Digital ID or Democracy?

An Advocate's Introduction to the Tech, Politics, and Urgent Demands Needed to Protect Human Dignity

Rebecca Williams and Cynthia Conti-Cook
Surveillance Resistance Lab
at the Collaborative Research Center for Resilience

Contents

Acknowledgments

The authors would like to thank Mizue Aizeki for her leadership, collaboration, research, ongoing thought partnership throughout the development of this report, and Rin Alajaji, Matt Bailey, Molly Buckley, Cade Diehm, Moses Karanja, Alexis Hancock, and Jay Stanley for their substantive feedback, edits, and thought partnership during the drafting process. Finally, the authors would like to thank the many organizations, advocates, researchers, and technologists whose work continues to shape conversations around digital identity, surveillance, privacy, civil liberties, and the ways these systems affect human rights, civil liberties, and social justice. We are especially grateful for colleagues and thought partners across the American Civil Liberties Union (ACLU) and affiliates, the Electronic Frontier Foundation (EFF), Center for Democracy & Technology (CDT), Electronic Privacy Information Center (EPIC), and many more allied organizations and coalitions.

CRCR's Digital ID Origin Story

The Collaborative Research Center for Resilience (CRCR) and a number of its researchers have been engaged in fights to push back against the harms associated with government rollout of digital ID systems for over a decade.

In 2014, New York City, under the leadership of Mayor Bill de Blasio's office, engaged in a collaborative approach to governance, as it set out to develop and implement a new municipal identification program: the IDNYC. The aim of the IDNYC was to provide a safe, accessible, and government-issued ID card for all New Yorkers, including immigrant, homeless, and other populations that often face barriers when attempting to acquire other forms of government-issued identification. The City administration brought together a wide range of advocates whose work was grounded in communities vulnerable to overpolicing–including homeless, formerly incarcerated people, gender non-conforming people, youth, and undocumented immigrants. Advocates came together (later called the NYC Municipal ID Coalition) to advocate for a card designed in the best interest of New Yorkers, including the privacy and security of cardholders. When the IDNYC was issued in 2015, advocates worked closely with the city to enroll community members, assuring people that this card would protect and grant access, rather than becoming a tool of surveillance and additional vulnerability.

A few years later, in May 2018, without consulting with the coalition, the de Blasio administration issued a Request for Expressions of Interest (RFEI) in the "IDNYC Dual Interface Card Payment Initiative." The RFEI was part of a public-private initiative, intended to create an all-in-one digital ID system, connecting formerly distinct City databases–such as medical records, public benefits, and homeless shelter stays–with a transit and financial services feature (through "smartchip" technology).

CRCR's founder Mizue Aizeki (then leading the Surveillance, Technology, and Immigrant Policing project at Immigrant Defense Project), along with the New Economy Project and New York Immigration Coalition, led the Coalition's defeat of this digitization effort. This campaign and how these smart-city systems can expand surveillance, automate decision-making, and

consolidate corporate control over public services are documented in the report *Smart-City Digital ID Projects Reinforcing Inequality and Increasing Surveillance through Corporate "Solutions"*[1] published in December 2021.

Purpose and Scope

This introduction is intended as a resource for advocates, organizers, researchers, policymakers, and members of the public navigating the rapid expansion of digital ID systems at the local, state, and federal levels. Drawing on CRCR's experience organizing around digital ID, surveillance, and co-governance with impacted communities, it examines how digital ID systems are expanding across more areas of life with limited public input and few meaningful guardrails. At its core, this introduction is grounded in the belief that communities should have a meaningful role in shaping whether, where, and how digital ID systems are adopted.

Digital ID systems are not futuristic technologies. They are already embedded throughout public and private life and are evolving far beyond physical ID checks. They include a growing ecosystem of technologies, data infrastructures, and verification systems used to establish, authenticate, infer, monitor, or condition identity and access across digital and physical spaces. Digital ID systems include not only identity credentials such as mobile driver's licenses (mDLs), Login.gov, and ID.me, but also facial recognition technology (FRT), age verification and estimation systems, surveillance pricing systems, biometric systems, persistent login and authentication tools, and the interoperable data infrastructures that connect them. While these technologies are often debated through separate policy and legislative processes, they often operate as part of a shared identity ecosystem and raise many of the same questions about privacy, surveillance, access, discrimination, governance, and power.

In recent years, it has become clear that these various forms of digital ID can no longer be understood in isolation. What began as debates about digitizing physical government ID cards has evolved into a rapidly expanding set of technologies used to identify, authenticate, monitor, and make decisions about people across both online and offline spaces. Physical IDs, digital credentials, facial recognition systems, biometric tools, and data broker information are used interchangeably or in combination to verify identity, determine eligibility, grant access, prevent fraud, or monitor activity in both government and commercial contexts. In online spaces, concerns about fraud and impersonation enabled by artificial intelligence (AI) are accelerating demand for new forms of identity verification, while in offline spaces technologies such as facial recognition continue to expand, in some cases supplementing or replacing physical IDs. Yet many of these decisions are made through technical, administrative, procurement, and legislative processes that can be difficult for the public to access or influence, leaving impacted communities without a meaningful voice in the technical development process.

This introduction is designed to help advocates understand where digital ID systems stand today and why this moment matters. Whether your community is confronting facial recognition

[1] Mizue Aizeki and Rashida Richardson, eds., *Smart-City Digital ID Projects: Reinforcing Inequality and Increasing Surveillance through Corporate "Solutions"*, New York, NY: Immigrant Defense Project, December 2021.

technology, a mDL program, digitized municipal identification, online age verification requirements, surveillance pricing, or another form of digital ID system, this introduction offers a framework for understanding the technology, the power structures behind it, and the urgent need for impacted and overpoliced communities to be centered in shaping how these systems are developed and governed.

Executive Summary

Digital ID systems are often presented as inevitable technological modernization rather than governance systems that the public should have the power to debate, challenge, and shape democratically. Government agencies and lawmakers frequently frame these systems as administrative upgrades or efficiency measures, rather than recognizing that they are constructing new infrastructures that reshape how people access rights, resources, services, and participation in society. Digital ID systems are creating a broader shift in public governance by granting technology vendors and government policing powers even more leverage to undermine impacted communities. Global researchers have warned that digital ID systems are creating a kind of "digital identity event horizon" in which identity verification becomes increasingly embedded across institutions, transactions, and everyday participation, making these systems difficult to meaningfully reverse once normalized.[2]

The Expansion of Digital ID Systems

People are encountering digital ID systems across both online and offline settings, often in ways that operate invisibly in the background. This includes data collected while people visit websites, make purchases, apply for jobs or benefits, enter buildings or events, access healthcare or financial services, cross borders, vote, or simply move through public space. Because digital ID systems can be deployed continuously and at scale, they create strong incentives to expand identity checks into more spaces and contexts. For example, age verification systems increasingly require everyone to verify their age, not just underage users, while also encouraging websites and platforms to gatekeep more content and services than laws may explicitly require.

This introduction examines three dimensions of digital ID systems:

- **The evolution from state documents to digital ID systems** is transforming paper-based identification into interoperable digital infrastructure embedded across institutions.
- **The ways digital ID systems are fundamentally different from physical ID checks** include new opportunities to collect, link, retain, share, and analyze identity information across contexts and over time.

[2] DCade Diehm and Benjamin Royer.*The Digital Identity Event Horizon: A New Design Congress Research Report*, 1st ed. (Berlin: New Design Congress, August 2025), https://newdesigncongress.org/content/files/2025/09/NDC_The_Digital_Identity_Event_Horizon_First_Edition_2025_08_22.pdf.

- **The growing role of corporate vendors in operating digital ID systems** giving private companies influence over how identity is verified, authenticated, and governed.

Who Is Driving Digital ID Systems and Why

Who we are, how we identify ourselves, and when our identity should be tracked, checked, or verified should be self-determined and socially shaped through democratic participation and respect for collective and individual rights. Yet governments and corporations are the primary drivers of digital ID expansion and designers of which attributes, credentials, and qualifications are recognized as evidence of eligibility, trustworthiness, and deservingness in practice. They also reshape which forms of evidence are treated as authoritative, increasingly elevating biometric matches, vendor-generated data, and algorithmic outputs over physical credentials, community testimony, and contextual human judgment.

As identity verification becomes more dependent on proprietary technologies, biometric systems, and interoperable databases, corporations gain leverage not only over public infrastructure, but over the practical administration of identity, citizenship, and belonging itself. Meanwhile, advocates, academics, organizers, and privacy groups are often limited to negotiating safeguards within systems already being built, particularly in the absence of comprehensive privacy protections in the United States.

