

**DEMANDS FOR
PROTECTING
HUMAN DIGNITY
AND CHOICE FROM
DIGITAL
IDENTIFICATION
SYSTEMS**



Without legal and digital guardrails, **digital drivers licenses (dDLs) and the systems used to verify them** are a risk to democracy and freedom. We must grab the wheel from the surveillance state and digital identity industry to steer digital identification systems down a road with guardrails that serve the public.

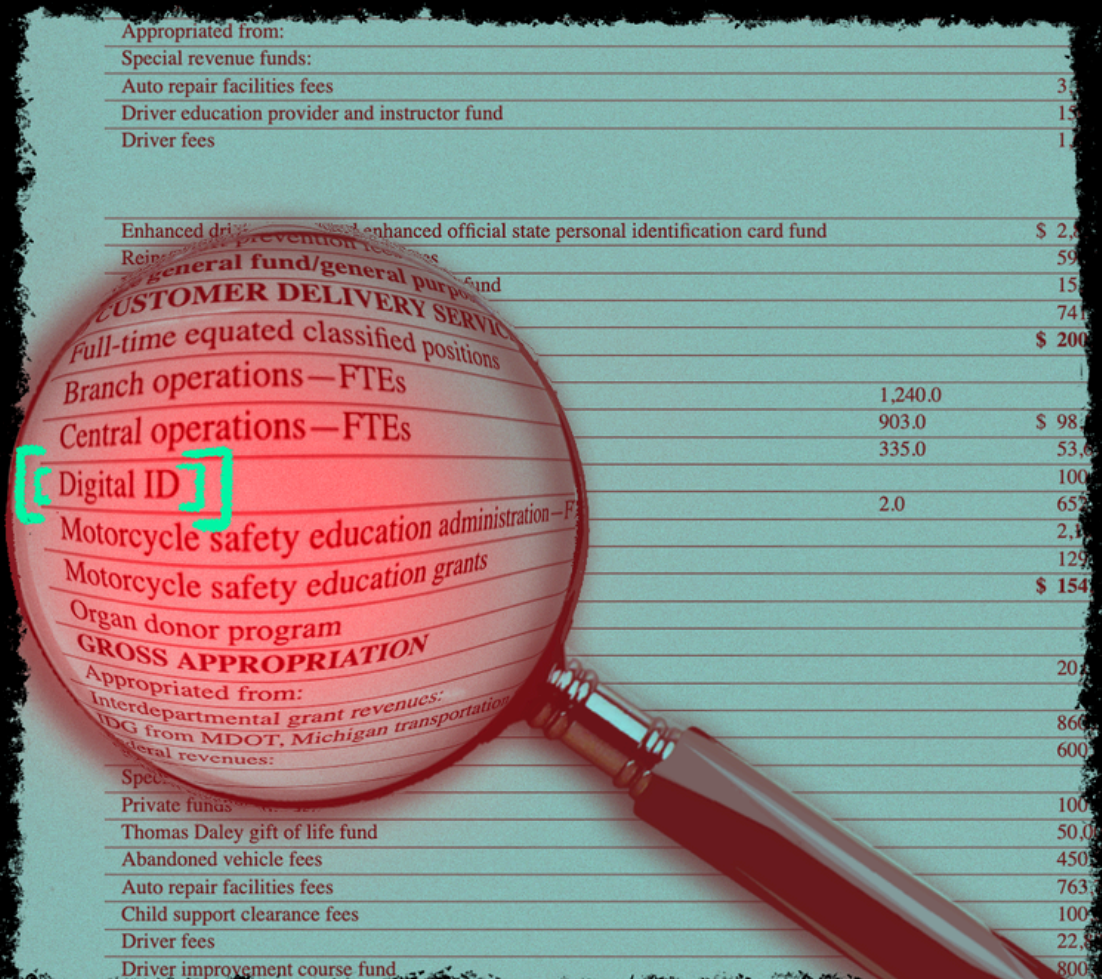


Digital identity systems are transforming how individuals access services, interact with governments, and engage in daily transactions—all with little to zero public debate or legislative guardrails. These systems use data and technology to verify identity, often relying on biometric data (like facial recognition) and other novel verification requirements. While these solutions are sold as a convenience, their growing complexity and reliance on invasive data collection potentially come with a steep cost to privacy, equity, and freedom.

At the moment, digital identity systems are primarily driven by a convergence of interests among state actors, financial and corporate interests, and international institutions.

These interests include surveillance under national security, financial and corporate monetization of personal data and transactions, and global scalability and interoperability.

The actors driving this convergence have circumvented public debate, avoid safeguards to the public interest through legislative guardrails, and overlook or seek to obscure risks to vulnerable members of the public.



