epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

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

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

Homeland Security Department

Request for Information: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Mobile Driver's Licenses

86 Fed. Reg. 20320, Docket No. DHS-2020-0028

July 30, 2021

---

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Homeland Security Department's (DHS's) Request for Information (RFI) on Mobile Driver's Licenses.[1] On June 16, 2021 the agency extended the original comment period to July 30, 2021.[2] DHS's RFI seeks input on the agency's planned "upcoming rulemaking that would address security standards and requirements for the issuance of mobile or digital driver's licenses".[3]

EPIC urges DHS to take a slow and careful approach to digital identity verification that fully addresses the substantial privacy implications of a shift to mobile driver's licenses (mDLs). EPIC is not opposed in theory to a mobile driver's license. However, implementing a phone-based driver's license policy would not solve any outstanding problems that DHS currently faces. The agency should take a cautious approach to establishing an mDL standard to ensure that these new systems improve, rather than diminish, individual privacy and autonomy. DHS should also ensure that physical IDs remain at least equivalent to Mobile Driver's Licenses and users of physical ID cards are not subjected to discrimination or other negative impacts such as longer waits or excess scrutiny.

[1] 86 Fed. Reg. 20320.
[2] 86 Fed. Reg. 31987.
[3] 86 Fed. Reg. 20320.

EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in ensuring that DHS's traveler screening and security policies, including identity verification are respectful of and adequately protect individual privacy.[4] EPIC also frequently provides expert input on the federal government's technical standards, including identity verification, to encourage the adoption of privacy-enhancing technologies and best practices.[5]

**EPIC's response to DHS's Request for Information.**

**Item 2. Privacy Generally**.

Provide comments on what privacy concerns or benefits may arise from mDL transactions, and how DHS should or should not address those concerns and benefits in the REAL ID context. Explain what digital security functions or features are available to protect the privacy of any personally identifiable information submitted in mDL transactions, including the advantages and disadvantages of each security feature.

---

[4] *See e.g* Comments of EPIC to the Department of Homeland Security/U.S. Customs and Border Protection, Collection of Biometric Data From Aliens Upon Entry to and Departure From the United States, Docket No. USCBP-2020-0062 (Dec. 21, 2020), https://epic.org/apa/comments/EPIC-Comments-CBP-Biometric-Entry-Exit-December-2020.pdf; *EPIC v. CBP (Biometric Entry/Exit Program)*, EPIC, https://epic.org/foia/dhs/cbp/biometric-entry- exit/default.html; *EPIC v. CBP (Biometric Entry-Exit Alternative Screening Procedures)*, EPIC, https://epic.org/foia/dhs/cbp/alt-screening-procedures/; Comments of EPIC to the Department of Homeland Security, Agency Information Collection Activities: Biometric Identity, Docket No. 1651-0138 (Jul. 24, 2018), https://epic.org/apa/comments/EPIC-CBP-Vehicular-Biometric-Entry-Exit-Program.pdf; EPIC v. CBP (Biometric Entry/Exit Program), https://epic.org/foia/dhs/cbp/biometric-entry-exit/default.html (EPIC obtained a report which evaluated iris imaging and facial recognition scans for border control); EPIC Statement to U.S. House Committee on Homeland Security, "Border Security, Commerce and Travel: Commissioner McAleenan's Vision for the Future of CBP" (Apr. 24, 2018), https://epic.org/testimony/congress/EPIC-HHSC-CBP-Apr2018.pdf; Comments of EPIC to the Department of Homeland Security, Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/U.S. Citizenship and Immigration Services—018 Immigration Biometric and Background Check (IBBC) System of Records, Docket Nos. DHS-2018-0002 and DHS-2018-0003 (Aug. 30, 2018), https://epic.org/apa/comments/EPIC-DHS-Immigration-Biometric-Database.pdf.

