ASPEN POLICY ACADEMY
aspen institute

Operational Plan

Comparison of Mobile Driver’s License Implementation: Informing Pennsylvania’s Path Forward

By Amber Turner

December 2025

This policy project was developed by an Aspen Policy Academy fellow while participating in the Science and Technology Policy Fellowship. This case study offers examples of mobile driver’s license implementation. The full project, including a policy brief explaining the fellow’s core recommendations, 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.

As Pennsylvania considers the adoption of a mobile driver’s license (mDL) program, it is critical to consider real-world examples of implementation in other jurisdictions to understand the risks and benefits of this technology. The growing interest in digital identity tools presents many opportunities and challenges. While mDLs offer modernization and convenience, they can introduce serious threats to users related to privacy, data governance, and law enforcement access.

To inform Pennsylvania’s approach, this case study examines noteworthy examples of the implementation of mDLs in jurisdictions in the United States and abroad. Each case highlights important themes, such as user control, technical guardrails, and function creep. By studying both successful and problematic deployments, Pennsylvania can take advantage of the lessons learned and design an mDL program that leverages the conveniences of tech innovation while protecting residents’ privacy.

1. Privacy Vulnerabilities: New South Wales, Australia

The state of New South Wales (NSW), Australia, was one of the first jurisdictions in the world to implement state-wide mobile driver’s licenses, launching the Digital Driver Licence (DDL) program in 2019 through the Service NSW mobile app. This mDL technology allows residents to display a digital version of their driver’s license and use it as legal identification at bars, during law enforcement checks, and at many government offices.

The program had over 2 million users within the first year, and it was initially considered a success. However, the app's technology was later found to have critical privacy vulnerabilities. The mDL technology used in NSW was QR-code based and provided full access to unencrypted sensitive personal information — including the license holder's full name, address, birthdate, and driver's license number. Anyone with a basic QR code scanner could easily access and store private data from the app without the license holder's consent or even their awareness.

In 2020, a major data leak was discovered in the DDL program, impacting over 50,000 residents. This data exposure was significant because the data were not believed to be retrieved directly from the government's system but from an unknown actor's compilation of data accessed and stored over time. The weak encryption of QR code technology highlighted the privacy vulnerabilities of the DDL program in an unfortunate real-life scenario.

Key Takeaways for Pennsylvania

The New South Wales case underscores the importance of prioritizing data minimization and privacy-by-design principles. While QR code technology was popular and trendy at the time of this mDL program deployment, its weak encryption and basic visual presentation made it easy to forge and breach. The following are some key takeaways for Pennsylvania:

- Avoid weak encryption. Choosing a simple technical solution could make the system too easy for the average technologist to exploit and hack.
- Independent testing and security auditing are critical before a statewide rollout. Employing a user-friendly system like QR codes comes with trade-offs; however, many security failures could be avoided with sophisticated penetration testing.

2. Implementation Trade-offs: Colorado

Colorado launched its mobile driver's license license through the myColorado app, which was positioned as a "one-stop shop" model for Colorado residents. The myColorado app was designed to house a variety of resident credentials, including mDLs, voter registration, vehicle registration, and hunting licenses. The mDL program was adopted as a part of a broader digital government initiative to simplify access to public services.

Colorado made significant investments in the technical components of its mDL program that contributed to acceptance of the app. For example, the system included a per-presentation capability that allows Colorado app users to choose what information from their driver's license is shown each time they open the app. Age verification at a restaurant or bar would show a 21+ symbol and the license holder's photo; a traffic stop by law enforcement, however, would require the full license to be shown. Instead of automatically exposing the entire license record, this focus on data minimization helps protect sensitive data from unnecessary disclosure.

However, the multifunctional capabilities of the myColorado app raise many privacy and civil liberties concerns. The app poses significant risk of function creep and cybersecurity attack because it houses sensitive data, including the user's identity, location, and service records. Currently, there are no guardrails regulating whether law enforcement can physically handle a resident's phone when an mDL is presented. Since the mDL is housed within the same app that contains other official records, there is nothing to stop officers from searching or exploring unrelated sections of the app. The aggregation of sensitive data could be leveraged to fuel surveillance and profiling practices.

