalf of leading experts in privacy and technology in response to the draft regulations for REAL ID.[2] At the time, we stated, "REAL ID is fundamentally flawed because it creates a national identification system. It cannot be fixed no matter what the implementation regulations say. Therefore, the REAL ID Act must be repealed."[3] EPIC also highlighted the privacy and security risks of REAL ID as part of the "Spotlight on Surveillance" series.[4] Additionally, EPIC testified before the DHS Data Privacy and Integrity Advisory Committee and explained that the REAL ID draft regulations impermissibly create a national identification system, prohibited by the law that established the DHS, and threaten national security and individual privacy.[5] In 2008, EPIC published a report detailing the significant costs of implementing REAL ID.[6] EPIC explained that "[DHS] [] believes that it can sweep aside the fact that REAL ID is an unfunded mandate by allocating $360 million to the States for REAL ID implementation…However, the number still pales next to the agency's 'reduced' estimate of $9.9 billion."[7] Our concerns about the problems with REAL ID are widely shared by many other organizations.[8]

---

[2] EPIC and 24 Experts in Privacy and Technology, *Comments on DHS 2006-0030: Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes* (May 8, 2007) [hereinafter "EPIC Expert Comments on Draft Regulations"],, https://www.epic.org/privacy/id_cards/epic_realid_comments.pdf.
[3] *Id.*
[4] *See* EPIC , *Federal REAL ID Proposal Threatens Privacy and Security* (Mar. 2007), https://epic.org/privacy/surveillance/spotlight/0307/.
[5] Melissa Ngo, EPIC, *Testimony and Statement for the Record at a Hearing Before the Data Privacy and Integrity Advisory Comm., Dep't of Homeland Sec.* (Mar. 21, 2007), http://epic.org/privacy/id_cards/ngo_test_032107.pdf.
[6] *See* EPIC, *REAL ID Implementation Review: Few Benefits, Staggering Costs* (May 2008), http://epic.org/privacy/id_cards/epic_realid_0508.pdf.
[7] *Id.*
[8] *Speak Out Against REAL ID*, The Privacy Coalition, https://www.privacycoalition.org/stoprealid/.

EPIC remains concerned that the REAL ID Act creates a national identification system, in violation of the DHS Act, and poses significant privacy risks to millions of individuals.

II. Privacy Risks Inherent in the REAL ID Act

a. The Department of Homeland Security is not fulfilling their responsibility to protect privacy

The DHS stated over ten years ago that it is constrained in its power to protect the privacy of individuals and their data under the REAL ID Act. The agency claimed in the draft regulations that, "The Act does not include statutory language authorizing DHS to prescribe privacy requirements for the state-controlled databases or data exchange necessary to implement the Act."[9] REAL ID creates a national identification system that affects hundreds of millions license and cardholders nationwide, yet today the DHS has still failed to institute strong privacy safeguards in the system itself.[10] The agency has the obligation to protect the privacy of individuals affected by this system and must do more than the feeble attempts set out in the Act.

The Privacy Act of 1974 applies to REAL ID under guidelines set out by OMB and DHS.[11] The OMB guidelines explain that the Privacy Act "stipulates that systems of records operated under contract or, in some instances, State or local governments operating under Federal mandate 'by or on behalf of the agency . . . to accomplish an agency function' are subject to . . . the Act."[12] The guidelines also explain that "systems 'maintained' by an agency

---

[9] Dep't of Homeland Sec., *Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*, 72 Fed. Reg. 10,819, 10,825 (Mar. 9, 2007) [hereinafter "REAL ID Draft Regulations"], http://edocket.access.gpo.gov/2007/07-1009.htm.

[10] EMERGENCY SUPPLEMENTAL APPROPRIATIONS ACT FOR DEFENSE, THE GLOBAL WAR ON TERROR, AND TSUNAMI RELIEF, 2005, 109 P.L. 13, 119 Stat. 231, 109 P.L. 13, 2005 Enacted H.R. 1268, 109 Enacted H.R. 1268; 6 C.F.R. 37.1 *et. seq.*

[11] EPIC Expert Comments on Draft Regulations, 6-12, *supra* note 2.