[5] *See e.g.,* ., Comments of EPIC to the National Institute of Standards and Technology, Request for Comments on Federal Information Processing Standard (FIPS) 201-3 (Personal Identity Verification), Docket No. 201023-0280 (Feb. 1, 2021), https://epic.org/apa/comments/EPIC-NIST-PIV-FIPS-Feb-2021-Comments.pdf; Comments of EPIC to the Data Privacy and Integrity Advisory Committee, October 27, 2020 Meeting and New Tasking, Docket No. DHS-2020-0039 (Nov. 10, 2020), https://epic.org/apa/comments/EPIC-DPIAC-Meeting-Oct-2020-Comments.pdf.

Mobile Driver's Licenses Must Not Broadcast Sensitive Data to Third Parties

EPIC urges DHS not to implement any Mobile Driver's License system unless it can ensure the system implements best cryptographic and data security standards to prevent tracking of identity or verification data by third parties. mDL systems should not wirelessly transmit identity verification information in a way that can be intercepted by third parties. Any scanning of mDLs should rely barcode or other non-broadcast communication methods wherever possible. When a phone wirelessly transmits data to a scanning device it creates a risk that information may be intercepted by third parties. Broadcasting user data thus creates significant risks of both tracking and the loss of individuals' sensitive data, including biometrics.

If mDLs transmit face templates for comparison, the loss of a face template could lead to serious privacy harms. EPIC urges DHS not to implement any mDL system that is capable of transmitting/receiving facial recognition templates. Individuals should not have to submit to nonconsensual facial recognition and public surveillance when verifying their identity for mundane events like travel. DHS should minimize the amount of data transmitted in the mDL verification process and use strong encryption protocols for what remains.

Mobile Driver's Licenses Should Not Be Implemented in Ways That Expand Police Searches of Electronic Devices

DHS should ensure that any mDL implementation allows the individual to retain control over their electronic device. Checking an mDL should not require individuals to be subject to pseudo-consensual investigative phone searches by handing over their unlocked devices to an officer. If MDLs require a phone to be unlocked before transmitting data to the identity verification device there is a significant risk that law enforcement officers will take advantage of unlocked phones to perform searches. It is well documented that U.S. Customs and Border Protection (CBP) has conducted many warrantless searches of phones and other electronic devices at the border, which has

subjecting border communities and travelers to invasive surveillance.[6] After sustained opposition by civil rights and immigrants' rights groups, the U.S. Court of Appeals for the Ninth Circuit recently limited border searches.[7] The American Bar Association has also urged Congress and DHS to implement a warrant standard for searches of US person phones at the border.[8] Mobile Driver's Licenses should not become another avenue to unchecked and unwarranted searches.

In evaluating the risk that rollout of mDLs will lead to increased invasive phone searches, the DHS consider the impact not only of the actions by federal law enforcement officials at TSA and HSI but also of local law enforcement. DHS's decision to implement mDLs would likely trigger broad adoption of the technology across the country. The existence of mDLs may lead states to permit digital identity verification in bars, at sporting events, and wherever physical IDs are now used. Because use of mDLs may expand far beyond DHS's intended use-case, the agency should slow implementation of mDLs to account for greater risks. As mDLs are used widely during daily life and during traffic stops, individuals will be forced to run a gauntlet of police interactions with potentially unlocked phones. Mandating a mDL that can be used with a locked phone would provide a substantial level of protection. DHS should carefully weigh the benefits of MDLs and only proceed when the agency can ensure that adopting MDLs will not expose individuals to increased surveillance.

Mobile Driver's Licenses Should Minimize the Risk of Tracking by Verifying Entities

DHS should only implement mDLs systems that comply with standards prioritizing data minimization for verifying entities to mitigate the risk of verifying entities tracking individuals. Both

[6] *See*, *EPIC v. CBP (Border Search Audits of Electronic Devices)*, https://epic.org/foia/dhs/cbp/border-search-audits/default.html;
[7] *United States v. Cano*, 934 F.3d 1002 (9th Cir. 2019).
[8] American Bar Assn., Resolutions with Reports to the House of Delegates 2019, Resolution 107A (Jan. 28, 2019), https://www.americanbar.org/content/dam/aba/administrative/house_of_delegates/ebook-of-resolutions-with-reports/2019-midyear-ebook-of-resolutions-with-reports.pdf.

the standards and technical features of mDL systems should require the minimum necessary amount of information for verification. For example, a system validating identity can request either a birthdate or the individual's age. Under data minimization principles, the mDL should send only the individual's age to reduce the risk of re-identification from bulk data and tracking by verifying entities. A system that requests only the minimum necessary information is substantially more privacy protective but equally reliable for the verifier.