This introduction maps the key actors driving digital ID systems and the incentives, institutions, and power structures shaping their development:

- **The state is expanding digital ID systems** through surveillance, means testing, fraud prevention efforts, policing, administrative control, and modernization initiatives, often in partnership with private vendors,
- **Big Tech and industry are scaling digital ID systems** through long-term government contracts and licensing programs, technical standards, data collection, interoperability frameworks, and profit incentives.
- **Advocates are pushing privacy safeguards within narrow constraints** through proposals such as selective disclosure, age estimation, and device-based identity frameworks, often within limited political and technical pathways.

Why We Need to Act Now

The visions for digital ID systems have been shaped by institutions and actors that prioritize surveillance, administrative control, efficiency, and market expansion. This is part of a larger trend of communities and elected officials increasingly being sidelined by digital decision-making. Some of the most influential figures in the technology industry have explicitly framed technological infrastructure as a way to circumvent democratic governance altogether. Peter Thiel, the billionaire cofounder of PayPal, an early prototype for many contemporary digital identity and financial verification systems, argued at the 2010 Libertopia conference in San Diego:

> *"We could never win an election on getting certain things because we were in such a small minority, but maybe you could actually unilaterally change the world without having to constantly convince people and beg people and plead with people who are never going to agree with you through technological means, and this is where I think technology is this incredible alternative to politics."*[3]

At the same time, the two decades-long backlash to REAL ID implementation and growing public distrust of Big Tech demonstrate that widespread digital identity expansion, most recently through state-government implementation of mobile drivers' license programs, is not the result of clear democratic demand or debate.

The cost of not publicly debating these developments is high. Establishing identity and access, whether with the state, commercial sector, or social sector, can play an important role in supporting safety, stability, dignity, participation in society, and access to rights and services. While this introduction focuses on the United States, many of the harms facilitated by digital ID systems have already materialized globally and provide important warning signs for U.S. advocates, policymakers and communities.[4] International human rights and development frameworks have increasingly recognized legal identity as critical for accessing healthcare, education, voting, housing, financial systems, and public participation.[5] But digital ID systems are increasingly being developed and implemented in ways that facilitate targeted harms while creating entirely new forms of surveillance, exclusion, gatekeeping, and control. Globally, digital ID systems are already creating more precarity for communities, including the denial of healthcare, housing, or benefits due to documentation barriers, registration failures, or exclusionary verification requirements.[6]

This introduction explains why now is a critical moment to engage communities on digital ID systems:

- **Communities often lack a meaningful seat at the table in digital ID decisions** despite growing public concern about surveillance technologies, leaving society to sleepwalk into digital identity infrastructure without meaningful input on who it affects or how it is governed.
- **This is a critical moment for action** as digital ID systems are adopted and are normalized faster than democratic institutions can evaluate, govern, or or meaningfully regulate them, potentially locking us into harmful architectural decisions.
- **Digital ID systems are already contributing to demonstrable harms** by deepening corporate capture of governance,[7] expanding conditional access to public

[3] Edsall, Thomas B. "'Surveil, Govern and Control': What Could Go Wrong?", *The New York Times,* Mar. 17, 2026, https://www.nytimes.com/2026/03/17/opinion/ai-economy-trump-future.html
[4] DiResta, CJ Larkin, Renée. "Lessons from National Digital ID Systems for Privacy, Security, and Trust in the AI Age." Tech Policy Press, June 25, 2025. https://techpolicy.press/lessons-from-national-digital-id-systems-for-privacy-security-and-trust-in-the-ai-age.
[5] *UN Sustainable Development Goal 16.9.* June 29, 2023. https://sdg16now.org/report/target16-9/, https://www.sdg16now.org/report/target16-9/.
[6] Baker, Sara and Rahman, Zara. "Understanding the Lived Effects of Digital ID: A Multi-Country Study." The Engine Room, January 2020. https://digitalid.theengineroom.org.
[7] "IRS Awards ID.Me $1B Agreement." *GovCon Wire*, January 6, 2026. https://www.govconwire.com/articles/idme-bpa-irs-award-digital-identity.

goods and criminalization,[8] chilling free expression and deterring democratic participation[9] , discriminating against targeted communities[10], and exposing sensitive information and privacy.[11]

What We Must Demand

It is not too late to challenge the expansion of digital ID systems and build on organizing that prioritizes dignity, privacy, accessibility, and community safety over surveillance and exclusion. Campaigns like Drivers License for All[12] demonstrated that identity systems can be designed to support immigrant communities while minimizing unnecessary data collection and exposure to policing.

States still retain significant authority over how digital ID systems are implemented, including whether people can access in-person public services, maintain access to physical credentials, and receive protections against surveillance, excessive data collection, and corporate misuse. Yet only two states have enacted significant legislative guardrails while a small number of states have enacted narrower piecemeal protections.[13]

Identity should not be treated merely as a technical or administrative problem to be optimized, tracked, or monetized, but as a deeply personal and socially situated aspect of human autonomy that cannot be fully reduced to interoperable data flows, behavioral profiles, or risk scores.

To protect dignity, human rights, and democracy, communities, advocates, and policymakers must:

- **Resist national digital ID systems by** blocking the expansion of surveillance infrastructure; preserving meaningful human and physical alternatives; and unwinding digital ID systems where possible.
- **Protect dignity, human rights, and democracy** by prioritizing democratic participation, free expression and association, privacy, self-determination, equity, access to justice, transparency, and accountability.
- **Rethink identity systems and their role in governance** by questioning when ID checks are necessary at all, addressing harms through structural and collective interventions rather than individualized surveillance, and ensuring that any remaining

[8] Rein, Lisa, Natanson, Hannah, and Sacchetti, Maria. "Social Security classifies thousands of immigrants as dead, as part of Trump crackdown" Washington Post, April 10, 2025. https://www.washingtonpost.com/politics/2025/04/10/self-deportation-immigrants-social-security-dead/.
[9] Cynthia Conti-Cook,, Pratika Katiyar, and Rebecca Williams. "Who Age Verification Laws Really Benefit & How to Resist" Aug 25, 2025, User Mag. https://www.usermag.co/p/we-must-fight-age-verification-with.
[10] Ryan Thoreson, US State Revokes Gender-Affirming Identification | Human Rights Watch. March 3, 2026. https://www.hrw.org/news/2026/03/03/us-state-revokes-gender-affirming-identification.
[11] Maiberg, Emanuel, and Joseph Cox. "Women Dating Safety App 'Tea' Breached, Users' IDs Posted to 4chan." 404 Media, July 25, 2025. https://www.404media.co/women-dating-safety-app-tea-breached-users-ids-posted-to-4chan/.
[12] "Driver Licenses For All." *Voces de La Frontera*, n.d. Accessed May 17, 2026. https://vdlf.org/driver-licenses-for-all/.
[13] See Section II "The State Expands Digital Identity Through Surveillance and Means Testing" for a detailed discussion.

identity systems are paired with meaningful, well-resourced protections for dignity, human rights, and democracy.

I. The Expansion of Digital ID Systems

From State Documents to Digital ID Systems

State-issued forms of identification have long been tied to efforts to classify populations, regulate movement, and determine who is recognized, protected, or excluded. Across different historical periods and regions, governments developed passports, population records, and identification documents to manage mobility, taxation, and policing. By the nineteenth century, British policing systems increasingly relied on identification numbers and population records to support surveillance and administration.[14] For much of modern history, however, these practices remained relatively localized and paper-based, relying on physical documents and human judgement rather than continuous technical verification.[15]

A combination of policy choices and expanding computational power transformed these paper-based state documentation systems into increasingly interoperable digital infrastructures. In the United States, federal digital ID systems emerged from post-9/11 security reforms and Clinton-era welfare-policing, combined with advances in computation which made it possible to store, link, and analyze massive quantities of data. Laws such as the USA PATRIOT Act and the REAL ID Act of 2005, which set federal standards for state-issued IDs,[16] helped normalize expanded identity checks, while creating nationwide databases of identifying information. States that refused to follow these specifications risked producing IDs that federal facilities and commercial airlines would not accept. In 2020, Congress passed the REAL ID Modernization Act that extended federal control over state-issued identity systems to digital identification systems. REAL ID functioned as a political compromise to longstanding public opposition against a centralized national ID system: rather than creating a single federal database outright, it used federal standards and interoperable data-sharing requirements to produce many of the same outcomes through state systems.

[14] In 2026, the United Kingdom's King Charles announced plans to advance digital ID systems and 'trusted digital verification services' as part of broader 'modernization' and economic policy efforts. ComputerWeekly.Com. "King's Speech Paves the Way for Digital ID | Computer Weekly." Accessed May 18, 2026. https://www.computerweekly.com/news/366643097/Kings-Speech-paves-the-way-for-digital-ID.
[15] Simone Browne further traces how identification practices have long been weaponized against communities targeted by systems of oppression, drawing connections between slave passes, lantern laws, and the modern surveillance of Black communities through biometric technologies and facial recognition systems. Browne, Simone. *Dark Matters: On the Surveillance of Blackness*. Duke University Press, 2015.
[16] NILC, "The REAL ID Act: Questions and Answers", *NILC*, last updated July 2021 https://media.nilc.org/wp-content/uploads/2015/11/REAL-ID-Act-Q-and-A.pdf

How Digital ID Systems Are Fundamentally Different from Physical ID Checks

It is important that policymakers and advocates understand that physical ID checks are not the same as digital ID systems. Digital ID is often framed as a simple modernization step, shifting offline identification into a more convenient online format, but the functions of the underlying systems operate fundamentally differently. The modernization argument obscures the dangerous new capabilities of digital ID systems.