[12] Office of Mgmt. & Budget, *Privacy Act Implementation: Guidelines and Responsibilities*, 40 Fed. Reg. 28,948, 28,951 (July 9, 1975), http://www.whitehouse.gov/omb/inforeg/implementation_guidelines.pdf.

are not limited to those operated by agency personnel on agency premises but include certain systems operated pursuant to the terms of a contract to which the agency is a party."[13] The REAL ID system is operated under a Federal mandate to accomplish several agency functions, including immigration control.

Because the DHS has created this system, the agency must fully apply Privacy Act requirements of notice, access, correction, and judicially enforceable redress to the entire REAL ID national identification system. The REAL ID Act states that individuals should attempt to exercise their rights to notice, access, correction and redress through State DMVs, the Social Security Administration, the Department of State, and the U.S. Citizenship and Immigration Service (a part of the Department of Homeland Security).[14]

In enacting REAL ID, DHS has punted the issue of privacy to the States, but the agency needs to lead.

b. Privacy Risks of REAL ID

There are significant threats to individual privacy and security that are created by REAL ID.[15] Some of these problems are based on the design of the card, the information required to be stored on the cards, and the safeguards for the underlying databases.

Under REAL ID, a substantial amount of personal information must be included on the card. This includes a full legal name, digital photograph, and signature that can be read by common machine readable technology and the information included on the card is not required to be encrypted. Prior to enactment, the DHS Privacy Office supported encryption "because 2D

[13] *Id.*
[14] *Final Rule, Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*, 73 Fed. Reg. 5271, 5284-5284 (Jan. 29, 2008), http://edocket.access.gpo.gov/2008/08-140.htm.
[15] EPIC Expert Comments on Draft Regulations at 17-28, *supra* note 2.

bar code readers are extremely common, the data could be captured from the driver's licenses and identification cards and accessed by unauthorized third parties by simply reading the 2D bar code on the credential" if the data is left unencrypted.[16] There are many examples of unauthorized users being able to download data from unencrypted machine-readable technology.[17] To protect privacy and improve security, this machine-readable technology must either include encryption or access must be limited in some other form. Without required encryption, REAL ID leaves hundreds of millions individuals at risk for individual tracking.[18]

DHS rejected encryption in the final rule because of "the complexities and costs of implementing an encryption infrastructure."[19] DHS is required to include security protections on the REAL ID card. Under the REAL ID Act, the card must include "Physical security features designed to prevent tampering, counterfeiting, or duplication of the document for any fraudulent purpose."[20] The agency has this obligation and it should not abdicate this responsibility. If DHS does not seek to limit access to the data on the REAL ID card, then it is signaling that it is acceptable for third parties to download, access and store data for purposes beyond the three official purposes.

Rejecting encryption for the 2D barcode helps to push the REAL ID system into "widespread" use in everyday life, a goal that former DHS Secretary Chertoff and the DHS final rule itself expect and support. Such an expansion would harm both individual privacy and

[16] Dep't of Homeland Sec. Privacy Office, *Privacy Impact Assessment for the REAL ID Act* 16 (Mar. 1, 2007), http://www.epic.org/privacy/id_cards/pia_030107.pdf.
[17] EPIC Expert Comments on Draft Regulations at 21-23, *supra* note 2.
[18] *Id.* at 17-18.
[19] *Final Rule, Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*, 73 Fed. Reg. 5271, 5292 (Jan. 29, 2008), http://edocket.access.gpo.gov/2008/08-140.htm.
[20] REAL ID Act at §202(b)(8).

security and facilitate turning the United States into a country where the REAL ID national identification card is involuntarily carried by everyone.

Furthermore, the amount of information contained on the REAL ID cards increases risks if the card is compromised. There are a number of "insider" and "outsider" threats to the massive identification database connecting 56 States and territories. Creating a national identification database containing personal data of hundreds of millions State license and ID cardholders nationwide, one that would be accessible from a massive number of DMVs across the country, is an invitation for all criminals – whether identity thieves or terrorists – to break into just one of these entrance points to gather such data for misuse.

