ASPEN POLICY ACADEMY
aspen institute

Policy Brief

Privacy in Pennsylvania: Educating Policymakers on Mobile Driver's License Security

By Amber Turner
December 2025

This policy project was developed by Aspen Policy Academy fellow Amber Turner while participating in the Science and Technology Policy Fellowship. This policy brief provides an overview of the fellow's proposed solution. The full project is available here. Please note that the author's opinions published here are their own. This publication does not reflect the views of the Aspen Policy Academy or the Aspen Institute.

Executive Summary

As Pennsylvania considers adopting mobile driver's licenses (mDLs) – driver's licenses that are stored on users' mobile phones – the state should prioritize targeted education for policymakers on the high-stakes privacy and cybersecurity risks associated with mDLs before proceeding with development, legislation, or deployment. While mDLs offer modernization and convenience, they can introduce serious privacy and cybersecurity risks for both residents and governments. These risks include real-time tracking of residents, unauthorized and/or improper data storage and retention, failed data storage and retention, and heightened cyberattack exposure.

To mitigate these risks, the Commonwealth of Pennsylvania should invest in structured policy briefings and workshops on mDL-specific risks, leveraging privacy experts, technologists, members of law enforcement, and civil rights advocates to ensure that policymakers gain a comprehensive understanding of how mDL implementation will impact a variety of stakeholders. From this informed foundation, Pennsylvania could responsibly pursue mDL implementation in a way that protects residents and upholds public trust.

Background

Pennsylvania is evaluating the adoption of mobile driver's licenses, which allow residents to present a state-issued identification digitally on a mobile device. Mobile driver's

licenses are emerging as a digital identity solution across the United States: 26 states are actively working on adoption, and 6 states have fully adopted mDLs. Some states have partnered with major tech vendors, while others are considering in-house solutions to maintain more control over sensitive data.

The Pennsylvania Department of Transportation (PennDOT) is in the exploratory stages of developing an mDL system. While PennDOT has publicly signaled interest in creating its own state-controlled mDL app, it faces several key challenges that impact its ability to move forward, including resource constraints, ambiguity in legislative direction, and technical talent to launch and maintain a project of this size.

PennDOT aims to protect Pennsylvania residents from the data practices of technology companies, focusing on concerns like data sovereignty and commercial exploitation. However, the agency lacks internal privacy, security, and ethics experts who can convey why residents should also be concerned about the state's access to and storage of their location data. If Pennsylvania policymakers better understood privacy risks and digital rights, they would recognize that shaping policy for mDLs requires creating a governance framework that safeguards residents — not just from private companies, but from the state itself.

Pennsylvania risks repeating the mistakes made in other jurisdictions — launching mDLs without adequate legal, technical, or ethical guardrails, which undermines public trust.

Recommendations

The Commonwealth of Pennsylvania should launch a structured, expert-led policymaker education initiative that helps lawmakers understand the risks and benefits of mDL implementation. This initiative should focus on equipping policymakers with the knowledge they need to make informed, rights-conscious decisions. Mobile driver's licenses implicate a range of sensitive issues that policymakers should prioritize, including individual privacy and government surveillance, cybersecurity vulnerabilities, and constitutional protections. These are high-stakes concerns, and uninformed decisions could result in long-term harm to residents' rights and public trust in government institutions.

The policymaker education initiative should begin with a series of curated briefings, workshops, and roundtable discussions with key stakeholders, including state legislators, regulatory agencies, PennDOT, privacy advocates, cybersecurity practitioners,

technologists, legal scholars, and law enforcement. Real-world case studies and emerging threat scenarios should ground the discussions, giving policymakers a concrete understanding of potential harms and consequences if critical safeguards are neglected. This approach would not only mitigate the risks of mDLs but also ensure that decisions about mDLs are grounded in a foundational understanding of their legal, technical, and social implications. Pennsylvania can position itself as a leader in responsible digital identity governance by making policymaker education a priority.

Implementation: Plan of Action

The state should take 3 steps to implement this recommendation:

1. Launch a statewide Digital Identity and Privacy Task Force on mDL risks and governance.

Pennsylvania should propose a statewide education task force made up of policymakers, law enforcement officials, PennDOT officials, and representatives of civil liberties organizations from across the political spectrum. Members of the task force would participate in the policymaker education initiative, which would equip them with a clear understanding of the privacy, cybersecurity, and civil liberties implications of mDLs. To recruit policymakers to join the task force, the state should emphasize its responsibility to anticipate and address these risks before authorizing the development and deployment of mDL technology. Members would gain a better understanding of the technical complexities and privacy tradeoffs of mDLs.

2. Convene a multi-stakeholder briefing series.

The state should then organize a series of policy briefings and interactive workshops that bring together a variety of stakeholders, including state legislators, regulatory agencies, PennDOT, privacy advocates, cybersecurity practitioners, technologists, legal scholars, and law enforcement. By convening a broad variety of experts in this field, policymakers would gain a deeper understanding of the potential risks and benefits associated with implementing mDLs. These sessions would focus on key areas of risk, such as digital surveillance, cybersecurity vulnerabilities, and the implications of device search. The format would encourage dialogue, ensuring that policymakers grasp both the technical and the societal consequences of mDLs.

3. Develop policy resources and action guides.
Finally, the state should produce a toolkit of practical resources, including policy briefs, legislative checklists, privacy-by-design guidance, and summaries of lessons learned from other states' mDL experiences. These formal deliverables should be developed in collaboration with the experts leading the education initiative workshops. The materials would be distributed broadly to legislators and PennDOT leadership to serve as lasting references informing future debates, bill drafting, oversight responsibilities, and technology development.

Once adopted, this initiative could serve as a model for educating policymakers on emerging technology issues statewide.

If you'd like to learn more, see the full project, including an education briefing series and a case study, at aspenpolicyacademy.org/project/mobile-drivers-licenses-2025.

About the Aspen Policy Academy

The Aspen Institute's Policy Academy helps community leaders and experts across the political spectrum elevate their voices, influence key decisions, and strengthen democracy from the ground up. Our innovative training programs and resources equip people across sectors – from tech to the environment, science to civic engagement – with the skills to shape critical policy efforts. Learn more at aspenpolicyacademy.org.

Photo credit: CHUTTERSNAP via Unsplash