A physical ID check is usually a limited interaction between two people: a credential is presented, visually verified, and the interaction generally ends there. Digital ID systems, by contrast, often rely on persistent identifiers, continuous authentication, and multiple layers of data collection to confirm that someone is who they claim to be. Because these systems are digital and interoperable, they have the capacity to aggregate, retain, infer, and share information across contexts over time unless explicitly limited by law or technical design. As a result, proposals such as mDLs represent more than a format change from physical to digital credentials. They mark a shift from relatively discrete, context-bound identity checks toward interoperable digital systems capable of expanding across institutions and services, enabling far more extensive surveillance, monitoring, gatekeeping, and behavioral profiling over time. Unlike physical ID checks, which are often limited to a narrow context and purpose, digital ID systems are designed to scale across contexts, allowing more frequent checks and for personal data collected in one setting to be linked, reused, or repurposed across other systems over time.

The design term “affordance” refers to the actions a technology makes possible or encourages. As discussed above, digital ID systems’ affordances fuel expanded data collection, from biometrics to behavioral patterns, creating systems that are not only vulnerable to spoofing and misidentification but also facilitate new forms of surveillance, behavioral profiling, access control, and gatekeeping, in which access to services, spaces, opportunities, and democratic participation is increasingly conditioned on identity verification, behavioral monitoring, or algorithmic assessment. As corporate vendors become the stewards of the technologies and data used to verify and govern identity, they are also beginning to scale forms of power historically exercised almost exclusively by governments.

The chart on the next page compares physical IDs with digital ID systems and highlights how these systems differ in enrollment, verification, authentication, authorization, and how these changes impact the underlying processes and the broader societal implications.

Physical IDs vs. Digital ID Systems				
Actor	**Activity**	**Physical IDs**	**Digital ID Systems**	**Key Shift**
Issuer *Issues IDs*	**Registration/ Enrollment** *Signing up*	Conducted in person by government employees using government-issued identity documents and proof of residency, (e.g., birth certificates, Social Security cards, utility bills, etc.)	Conducted online using scanned documents, biometrics, and government and commercial data sources.	Enrollment shifts from in-person submission of physical documents to online collection of digital identity information, expanding the role of corporate actors and the number of systems involved in identity verification.
	Identity Verification *Confirming it's you*	Identity is typically verified by a human reviewing documents and comparing photographs to the individual presenting them in person.	Identity is verified through automated document review, biometric matching, liveness checks, and comparisons against government and commercial data sources, including phone numbers, email addresses, and device information.	Verification shifts from human review of a person and a few documents to automated matching across biometrics, devices, and government and commercial databases, increasing opportunities for surveillance, error, and exclusion.
	Credential Creation *Issuing an ID*	Physical credential with embedded security features, such as holograms, barcodes, and watermarks.	Digital credentials are derived from identity records and stored as digital or cryptographic credentials that can be used across multiple systems and services.	Credentials shift from relatively static physical cards to interoperable digital records that can be linked to additional data, attributes, and services over time.
Verifier *Checks IDs*	**Authentication** *Checking an ID*	A human checks whether a credential appears genuine by comparing a photograph to the person presenting it and inspecting security features such as holograms or watermarks.	Authentication relies on passwords, biometrics, cryptographic verification, devices, and other technical mechanisms to confirm the credential or user.	Authentication shifts from human inspection of a credential to automated validation through devices, biometrics, and technical systems, making identity checks easier to scale and repeat.
	Authorization *Granting access*	Access is typically granted by a human reviewing limited information presented on a credential, such as age, identity, residency status, or reputation[17].	**Credential-based authorization:** Access is granted by validating a credential issued by a trusted authority (e.g., a government ID or verified account). **Inference-based authorization:** Access is granted based on estimated attributes, eligibility determinations, or risk scores rather than a specific credential (e.g., age assurance).	Authorization shifts from human review of limited information to automated decisions based on credentials, inferred attributes, and aggregated data.

[17] Carollo, Malena. "ID Scanners Can Change How Your Local Bar Treats You—and Whether It Lets You In – The Markup." July 27, 2024. https://themarkup.org/2024/07/27/id-scanners-can-change-how-your-local-bar-treats-you-and-whether-it-lets-you-in.

Corporate Vendors Operate Digital ID Systems

While government IDs were historically maintained through state-issued documents and government record-keeping, other forms of personal identification have long existed across religious, social, and commercial contexts. States historically exercised primary authority over what counted as legal identity through government-issued documents and public record-keeping systems.[18] Advances in computing, expanding technical capacities for data collection and analysis, and growing profit incentives expanded opportunities for private corporations in mediating, verifying, scoring, and operationalizing identity for governments.[19] These developments justified investment, experimentation, and scaling of credit bureaus, predictive policing systems, fraud detection tools, biometrics, and other data-driven infrastructures that transformed identity from a relatively static credential into a continuously monitored and algorithmically evaluated profile.[20]

Today, identity vendors, including companies that work directly with state Department of Motor Vehicles (DMVs) to service digital ID systems, play a central role in determining how identity is authenticated, shared, and governed. For example, state mDL programs are often implemented through vendors such as IDEMIA and Thales and rely on credentials being stored and presented through Apple Wallet, Google Wallet, and Samsung Wallet. State and federal agencies also increasingly rely on ID.me , which is used across a range of government services, including by the IRS. Even when identity verification appears to be conducted directly against government records, the underlying infrastructure frequently depends on private vendors and commercial data sources. For example, Login.gov relies on corporate vendors, including LexisNexis, Experian, TransUnion, IDEMIA, Adreas, Diamond Capture, and Carashsoft[21], while TSA PreCheck enrollment has been administered through corporations such as CLEAR, IDEMIA, and Telos. As these corporations appear across state and federal initiatives, they increasingly function as de facto infrastructure providers. These vendors shape identity practices and standards across jurisdictions, enabling interoperability with commercial systems while creating new pathways for the sharing and secondary use of personal data.

Interoperability, or the ability for different data systems to easily share information with one another, facilitates systems such as surveillance pricing, where identity verification, transaction histories, behavioral analytics, and payment systems work together to carry out individualized pricing and automated decision-making. As a result, interoperability is not merely a technical feature but a political and economic one, shaping who can access, monetize, and govern flows of identity-linked data across sectors.

---

[18] Ecclesiastical documents such as baptismal records, for example, could function as forms of identification, but states largely determined which credentials carried legal recognition and authority.
[19] David Burnham, *The Rise of the Computer State: The Rise of the Computer State: The Threat to Our Freedoms, Our Ethics and Our Democratic Process,* Random House Publishers, (1983), 63-69.
[20] "Anthropotelemetry: Dr. Schwitzgebel's Machine." *Harvard Law Review* 80, no. 2 (1966): 409.
[21] "GSA Selects 8 Vendors for $195M Login.Gov Next-Gen Identity Proofing BPA." *GovCon Wire*, March 18, 2024. https://www.govconwire.com/articles/gsa-selects-8-vendors-for-195m-login-gov-next-gen-identity-proofing-bpa.