Such a system would also be at risk of abuse from authorized users, such as DMV employees, who are bribed or threatened into changing the system data or issuing "authentic" national identification cards. It is appropriate to note here that, on the day that DHS released the final regulations for REAL ID, "A Maryland Motor Vehicle Administration employee [...] and four others were indicted [ ] on charges that they made and sold fake State driver's licenses and identification cards in exchange for money."[21]

Identity theft continues to be one of the leading concerns for consumers.[22] In 2018, the last year for which information is currently available, the number of identity theft claims the FTC

[21] *Five indicted in identity theft scheme*, BALTIMORE SUN, Jan. 11, 2008.
[22] *Imposter Scams Top Complaints Made to FTC in 2018*, FEDERAL TRADE COMMISSION, Feb. 28, 2019, https://www.ftc.gov/news-events/press-releases/2019/02/imposter-scams-top-complaints-made-ftc-2018.

received increased by more than 16% compared to the identity theft incidents reported in 2017.[23] Furthermore, identity theft has been one of the top consumer issues for the past fifteen years.[24]

Large-scale data breaches have occurred in State DMVs across the country; if the databases are linked under REAL ID, these breaches will only grow in scale. The Oregon DMV lost half a million records in 2005.[114] Also that year, in Georgia, a dishonest insider exposed 465,000 records.[115] In 2011 a North Carolina DMV worker was charged with five counts of identity theft after she used DMV computers to obtain information to take out payday loans in other people's names.[25] In 2014, the California DMV suffered a data breach where credit card information was compromised via their online payment system.[26] In 2015, an Oregon man was able to download a list that contained a DMV list of identification numbers as well as federal income tax forms and was charged with 26 counts of aggravated identity theft.[27] The list goes on, and the personal information of individuals will be endangered under the REAL ID national identification system.

III. DHS Must Increase Transparency and Reevaluate Data Collection Under REAL ID

The REAL ID Act poses serious privacy risks that DHS has failed to address. As EPIC stated previously in its comment on the proposed REAL ID rule, the REAL ID Act should be

---

[23] *See*, FTC, *Consumer Sentinel Network: Data Book 2018*, Appendix B2 (Feb. 2019), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2018/consumer_sentinel_network_data_book_2018_0.pdf.
[24] *See FTC Releases Annual Summary of Consumer Complaints*, FEDERAL TRADE COMMISSION, Mar. 1, 2016, https://www.ftc.gov/news-events/press-releases/2016/03/ftc-releases-annual-summary-consumer- complaints; *see also FTC Releases Annual Summary of Complaints Reported by Consumers*, FEDERAL TRADE COMMISSION, Mar 1, 2018, https://www.ftc.gov/news-events/press-releases/2018/03/ftc-releases-annual-summary-complaints-reported-consumers.
[25] Sloane Heffernan, *Charge: Worker Used DMV Computers for ID Theft,* WRAL, Oct. 17, 2011, http://www.wral.com/news/local/story/10268291/.
[26] *Sources: Credit Card breach at California DMV,* KREBS ON SECURITY, Mar. 22, 2014, https://krebsonsecurity.com/2014/03/sources-credit-card-breach-at-california-dmv/.
[27] Brent Welsberg, *Convicted ID Thief Found With 'How To' Guide, DMV Database*, KOIN6, http://koin.com/2015/02/12/convicted-id-thief-found-with-how-to-guide-dmv-database/.

repealed. Although DHS is not initiating any new collection of data under the current notice for comments, EPIC urges the agency to increase the transparency around the state certification/recertification requirements and release publicly the documents associated with that process for each state, particularly the security plan that is required. The security plan has vital information on how the DMVs secure personal information, the privacy policies, and the standards and procedures for document retention and destruction. Additionally, the security plan submitted for certification/recertification contains information on the use of biometric data.

DHS must also reevaluate the current data collection and recordkeeping requirements under REAL ID. DHS must minimize the amount of information that the agency collects and similarly should work with states to reduce the amount of information the state DMVs collect and retain for REAL ID purposes. DHS and state DMVs should not collect more information than is necessary or retain information longer than is necessary.

IV. Conclusion

For the foregoing reasons, EPIC urges DHS to implement additional transparency and minimization requirements associated with the current collection activities under the REAL ID.

Respectfully submitted,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President and Executive Director

/s/ Jeramie D. Scott
Jeramie D. Scott
EPIC Senior Counsel