Appropriated from:	
Special revenue funds:	
Auto repair facilities fees	35
Driver education provider and instructor fund	15
Driver fees	12
Enhanced driver education enhanced official state personal identification card fund	\$ 2,500
Reimbursement for general fund/general purpose fund	59
CUSTOMER DELIVERY SERVICE	15
Full-time equated classified positions	74
Branch operations — FTEs	\$ 200
Central operations — FTEs	1,240.0
Digital ID	903.0
Motorcycle safety education administration — FTEs	\$ 98
Motorcycle safety education grants	335.0
Organ donor program	53
GROSS APPROPRIATION	100
Appropriated from:	
Interdepartmental grant revenues:	
IDG from MDOT, Michigan transportation	2.0
General revenues:	65
Special revenues:	2,300
Private funds	129
Thomas Daley gift of life fund	\$ 154
Abandoned vehicle fees	20
Auto repair facilities fees	860
Child support clearance fees	600
Driver fees	100
Driver improvement course fund	450

PROTECTING PERSONAL AND DEMOCRATIC CONTROL FOR ID CARDS, CASH, & CLERKS

1

What?

Preserve Physical Cards

Why?

Every individual has the right to a physical form of identification, ensuring that no one is solely dependent on digital identification.

How?

This right guarantees that individuals can always access a physical ID as a backup, and can freely shift between digital and physical forms without penalty or discrimination. Whether transitioning from digital to paper or vice versa, holders should not face barriers or disadvantages in accessing or using either form of identification.

2

What?

Protect Cash

Why?

Every individual has the right to **use cash at any time without penalty or discrimination.**

How?

There should be no cost or added charges for using either digital or physical payment, and no financial incentives or preferential treatment for choosing a digital payment. This ensures cash remains a viable and common payment option.

3

What?

Protect Clerks

Why?

Individuals have the right to interact **in-person with a clerk whether checking out at a store or enrolling** in government services, ensuring equitable access and protecting both workers and communities.

How?

Disincentive stores to replace or reduce staffing based on self-checkout machines by requiring a reasonable ratio of staff to kiosk that would take into account the challenges customers face with self-checkout machines.

4

What?

Protect Data

Why?

Every individual has the right to **control their personal information, including by protecting existing alternatives to REAL ID.**

How?

Individuals must have control over what data they share and with whom they share it, ensuring that only the necessary information is disclosed.

5

What?

Protect Autonomy

Why?

Every individual has the right to **autonomously characterize their identity**, both digitally and physically, allowing for flexibility and adaptability over time.

How?

Autonomous digital identification means that individuals can correct inaccuracies, update outdated information, and change aspects of their identity, such as name, address, race, or gender, as they see fit. This ensures that individuals can express and control their identity freely, without unnecessary barriers beyond what is needed to prevent fraud.

6

What?

Protect from Police

Why?

Every individual must be protected from state actors using digital identities to control access to information online, control travel or internet access, for targeted searches without warrants or for broader surveillance.

How?

No law enforcement officer should be permitted to access a device or personal data without a warrant. Digital ID systems must not be used by state actors to surveil someone's movements, in real life or online.

PROCESS PROTECTIONS

7

What?

Right to Justice

Why?

Every individual shall have the right to legal recourse if their rights under the implementation of Digital ID Systems are violated, addressing harms such as physical, economic, reputational, psychological, autonomy, discrimination, and relationship harms.

How?

Individuals have a private right of action to sue in court for damages, including financial loss, emotional distress, reputational harm, and social determinants, and to recover reasonable attorneys' fees, injunctions, or other relief. For systemic violations, class actions may be pursued to provide collective remedies, ensuring fair compensation for affected groups. State attorneys general shall have the authority to enforce these rights by initiating legal action, conducting investigations, and imposing financial penalties on non-compliant entities, with heightened penalties for repeated violations.

8

What?

Right to Know

Why?

Every individual has the right to full transparency and accountability within Digital Identity systems. These systems must be non-proprietary, auditable, and subject to continuous public scrutiny.

How?

Issuers and verifiers must publicly disclose all processes related to enrollment, verification, and data management, with clear visibility into identity proofing data sources, vendors, and transactions. Transparency must be reinforced by independent third-party audits to ensure continuous verification of the system's integrity and compliance.

9

What?

Right to Democratic Process

Why?

Every individual has the right to engage in the development and oversight of Digital Identity Systems, ensuring they serve the public interest. Currently, these systems are procured through opaque administrative procurement processes that circumvent public debate, opportunities for expertise to be offered, and adversarial testing.

How?

Civic engagement must prioritize marginalized voices, ensuring the system works for all, including vulnerable and immigrant communities. Input can be provided through voting, rulemaking, public consultations, advisory boards, community meetings, and digital platforms. Global perspectives should also be included through international forums and cross-border consultations.