II. Who Is Driving Digital ID Systems and Why

The State Expands Digital ID Through Surveillance and Means Testing

In the United States, digital ID systems are being shaped through disparate and sometimes overlapping laws, agencies, procurement systems, and technical standards that collectively expand surveillance, fraud prevention systems, and means testing. Means testing refers to systems that determine whether a person qualifies for services, benefits, or rights based on income, assets, immigration status, disability status, household composition, or other personal criteria.[22] These systems are not emerging from a single national digital ID law or coherent democratic process. Instead, a wide range of sectors including immigration, banking, transportation, telecommunications, public benefits, employment, border security, online speech, and consumer protection have each developed their own identity verification requirements, administrative systems, and data-sharing practices over time.[23] Different agencies and industries often operate with different incentives and authorities, yet their systems increasingly converge through digital ID systems designed to be interoperable.[24]

This pattern has developed incrementally over decades. After 9/11, Congress and the Executive Branch created the Department of Homeland Security (DHS) and a new set of authorities that normalized identity checks across borders, airports, workplaces, and public programs. REAL ID gave DHS the practical ability to standardize driver's licenses and identity infrastructure and data across all states, transforming licenses originally intended for driving into de facto national identity documents.[25] The State Pointer Exchange Services (SPEXS) database, as analyzed by Papers Please[26], further linked state driver's license systems into a national identity infrastructure, even though Congress never openly debated creating one.[27] Financial identity

[22] Luke Farrell, The Means-Testing Industrial Complex." January 28, 2026, LPE Project. https://lpeproject.org/blog/the-means-testing-industrial-complex/.
[23] Ayang MacDonald, "Digital identity must be built for interoperability from day one, says Margins CEO", *Biometric Update*, June 1. 2026, https://www.biometricupdate.com/202606/digital-identity-must-be-built-for-interoperability-from-day-one-says-margins-ceo
[24] Id.
[25] Surveillance Resistance Lab and National Immigration Law Center, "Mobile Driver's Licenses and the Costs To Privacy, Safety, and Security" *The CRCR*, January 2024, https://thecrcr.org/wp-content/uploads/Mobile-Drivers-Licenses-and-the-Costs-to-Privacy-Safety-Security-2023.pdf
[26] Ed Hasbrouck, "How the REAL-ID Act is creating a national ID database", Papers, please. Feb. 11, 2016, https://papersplease.org/wp/2016/02/11/how-the-real-id-act-is-creating-a-national-id-database/
[27] And despite the concerns about record accuracy, potential harm, and centralization of power raised by the LEAA itself in the late 1960s when federal databases of criminal records were being debated. David Burnham, *The Rise of the Computer State: The Rise of the Computer State: The Threat to Our Freedoms, Our Ethics and Our Democratic Process,* Random House Publishers, (1983) 69.

laws such as the Bank Secrecy Act[28], Gramm-Leach-Bliley[29], anti-money laundering rules[30], and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act[31] built a parallel regime requiring banks and private institutions to verify identity on behalf of the state. Other laws including the Driver's Privacy Protection Act[32], the Fair Credit Reporting Act[33], and the Identity Theft Enforcement and Restitution Act[34] expanded the collection, retention, and exchange of identity-linked information in the name of safety, fraud prevention, and consumer protection. Agencies such as DHS, Social Security Administration (SSA), DMVs, U.S. Citizenship and Immigration Services (USCIS), the Internal Revenue Service (IRS), and (United States Postal Service) USPS now administer overlapping identity systems with different purposes and incentives, while identity standards from National Institute of Standards and Technology (NIST) increasingly translate those assumptions into technical rules governing the broader marketplace and ensuring ever greater interoperability of these systems over time by default.[35]

More recent laws frame digital identity expansion as "modernization," cybersecurity, or administrative efficiency rather than as major structural changes to public governance. Federal laws such as the REAL ID Modernization Act (2020)[36], the CHIPS Act (2022)[37], and the GSA Technology Accountability Act (2024)[38] have delegated substantial authority to agencies such as DHS, General Services Administration (GSA), and NIST to build and expand digital identity infrastructure, including Login.gov and related verification systems, often through appropriations bills and industrial policy legislation receiving limited public scrutiny.

At the state and local level, governments are similarly expanding mDL programs,[39] through several legislative and administrative mechanisms. Some jurisdictions have advanced mDL programs through appropriations legislation, including budget provisions funding, authorizing, or expanding pilot programs (California, Hawaii, and Vermont).[40] Others have incorporated mDL provisions into existing motor vehicle, driver's license, identification, or transportation statutes, treating digital credentials as extensions of existing administrative frameworks rather than creating a new digital identity framework (Arkansas, Colorado, Idaho, Illinois, Indiana,

---

[28] Financial Crimes Enforcement Network, "Bank Secrecy Act," FinCEN.gov, accessed June 7, 2026, https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act
[29] Federal Trade Commission, "Gramm-Leach-Bliley Act," accessed June 7, 2026,https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act
[30] Federal Deposit Insurance Corporation, "Anti-Money Laundering / Countering the Financing of Terrorism (AML/CFT)," accessed June 7, 2026, https://www.fdic.gov/banker-resource-center/anti-money-laundering-countering-financing-terrorism-amlcft
[31] "USA PATRIOT Act", FinCEN.gov, https://www.fincen.gov/resources/statutes-and-regulations/usa-patriot-act
[32] H.R.3365 - 103rd Congress (1993-1994): Driver's Privacy Protection Act of 1993.
[33] Fair Credit Reporting Act | Federal Trade Commission.
[34] H.R.6060 - 110th Congress (2007-2008): Identity Theft Enforcement and Restitution Act of 2008.
[35] NIST, "NIST SP 800-63 Digital Identity Guidelines", July 2025, https://pages.nist.gov/800-63-4/
[36] S. Rept. 116-303 - REAL ID MODERNIZATION ACT.
[37] H.R.4346 - 117th Congress (2021-2022): CHIPS and Science Act.
[38] H.R.7524 - 118th Congress (2023-2024): GSA Technology Accountability Act.
[39] CRCR, "Toolkit for Navigating Your State's Digital ID System"
[40] California, *Budget Act of 2021*, AB 149 (establishing mDL pilot authority); California, SB 125 (2023) (expanding the pilot); Hawaii, appropriations legislation funding mDL pilot activity (2023); Vermont, appropriations legislation funding mDL pilot activity (2023–2024).

Louisiana, Montana, Utah, Vermont, Washington, and the District of Columbia).[41] A smaller number of jurisdictions have considered or enacted dedicated digital ID legislation, including mDL legislation, creating a more direct vehicle for legislative debate about digital ID systems (Massachusetts, New Jersey, and New Mexico).[42] Some jurisdictions have also launched mDL programs through agency implementation, pilot programs, or vendor partnerships, demonstrating that digital ID infrastructure can sometimes advance through administrative processes and receive less public scrutiny than dedicated legislative debates (Alaska, Iowa, Maryland, Mississippi, Missouri, and New York)[43].

Yet only New Jersey[44] and Utah[45] have enacted significant legislative guardrails on mDL systems. Outside of those laws, protections are typically narrower and more fragmented. A small number of states have enacted discrete protections, including preserving physical identity cards and preventing the denial of services for not using a digital ID (Idaho),[46] and clarifying that displaying a digital or electronic credential does not constitute consent to a search (Idaho and Montana).[47] As of this writing, other states have considered similar or additional safeguards, including preserving physical IDs (West Virginia),[48] protections against law-enforcement access to biometric data (Illinois),[49] consent requirements and private rights of action (Missouri),[50] protections against denial of government services for individuals who do not use digital identification (Oklahoma),[51] and privacy protections for mobile identification systems (South Dakota and Vermont),[52] but these efforts remain piecemeal and uneven.[53]

Mobile drivers license legislation represents only one part of the broader digital ID legislative landscape. States are also advancing digital ID systems through age-verification laws[54], which

---

[41] Arkansas, HB 1506 (2019); Arkansas, HB 1135 (2025); Colorado, *Motor Vehicle Regulation Administration*, HB 25-1076 (2025); Idaho, HB 519 (2023); Idaho, HB 196 (2025); Idaho, HB 124 (2025); Illinois, HB 4592 (2024); Indiana, digital credential legislation amending existing motor vehicle law; Louisiana, SB 204 (2021); Montana, HB 519 (2023); Utah, *Mobile Driver License Amendments*, HB 5 (2020); Vermont, S.99 (2023); Washington, HB 2229 (2017); District of Columbia, B24-0043 (2021).

[42] Massachusetts, *An Act Relative to Mobile Driver's Licenses*, H.23; Massachusetts, *An Act Relative to Mobile Driver's Licenses*, S.1299; Massachusetts, *An Act Relative to Mobile Driver's Licenses*, H.4592; Massachusetts, *An Act Relative to Mobile Driver's Licenses*, H.1110; New Jersey, A.3518 / S.1297, *Requires MVC to Create Digital Driver's Licenses and Digital Non-Driver Identification Cards* (enacted 2025); New Mexico, SB 88 (2024).

[43] Alaska DMV mID program; Iowa Mobile ID; Maryland Mobile ID; Mississippi Mobile ID; Missouri Mobile ID; New York MiD

[44] New Jersey A. 3518, An Act Creating Digital Driver's Licenses and Digital Non-Driver Identification Cards (2025).

[45] Utah S.B. 275, State-Endorsed Digital Identity Program Amendments (2026).

[46] Idaho S. 1299, Adds to Existing Law to Establish Provisions Regarding Limitations on Digital Identification (2026)

[47] Idaho S. 1299, Adds to Existing Law to Establish Provisions Regarding Limitations on Digital Identification (2026), Montana S.B. 124, An Act Revising Electronic License Privacy Law (2025

[48]West Virginia H.B. 5551, Protecting State Licensing Act (2026)

[49] Illinois H.B. 5521, Illinois Biometric Surveillance Act (2025)

[50]Missouri S.B. 921, Creates New Provisions Relating to Digital Forms of Identification (2026).