**8. Data Freshness.**

a. Provide comments regarding what data synchronization periods commenters believe are appropriate for mDL transactions. Explain the advantages and disadvantages of a longer or shorter periods.

DHS should only implement mDL systems that permit long data synchronization periods to minimize the privacy harms from repeatedly refreshing digital identity credentials. Because DHS intends to use mDLs only for identity verification there is no need for rapid data synchronization periods. Travelers only infrequently update their physical drivers' licenses, which usually have long renewal periods. The median license renewal period in the US is 5-6 years while Arizona and South Carolina licenses are good for more than a decade.[9] In practice most individuals will replace their cell phones before they renew their driver's license. Most cell phone users in the US replace their phones in 18 months to 3 years.[10] DHS then does not need to enforce a short data freshness period and should instead tie freshness to the median physical driver's license renewal time.

Shorter freshness periods pose a threat to privacy by increasing contacts between phones and state DMV databases. More connections run a greater risk of data breach and permit greater

[9] Andrew Perez, State By State: Differences In How States Handle Driver's License Renewals, DMV.com (Aug. 6, 2018), https://www.dmv.com/blog/how-states-handle-drivers-license-renewals-091283-524180?tg1=DVA&utm_content=dmv.com&utm_medium=dmv_&tg7=dmv_&utm_source=dmv.com&tg9=dmv.com&utm_term=organic_dmv&utm_campaign=organic_dmv.

[10] Mariella Moon, Americans are waiting three years to replace their phones, study finds, Engadget (Aug. 23, 2019), https://www.engadget.com/2019-08-23-us-phone-upgrade-strategy-analytics.html.

electronic surveillance. In contrast longer synchronization periods reduce the amount of information in government databases and lower the risk of data loss without substantial tradeoffs. DHS should consider mDLs sufficiently "fresh" for a period of several years to match physical IDs.

**11. Offline and Online Data Transfer Modes.**

DHS understands that mDL Data may be transferred to a Federal agency via offline and online modes. a. Explain the security and privacy risks, from the perspective of any stakeholder, presented by both offline and online data transfer modes.

Mobile Driver's Licenses Must Not Permit Location Tracking

DHS must ensure that mDLs do not permit the identity verification process to create a record establishing the individual's physical location. The draft ISO/IEC 18013-5 standard DHS proposes to adopt permits "online data transfer" between DHS and state DMVs to verify licenses. Online data transfer is unnecessary to validly establishing identity and exposes individuals to location tracking. As mDLs proliferate, they will be used in bars, to enter sporting events and other secured areas, and scanned by police during traffic stops and other interactions. A series of ID verifications linked to individual scanner devices will create a location history tied to the mDL. EPIC has long opposed phone-based location tracking.[11]

**Conclusion**

EPIC supports DHS's careful consideration of Mobile Driver's Licenses and urges the agency to slow the process of adopting MDLs until the risks of privacy harms are resolved. DHS must consider the broader implications of MDLs and seriously weigh the risks of catalyzing the spread of a new form of identity verification. EPIC emphasizes that there is no urgency to adopt mDLs and reminds the agency of numerous potential privacy harms from poorly designed digital

[11] *See e.g.*, *EPIC Amicus Brief, Carpenter v. United States*, 585 U.S. ___ (2018), https://epic.org/amicus/location/carpenter/Carpenter-v-US-amicus-EPIC.pdf; EPIC v. Accuweather, https://epic.org/privacy/litigation/consumer/epic-v-accuweather/ (EPIC filed a consumer protection lawsuit against AccuWeather International, Inc. alleging that the company engaged in unlawful and deceptive practices in tracking consumers' locations. AccuWeather changed its location tracking practices.).

IDs. For more information or any other questions please contact EPIC Fellow Jake Wiener at wiener@epic.org.

Respectfully Submitted,

*Jake Wiener*
Jake Wiener
EPIC Law Fellow