Key Takeaways for Pennsylvania

The Colorado case illustrates the trade-offs involved in integrating multiple services into a single government app. While bundling services may seem efficient, the myColorado app increases the attack surface for cyberthreats. In many ways, Colorado residents' data are overexposed in exchange for convenience. The following are some key takeaways for Pennsylvania:

- A stand-alone mDL app or functionality that is separate from other government digital services provides more protection for residents and is the most secure. When the mDL app is housed with other government records, the risk of function creep, unrelated search, or unauthorized surveillance increases.
- Mobile driver's license apps that are designed with per-presentation user control give residents the ability to choose how much of their sensitive data is displayed or shared in each situation.

3. Strong Design and Privacy: Louisiana

Louisiana launched its mobile driver's license program in partnership with the private technology firm Envoc. Louisiana's mDL is part of the LA Wallet app, and it is widely accepted by Louisiana law enforcement agencies and businesses. The LA Wallet app includes COVID-19 vaccination records, voter registration status, and other records and allows real-time verification. Like Colorado's program, Louisiana's mDL offers users the ability to select what information is disclosed (e.g., age, photo, address) each time they open the app, thus minimizing data exposure.

The most notable feature of Louisiana'smDL program is its "no-touch" policy, which allows users to maintain control of their mobile phone at all times. In designing its mDL, Louisiana paired technology capability with legislative policy requiring all law enforcement officers be trained to view and verify license credentials without ever needing to physically touch the resident's phone. The policy that drove the app's capabilities and design focused on scan technology, which uses a technology reading tool that allows officers to view and verify the mDL without needing to hold the resident's phone or even have the phone unlocked.

Despite these strong privacy features, there is continued concern about Louisiana's server-based identity verification. This function allows real-time verification, but it also means that a centralized server is tracking when and where licenses are being verified. Louisiana does not currently regulate how this automatic data collection can be used, which leaves many opportunities for surveillance. Additionally, Louisiana's public-private partnership model could present long-term risks associated with Envoc's data retention policy and future incentives. Data archives of sensitive resident details and use could be vulnerable to a cybersecurity breach. Alternatively, these data could be leveraged in the future for commercial incentives by analyzing or monetizing mDL use patterns.

Key Takeaways for Pennsylvania

Louisiana offers a great example of how strong design and informed policy choices can be made from the outset when considering mDL programs. To date, Louisiana's mDL program has been widely adopted, and it is regarded as privacy aware because of the pairing of the policy with the technology rollout. The no-touch interaction model and selective disclosure features align closely with privacy best practices and public expectations. The following are some key takeaways for Pennsylvania:

- Privacy-preserving mDLs are feasible, but only if functionality is guided by clear values and policy guardrails.
- Legal and technical measures should ensure that server retrieval and tracking functionality are disabled or tightly regulated.

- Training for law enforcement and businesses ensures user-controlled and neutral identity verification processes.
- Public-private partnerships should explicitly explore data collection and retention limitations for real-time verification logs; public reporting requirements help with accountability, ensuring clear guidelines on what resident data are stored, for how long, and by whom.

mDL Highlights and Risks Matrix

Jurisdiction	Highlights	Failures/Risks	Key Takeaways for PA
New South Wales	• Broad rollout and adoption	• Weak encryption through QR code technology • Advanced software expenses are necessary	• Use temporary encrypted tokens that are automatically deleted after each use (ephemeral encrypted) instead of static QR codes
Colorado	• One-stop shop app model • User per-presentation control	• mDL app function creep • Risk of device surrender to law enforcement	• A stand-alone mDL app is needed • Do not allow data sharing across government services
Louisiana	• Widely adopted • Touchless presentation and verification	• Activation of “phone-home” data features	• Do not allow app to track users or send logs of activity back to the state • Policy paired with mDL technology rollout can be successful and increase trust

If you’d like to learn more, see the full project, including a policy brief explaining the fellow’s core recommendations, at aspenpolicyacademy.org/project/mobile-drivers-licenses-2025.

CHUTTERSNAP via Unsplash

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.