[51] Oklahoma S.B. 1231, Digital Identification (2026)

[52] South Dakota H.B. 1211, An Act to establish requirements for the use of a mDL (2025); Vermont H.360, An Act Relating to Vermont's Data Privacy and Online Surveillance Act (2025); Vermont S.150, An Act Relating to Privacy Protections for Mobile Identification and Images Recorded by Automated Traffic Law Enforcement Systems (2025).

[53] CRCR hosts a toolkit and a spreadsheet for navigating what digital ID administrative action or legislation each state has. See "Toolkit for Navigating Your State's Digital ID System" https://thecrcr.org/wp-content/uploads/Toolkit-for-Navigating-Your-States-Digital-ID-System_Print.pdf and "Digital ID Systems - Policies, Tech, Uses, Protections" https://docs.google.com/spreadsheets/d/1EKzZqsLUG_r_H7lby06US4aURRl7-r4D0ixdgq4p-2g/edit?gid=1286523486#gid=1286523486 (updated May 2026).

[54] Free Speech Coalition, "Action Center," accessed June 7, 2026, https://action.freespeechcoalition.com.

may rely on various digital ID systems and are presenting novel harms. At the same time, some states have adopted partial safeguards through consumer privacy laws[55], biometric privacy statutes, and restrictions on surveillance pricing, but these protections generally address specific harms rather than providing a comprehensive framework for governing digital ID systems.

Globally, large-scale governance frameworks such as the European Union's revised eIDAS regulation are further institutionalizing interoperable digital identity infrastructure through technical and regulatory standards for cross-border digital ID systems and digital identity wallets.[56] Still, much of the current policy landscape treats digital identity expansion as an inevitable modernization of existing systems rather than presenting meaningful alternatives that minimize surveillance, preserve anonymity, or reduce dependency on centralized identity verification.

Participation in digital ID systems is also becoming increasingly coercive. In 2025, Transportation Security Administration (TSA) announced a fee-based 'alternative identity verification' program requiring travelers without REAL ID-compliant identification to pay for additional biometric and biographic screening in order to travel, effectively imposing financial penalties on people who do not participate in the preferred identity infrastructure.[57] This reflects a broader shift in which physical credentials and anonymous or low-data forms of access are at risk of not being treated as equal alternatives, but as deviations requiring additional scrutiny, friction, or cost. Framed as modernization, efficiency, fraud prevention, or administrative convenience, these systems increasingly condition access on participation in interoperable digital ID systems.

Big Tech and Industry Scale Digital ID for Profit

Big Tech companies, identity verification vendors, trade associations, and private technical standards bodies are increasingly shaping digital ID systems. Their incentives differ from the public interest. For technology and identity verification companies, more identity checks mean more data collection, more authentication services, more behavioral analytics, and more opportunities to build profitable identity-linked products. Corporate actors have become deeply embedded in the design, deployment, and governance of digital ID systems. These companies originate from sectors including consumer technology, banking, telecommunications, fraud prevention, biometrics, border security, credit reporting, and financial compliance, but largely share the same incentive: profit through expansion of identity verification, interoperability, and identity-linked data collection.

- **Big Tech platforms, devices, and wallets:** Companies such as Apple, Google, Samsung, Amazon, and Microsoft increasingly bind identity verification directly to

[55] International Association of Privacy Professionals (IAPP), "US State Privacy Legislation Tracker," accessed June 7, 2026, https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.
[56] eIDAS Regulation | Shaping Europe's digital future, https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation
[57] *Federal Register*, "TSA Modernized Alternative Identity Verification User Fee," November 20, 2025,https://www.federalregister.gov/documents/2025/11/20/2025-20474/tsa-modernized-alternative-identity-verification-user-fee.

consumer and government platforms, devices, wallets, cloud systems, and mobile ecosystems, extending existing control over user accounts, devices, and digital behavior into persistent identity infrastructure capable of linking credentials, devices, and activity across contexts.[58]

- **Legacy credit bureaus and financial compliance companies:** Companies such as LexisNexis, Experian, Equifax, and TransUnion increasingly expand from credit reporting and financial compliance into behavioral analytics, device intelligence, authentication services, and risk scoring systems tied to anti-money laundering (AML) and know-your-customer (KYC) compliance regimes.[59]
- **Emerging identity verification and biometric vendors:** Companies such as ID.me, Jumio, Yoti, Clear, Veriff, Socure, AU10TIX, iProov, Onfido, and IDEMIA increasingly provide governments and corporations with facial recognition, liveness detection, document verification, fraud scoring, remote identity proofing systems, airport screening systems, and mDL infrastructure.[60]
- **Emerging generative AI threat and solution markets:** Sam Altman is both a leading vendor of generative AI tools that enable fraud, bots, deepfakes, and synthetic accounts and a board member of World, which markets digital ID systems[61] as a necessary response to those same problems. World explicitly frames anonymity online as a threat to trust and safety, positioning persistent identity verification as the solution to the harms created by increasingly automated and synthetic online environments.[62]

Trade associations, lobbying groups, and industry coalitions also play a major role in expanding digital ID systems globally. Organizations such as the Better Identity Coalition openly advocate for expanded digital identity infrastructure and interoperability standards while framing these efforts as necessary for modernization, fraud prevention, child safety, and online trust.[63] Industry-backed campaigns have increasingly pushed mandatory identity verification requirements across social media, app stores, and online platforms, creating new commercial demand for biometric and identity verification services.[64]

---

[58] Dan Yerushalmi, "Is The Future Of Identity Verification Tied To Digital Wallets?" Forbes.com, Nov. 25, 2024, https://www.forbes.com/councils/forbestechcouncil/2024/11/25/is-the-future-of-identity-verification-tied-to-digital-wallets/

[59] "The Rise of US Identity Verification Market: A $21.8 billion Industry Dominated by Tech Giants - LexisNexis Risk Solutions, Equifax, and TransUnion, MarketsandMarkets, Apr. 7, 2025, https://www.globenewswire.com/news-release/2025/04/07/3056875/0/en/The-Rise-of-US-Identity-Verification-Market-A-21-8-billion-Industry-Dominated-by-Tech-Giants-LexisNexis-Risk-Solutions-Equifax-and-TransUnion-MarketsandMarkets.html

[60] "Digital Identification," *Biometric Update*, accessed May 18, 2026, https://www.biometricupdate.com/service-directory/digital-identification

[61] Ropek, Lucas. "Sam Altman's Project World Looks to Scale Its Human Verification Empire. First Stop: Tinder." *TechCrunch*, April 17, 2026. https://techcrunch.com/2026/04/17/sam-altmans-project-world-looks-to-scale-its-human-verification-empire-first-stop-tinder

[62] World ID, https://world.org/world-id

[63] Masha Borak, , "Better Identity Coalition wants to provide the US with rules for verifiable credentials", *Biometric Update*, Feb., 2, 2026. https://www.biometricupdate.com/202602/better-identity-coalition-wants-to-provide-u-s-with-rules-for-verifiable-credentials

[64] C. da Costa, "Reddit User Uncovers Who Is Behind Meta's $2B Lobbying for Invasive Age Verification Tech," *Gadget Review*, March 16, 2026, https://www.gadgetreview.com/reddit-user-uncovers-who-is-behind-metas-2b-lobbying-for-invasive-age-verification-tech

Conference and trade associations, such as Identity Week[65] and the Border Technology Summit, convene corporations, border security agencies, law enforcement officials, and government procurement actors to accelerate deployment of biometric surveillance, border technologies, and digital identity infrastructure globally. These lobbying and trade ecosystems normalize the assumption that more identity verification, more biometric collection, and more continuous authentication are inevitable responses to fraud, safety, migration, and platform governance challenges.

Technical standards bodies such as International Organization for Standardization (ISO), World Wide Web Consortium (W3C), and the stewarding organizations behind OAuth, OpenID Connect, and Fast Identity Online 2 (FIDO2) convert the assumptions of governments, vendors, and industry coalitions into the technical rules that govern how identity data moves across systems.[66] Even privacy-oriented protocols like Verifiable Credentials are shaped by debates over interoperability, wallet design, revocation, telemetry, and continuous authentication.[67]

Through corporate mergers and acquisitions, data sharing and interoperability agreements, sole-source procurement, licensing, master service agreements, and industry standardization of government technologies, corporations are centralizing control over the infrastructure underlying digital ID systems. As a result, corporate mergers can suddenly influence public systems in ways that implicate security and public safety. For example, in the Netherlands, the national digital ID system is "used by Dutch citizens to access government services, such as health insurance, pension funds, municipal services and tax."[68] When the Dutch vendor who held citizens' data and has been performing the country's digital identity services was narrowly outbid by a U.S. based corporation, the corporate merger raised national security concerns. Concerned about the state of geopolitics between Europe and the U.S., Dutch lawmakers convened a task force to determine whether to block the U.S. vendor's acquisition of sensitive Dutch residential data and control over their services.[69]

Fear of generative AI spoofing tools[70] have justified even more invasive identity verification systems and data collection requirements in a self-reinforcing cycle. At the same time, state prosecutors have treated engaging services to protect oneself against invasive data collection, such as using encrypted communication services and virtual private networks (VPNs) as suspicious behavior.[71] Even the absence of information, for example, something as intimate as

[65] "Identity Week" expos and panels with commercial and government leaders are organized by Terrapinn, https://www.terrapinn.com/exhibition/identity-week-america/our-story.stm
[66] "A Global First: OpenID Foundation Demonstrates Real-World Interoperability of New Digital Identity Standards," *OpenID Foundation*, May 28, 2025.
https://openid.net/openid-foundation-demonstrates-real-world-interoperabiity-of-new-digital-identity-standards/
[67] "What are Verifiable Credentials and how do they work?", *One Identity,*
https://www.oneidentity.com/learn/what-are-verifiable-credentials-in-cybersecurity.aspx
[68] Masha Borak, . "US bid for Dutch digital ID infrastructure company raises national security fears", Biometric Update, Jan. 26, 2026.
[69] Id.
[70] Subharup Das Sharma. "After Ghibli Madness, ChatGPT Users Go on Overdrive with Deepfake Aadhaar Cards." *Telegraph India,*
https://www.telegraphindia.com/india/after-ghibli-madness-chatgpt-users-go-on-overdrive-with-deepfake-aadhaar-cards/cid/2092480.
[71] Sam Levine. "Inside DOJ's controversial prosecution of a Texas 'antifa cell' charged with terrorism," *The Guardian,* Dec. 18, 2025, https://www.theguardian.com/us-news/2025/dec/18/texas-antifa-ice-detention-center

hiding a pregnancy online, can create the perception of evasiveness, casting ordinary privacy choices as suspicious.[72]

Lastly, digital ID systems are being expanded as critical components of other emerging commercial technologies, creating unforeseeable harms with few mechanisms for legal recourse. Generative and agentic AI systems already are being granted credentials and permissions once reserved only for people. These pressures are likely to intensify as AI systems become more deeply integrated with digital identity infrastructures. Increasing concerns about bots, synthetic media, and automated fraud are already being used to justify broader identity verification requirements and more invasive forms of data collection.[73] As more identity data is collected in response to spoofing and AI-generated fraud, digital ID systems risk deepening the same cycle of surveillance, insecurity, and data extraction they claim to solve.[74]

Advocates Push Privacy Safeguards Within Narrow Constraints

Civil society organizations have repeatedly warned that digital ID systems create new forms of surveillance, exclusion, and political risk. Early advocacy against facial recognition technology, including the ACLU of Massachusetts' "Press Pause on Face Surveillance" campaign[75] and Amnesty International's "Ban the Scan" campaign[76], called for halting or restricting government facial recognition deployments because of their discriminatory impacts, threats to civil liberties, and risks of pervasive tracking. Other advocates similarly challenged facial recognition systems as tools of racial discrimination, wrongful identification, and mass surveillance, yet many government and industry responses focused primarily on technical fixes such as improving accuracy rates, reducing bias, or adding procedural safeguards rather than questioning whether these systems should exist at all.

Alongside broader organizing around sanctuary protections and community-controlled identification systems, immigrant justice organizations have warned that mDL and interoperable digital ID systems can expose immigrants and other vulnerable communities to expanded surveillance and law enforcement access.[77] Public interest groups such as Fight for the

---

[72] Hill, Kashmir. "You Can Hide Your Pregnancy Online, But You'll Feel Like A Criminal." *Forbes*, Apr. 29, 2014, https://www.forbes.com/sites/kashmirhill/2014/04/29/you-can-hide-your-pregnancy-online-but-youll-feel-like-a-criminal/.

[73] Meredith Whittaker, CEO of Signal, has warned that emerging forms of "agentic AI" may require extensive "root access" into devices and access to identity credentials and obtain information from calendars, communications, financial accounts, and behavioral activity in order to, in her example, coordinate your birthday party: making reservations, paying for food, and inviting your friends. She warns this root access to device and identity credentials threatens to "break the blood-brain barrier" between encrypted applications and operating systems, rendering many existing identity and privacy protections ineffective. "Signals's Whittaker on Privacy in the Age of Data and AI", Bloomberg Live, 9:34-12:03, https://www.youtube.com/watch?v=-CHfHA5ptaU

[74] Early examples of the risks are already visible in products such as Microsoft Recall and similar systems which normalize expansive device-level monitoring, memory, and automation. Warren, Tom. "Microsoft faces fresh Windows Recall security concerns", *The Verge*. Apr. 15, 2026, https://www.theverge.com/report/912101/microsoft-windows-recall-new-security-concerns-response.

[75] Press Pause on Face Surveillance. *ACLU of Massachusetts*, n.d. Accessed May 18, 2026. https://www.aclum.org/campaigns-initiatives/press-pause-face-surveillance/.

[76] Ban the Scan. *Amnesty International,* n.d. Accessed May 18, 2026. https://banthescan.amnesty.org/index.html.

[77] Broder, Tanya, Finn, Alli, Gosrani, Chiraayu, Kim Pak, Sarah, and Vogel, Ed. "FAQ: Mobile Driver's Licenses and the Costs To Privacy, Safety, and Security," National Immigration Law Center, January 23, 2024, https://www.nilc.org/resources/faq-mobile-drivers-licenses-and-the-costs-to-privacy-safety-and-security/

Future have also challenged age verification mandates and identity-linked internet governance systems through campaigns such as "Stop Online ID Checks,"[78] warning that they threaten anonymous speech, privacy, and access to information online. Despite these efforts, most digital ID systems have continued to expand through administrative modernization programs, opaque procurement pipelines, interoperability standards, and fragmented sector-specific mandates rather than through broad democratic debate about whether these systems should exist at all.

Many advocacy organizations increasingly find themselves confined to a narrow harm-reduction framework in which they are forced to negotiate how identity checks occur technically rather than whether pervasive identity verification systems should be required in the first place. Groups such as ACLU, CDT, EPIC, and EFF routinely submit comments to agencies[79], standards bodies[80], and procurement processes seeking selective disclosure protections[81], "no phone home" architectures intended to prevent credentials from notifying issuers every time they are used[82], device-controlled and browser-controlled privacy protections, accessibility requirements[83], meaningful consent standards, limits on biometric retention, and restrictions on centralized tracking. These interventions are important and can meaningfully reduce some harms, but they also reveal how limited advocates' role has become. Many of these safeguards remain optional, inconsistently implemented, or dependent upon the goodwill of vendors and governments already committed to expanding digital identity infrastructure.

Lessons from international digital identity rollouts further suggest that many promised privacy protections remain unevenly implemented in practice and that decentralization frequently functions more as a policy promise than a lived reality.[84]

III. Why We Must Act Now

Passing new mandates for mDLs, age verification, or other digital ID schemes without enforceable safeguards will only accelerate these harms: people denied services, youth blocked from online communities, sensitive data exposed, and public funds diverted into vendor contracts that fail at scale.

---

[78] Fight for the Future. "ONLINE ID CHECKS WILL RUIN THE INTERNET." Accessed May 25, 2026. https://stoponlineidchecks.org.
[79] "Comments of EPIC, ACLU, CDT, and EFF to the TSA on Interim Waiver Process Rulemaking for Mobile Driver's Licenses." *Regulations.Gov*. Accessed May 18, 2026. https://www.regulations.gov/comment/TSA-2023-0002-0026.
[80]World Wide Web Consortium, "Credential Considerations," GitHub repository, accessed May 18, 2026,https://github.com/w3c/credential-considerations/blob/main/credentials-considerations.md.
[81] "ACLU Digital ID State Legislative Recommendations." *American Civil Liberties Union*, n.d. Accessed May 18, 2026. https://www.aclu.org/publications/aclu-digital-id-state-legislative-recommendations.
[82] Hancock, Alexis and Collings, Paige. "Zero Knowledge Proofs Alone Are Not a Digital ID Solution to Protecting User Privacy." Electronic Frontier Foundation, July 25, 2025. https://www.eff.org/deeplinks/2025/07/zero-knowledge-proofs-alone-are-not-digital-id-solution-protecting-user-privacy.
[83] Doty, Nick. "Digital IDs Must Be Safe, Secure and Accessible," Center for Democracy & Technology, April 11, 2025, https://cdt.org/insights/digital-ids-must-be-safe-secure-and-accessible/
[84] DiResta, CJ Larkin, Renée. "Lessons from National Digital ID Systems for Privacy, Security, and Trust in the AI Age." Tech Policy Press, June 25, 2025. https://techpolicy.press/lessons-from-national-digital-id-systems-for-privacy-security-and-trust-in-the-ai-age.

Communities Do Not Have A Seat At the Table of Digital ID Decisions

Public resistance to national identification systems like REAL ID, biometric surveillance, data breaches, and corporate technology power has remained persistent for decades. Many of the most consequential decisions about digital ID systems are made without broad public debate about the systems' cumulative impacts. For example, age-verification laws are often enacted to address concerns about online harms affecting children, but frequently fail to account for broader impacts on free expression, access to health and educational information, privacy and data security, anonymity, discrimination, and the growing concentration of state and corporate power enabled by digital ID systems.[85] Communities are frequently asked to adapt to these systems after key decisions have been made, limiting opportunities to shape whether digital ID systems are adopted, how they are governed, and what safeguards are put in place to prevent harm.

This Is a Critical Moment for Action

Digital ID systems increase the leverage that powerful technology industries and the security state already have to further expand their capacity to surveil and control communities. Digital ID systems are being adopted, integrated, and normalized across public and private life faster than democratic institutions can evaluate, govern, or meaningfully constrain them. While some proposals have faced resistance, the broader trajectory remains one of expansion through administrative modernization efforts, fraud prevention initiatives, security programs, and private-sector adoption.

This is a critical moment for intervention: once technical standards, procurement decisions, and identity infrastructures become embedded across institutions, they become far more difficult to challenge, reform, or unwind. Halting further digital ID expansion until enforceable rights and democratic safeguards are in place is the only way to protect dignity, equity, and freedom. The future of identity should not be built on more sophisticated surveillance but on systems that respect human rights and collective self-determination.

Digital ID Systems Are Already Facilitating Harm

Digital ID systems are exacerbating existing harms and creating novel threats to longstanding human rights principles including privacy, autonomy and self-determination, equity, freedom of movement and association, access to justice, the right to know, democratic participation, and meaningful access to public goods and essential services.

International human rights advocates and researchers have warned that digital ID systems risk transforming legal identification from a protected right into a prerequisite for accessing other

[85] Conti Cook, Cynthia, Katiyar, Pratika, and Williams, Rebecca. "Who Age Verification Laws Really Benefit & How to Resist" Aug 25, 2025, User Mag. https://www.usermag.co/p/we-must-fight-age-verification-with.

rights and services, particularly for vulnerable communities already facing structural barriers.[86] The individualized behavioral profiling tactic that powers advertising technology and pervades the web is now being applied to identity itself to facilitate micro-targeted denials of essential services, flags at borders, restrictions on movement or participation, and new forms of discrimination, profiling, and coercive control.[87]

Concentrated Corporate Power in Governance

Digital ID systems are increasingly shifting control over identity, deservedness, and public governance away from democratically-accountable institutions and toward private corporations with opaque technical systems. These systems continue to proliferate not because governments have created meaningful safeguards against the many foreseeable harms discussed above, nor because they have proven safe or effective for communities, but because corporate vendors and security actors are increasingly shaping the future of government technology procurement and administration.[88] As governments outsource more public infrastructure to private technology companies, the public increasingly absorbs the costs of surveillance, exclusion, failed deployments, cybersecurity risks, and wasteful spending while losing opportunities for democratic oversight, transparency, and investment in equitable alternatives aligned with community safety and privacy protections.[89]

First, governments are increasingly relying on private technology companies not simply as vendors, but by outsourcing historically public functions into privately operated technological systems, including chatbots instead of direct government interaction,[90] cryptocurrency systems[91] instead of state-controlled financial infrastructure, and now digital ID systems. Rather than interacting directly with public institutions, people increasingly navigate privatized technological systems that shape access to public goods, rights, and participation. Public systems are digitized through long-term agreements such as Master Service Agreements (MSAs) with major technology corporations.[92] For example, when New York City launched a public communications chatbot through its MyCity portal, it was delivered through New York City's

---

[86] Arroyo, Verónica, Carter, Emma (pseudonym), Karanja, , Kate Robertson, and Emile Dirks. "The Citizen Lab's Submission to the UN on Universal Birth Registration and the Use of Digital Technologies." *The Citizen Lab*, July 21, 2025.
https://citizenlab.ca/the-citizen-labs-submission-to-the-un-on-universal-birth-registration-and-the-use-of-digital-technologies/

[87] Baker, Sara and Rahman, Zara, *Understanding the Lived Effects of Digital ID: A Multi-Country Study* London: The Engine Room, January 2020.
https://digitalid.theengineroom.org/assets/pdfs/200310_TER_Digital_ID_Report+Annexes_English_Interactive_Edit3.pdf

[88] Garber, Nick and Groz, Zachary, "New York City's Multibillion-Dollar Black Box Contracts Face Scrutiny", *NY Focus,* May 6, 2026, https://nysfocus.com/2026/05/06/new-york-city-contracting-master-agreements.

[89] Westoll, Nick, "Toronto audit finds City staff spent $11M for unused, underutilized software licences," *CityNews*, Dec. 3, 2024,
https://toronto.citynews.ca/2024/12/03/toronto-audit-finds-city-staff-spent-11m-for-unused-underutilized-software-licences/

[90] "NYC MYCITY CHATBOT", *Museum of Failure*, https://museumoffailure.com/exhibition/nyc-ai-crime

[91] "How the U.S. Government Is Using Crypto, and Where It Could Go Next", Jun. 20, 2025
https://blogs.usfcr.com/gov-crypto-projects

[92] Pakzad, Roya and Conti-Cook, Cynthia, "Key Considerations in AI Procurement," Taraaz, Aug. 2025, https://taraazresearch.org/ai-procurement.

first vendor to have a MSA contract—Microsoft.[93] The chatbot infamously provided inaccurate and potentially unlawful advice to landlords and employers, creating risks for tenants and workers.[94] When members of the public sought information about the chatbot's training data through the City's mandatory algorithmic reporting process, the program's entry indicated the information was proprietary.[95] During an oversight hearing, City officials reported that the vendor itself[96] determined when the chatbot was ready for deployment. Later Freedom of Information Law (FOIL) requests seeking the underlying agreements and costs produced fragmented and incomplete disclosures.[97] Subsequent reporting and a 2026 NYC Comptroller audit[98] further raised concerns that MSAs obscured both fiscal oversight and public accountability.[99] While the MyCity chatbot itself was not a digital ID system, it illustrates how privatized government technology infrastructure obstructs transparency into decision-making by both the corporate vendor and the government agency, undermines democratic intervention and meaningful public oversight. The private-public structure of digital ID systems threaten to repeat this dynamic.

At the same time, government-recognized forms of identification are being treated as subordinate to digital ID systems supplied by private vendors (or private vendors' systems are being embedded into government enforcement systems). In recent litigation, DHS stated that REAL ID itself "can be unreliable to confirm U.S. citizenship,"[100] while U.S. Immigration and Customs Enforcement (ICE) officials reportedly asserted that biometric matches generated through a vendor's mobile surveillance tools could override traditional evidence of citizenship, including birth certificates.[101] ICE officers also reportedly rejected federally recognized tribal identification documents as "fake" before detaining Indigenous family members.[102]

Together, these developments illustrate how digital ID systems grant policing forces in government and corporate vendors more leverage to redefine identity.

---

[93] Microsoft Media Relations, "Michael Bloomberg, Steve Ballmer: News Conference", Oct. 20, 2010, https://news.microsoft.com/speeches/michael-bloomberg-steve-ballmer-news-conference/.
[94] Lecher, Colin, "NYC's AI Chatbot Tells Businesses to Break the Law", *The Markup,* Mar. 29, 2025, https://themarkup.org/artificial-intelligence/2024/03/29/nycs-ai-chatbot-tells-businesses-to-break-the-law.
[95] Reports, "Summary of Agency Compliance Reporting of Algorithmic Tools CY 2023", *Office of Technology and Innovation*, Mar. 2024 https://www.nyc.gov/assets/oti/downloads/pdf/reports/2023-algorithmic-tools-reporting-updated.pdf.
[96] City Council Committee on Technology Oversight Hearing, "AI and ADS Systems", New York City Council, Oct. 31, 2024
[97] Results from FOIL request from the New York City Comptroller, on file with author.
[98] Dan Roboff, Sr. Director of Contract Analytics; James Leidy, Procurement Analyst; and Yifeng Zheng, CUNY Fellow, "The Monty Hall Contracts: Unchecked Spending Across the City's Master Agreements"
[99] Garber, Nick and Groz, Zachary, "New York City's Multibillion-Dollar Black Box Contracts Face Scrutiny", *NY Focus,* May 6, 2026, https://nysfocus.com/2026/05/06/new-york-city-contracting-master-agreements.
[100] *Venegas v. Homan et al.*, No. 1:25-cv-000397 (S.D. Ala. filed 2025).
[101] Cox , Joseph. "ICE and CBP Agents Are Scanning Peoples' Faces on the Street To Verify Citizenship." 404 Media, October 29, 2025. https://www.404media.co/ice-and-cbp-agents-are-scanning-peoples-faces-on-the-street-to-verify-citizenship/.
[102] Levi Rickert, "Tribal IDs Are Federally Recognized. ICE Agents Are Ignoring Them", *Native News Online*, Nov. 30, 2025, https://nativenewsonline.net/opinion/tribal-ids-are-federally-recognized-ice-agents-are-ignoring-them/

Conditional Access and Criminalization

Digital ID systems accelerate conditional access and criminalization because their affordances encourage the creation of persistent and interoperable records about individuals that can be used to assess, monitor, gatekeep, and condition access across public, private, and social sectors.[103] The systems rely heavily on "means-testing industrial complex"[104] describe a growing corporate and administrative apparatus devoted to testing, monitoring, and verifying whether people qualify for public goods and social welfare programs.[105] Systems that once operated separately can increasingly be linked together, allowing identity itself to become a site of continuous evaluation and control. These infrastructures make punitive governance easier to scale and harder to escape, moving societies further away from models grounded in dignity, trust, and care.[106]

Digital ID systems expand the power of policing through integrated databases, biometric verification, mobile surveillance tools, and information sharing far beyond ports of entry or physical borders.[107] As of this writing, reporting on Palantir tools used by ICE describes agents carrying access to dossiers on roughly 20 million people directly on their mobile devices, combining identity, employment, location, and relational data into searchable enforcement profiles.[108] ICE and U.S. Customs and Border Protection (CBP) agents have also reportedly used facial recognition tools in the field to scan people's faces during ordinary public encounters in order to verify identity or citizenship status.[109] These systems create persistent surveillance infrastructures capable of tracking, monitoring, and targeting people across institutions and every instance of daily life. These developments are especially concerning as longstanding privacy principles such as purpose limitation continue to erode. For example, the IRS recently agreed to share taxpayer information with DHS for immigration policing, illustrating how data collected for one administrative purpose can later be repurposed for a carceral purpose.[110]

Digital ID systems also often place the greatest burdens on the most vulnerable people seeking support. Research from Georgetown University's Beeck Center documenting identity proofing requirements across Supplemental Nutrition Assistance Program (SNAP), Medicaid, Temporary

[103] Recent scholarship across public policy, abolitionist organizing, and critical political economy has increasingly warned against governance systems that manage social problems through surveillance, gatekeeping, criminalization, and punishment rather than addressing their material root causes through public support and collective care. Gilmore, Ruth Wilson, Brenna Bhandar, and Alberto Toscano. *Abolition Geography: Essays towards Liberation*. Verso, 2023.

[104] Farrel, Luke, "The Means-Testing Industrial Complex." January 28, 2026, LPE Project. https://lpeproject.org/blog/the-means-testing-industrial-complex/.

[105] Spade, Dean. Normal Life: Administrative Violence, Critical Trans Politics, and the Limits of Law. Duke University Press, 2015.

[106] Spade, Dean. Normal Life: Administrative Violence, Critical Trans Politics, and the Limits of Law. Duke University Press, 2015.

[107] Aizeki, Mizue, Bingham, Laura and Narváez, Santiago. "The Everywhere Border: Digital Migration Control Infrastructure in the Americas," in *State of Power 2023* (Amsterdam: Transnational Institute, 2023).

[108] Cox, Joseph. "ICE Agents Have List of 20 Million People on Their iPhones Thanks to Palantir." 404 Media, May 12, 2026. https://www.404media.co/ice-agents-have-list-of-20-million-people-on-their-iphones-thanks-to-palantir/

[109] Cox, Joseph. "ICE and CBP Agents Are Scanning Peoples' Faces on the Street To Verify Citizenship." 404 Media, October 29, 2025. https://www.404media.co/ice-and-cbp-agents-are-scanning-peoples-faces-on-the-street-to-verify-citizenship/.

[110] "The IRS Is Building a Vast System to Share Millions of Taxpayers' Data With ICE." ProPublica, July 15, 2025. https://www.propublica.org/article/trump-irs-share-tax-records-ice-dhs-deportations.

Assistance for Needy Families (TANF), Special Supplemental Nutrition Program for Women, Infants, and Children (WIC), unemployment insurance, child care, and other public benefits programs illustrates how deeply digital authentication and identity verification systems are already embedded into access to public assistance in the United States.[111] Governments expand identity proofing requirements in the name of fraud prevention, but the practical effect, much like means testing itself, is often de facto denial of essential services. Digital ID systems require vulnerable populations to disclose increasing amounts of sensitive personal information in moments of need while imposing complex verification burdens that many people cannot successfully navigate.[112]

When access to essential services is conditioned on compliance with error-prone, burdensome, or exclusionary digital ID systems, denial of service becomes a policy, pattern, and practice-based systemic rights violation rather than an isolated administrative error.[113] Recent reporting on proposed Social Security A identity verification changes similarly found that requiring additional digital ID checks would likely force millions of elderly, disabled, rural, low-income, or technologically disconnected individuals into burdensome verification systems they could struggle to navigate.[114]

As digital ID systems become more deeply embedded into participation in society, identity credentials are simultaneously becoming sites of governance and punishment. These systems create new feedback loops in which restrictions can more easily become attached to identity records across institutions. For example, the U.S. federal government has reportedly revoked Global Entry access for an ICE protester,[115] while states have proposed or implemented passport restrictions for individuals with unpaid child support.[116] Where political will exists to impose new forms of punishment or exclusion, digital ID systems may facilitate these forms of identity-linked restriction easier to expand, automate, and normalize.

Chilling Free Expression and Democratic Participation

Democratic participation has long depended on the ability to speak, organize, read, associate, dissent, and vote without continuous identity verification or surveillance. Political theorists such

---

[111] Digital Government Hub. "Digital Authentication and Identity Proofing in Public Benefits Applications." Accessed May 17, 2026. https://digitalgovernmenthub.org/publications/digital-authentication-and-identity-proofing-in-public-benefits-applications/

[112] India's Aadhaar system and broader "citizenship by algorithm" models have already demonstrated how interconnected identity infrastructures can expand means testing, automate eligibility determinations, and create new opportunities to gatekeep access to healthcare, welfare, and other public goods through continuous data-driven verification processes.Soon-Shiong, Nika. "Citizenship by Algorithm." Jacobin, September 15, 2025. https://jacobin.com/2025/09/citizenship-by-algorithm.

[113] *Monell v. Department of Soc. Svcs*., 436 U.S. 658 (1978)

[114] Legum, Judd. "EXCLUSIVE: Memo Details Trump Plan to Sabotage the Social Security Administration." Accessed May 17, 2026. https://popular.info/p/exclusive-memo-details-trump-plan.

[115] Brodkin, Jon. "ICE Observer Says Her Global Entry Was Revoked after Agent Scanned Her Face." Ars Technica, January 30, 2026. https://arstechnica.com/tech-policy/2026/01/ice-protester-says-her-global-entry-was-revoked-after-agent-scanned-her-face/

[116] "Passports and Child Support Debt." Accessed May 17, 2026. https://travel.state.gov/content/travel/en/passports/legal-matters/child-support.html.

as Hannah Arendt describe democratic participation as dependent upon a "right of appearance" in public life, believing that democracies require spaces where people can collectively organize, deliberate, and act without total state or institutional control.[117] Voting itself has similarly long depended upon secrecy and anonymity, the proverbial curtain we all pull behind us in a voting booth.[118]

Digital ID systems create new risks to a cornerstone of democracy: voting itself. Researchers and advocates have documented how digital ID systems in countries including Venezuela[119] and Zimbabwe[120] have been tied to political surveillance, voter exclusion, and distrust surrounding democratic participation. Similar concerns emerged in Kenya, where presidential elections in 2013 and 2017 were challenged over irregularities involving biometric voter registration and electronic results transmission systems administered by the Independent Electoral and Boundaries Commission (IEBC). Although these technologies were introduced to strengthen electoral integrity and public confidence, repeated technical failures and the unprecedented nullification of the 2017 presidential election by Kenya's Supreme Court contributed to declining trust in the electoral process rather than strengthening confidence in it.[121]

In the United States, these concerns are emerging amid broader attacks on voting rights, including the weakening of Voting Rights Act protections, aggressive gerrymandering, expanded citizenship verification efforts through Social Security Administration records,[122] and proposed legislation such as the SAVE Act that would impose additional documentary burdens for voter registration on married women, immigrants, low-income voters, and people whose records do not neatly align across databases. This growing wave of voter verification and citizenship checks could increasingly be exploited through digital ID systems and interconnected identity infrastructures, creating new opportunities for voter suppression, political exclusion, and democratic chilling.

Labor organizing, whistleblowing, mutual aid, and justice movements have likewise depended upon spaces for confidential association and anonymous speech. Privacy and anonymity are not incidental to democracy and democratic resilience; they are conditions that make democratic participation, organizing, dissent, and free political expression possible. Digital ID systems like age verification threaten freedom of speech, expression, association, and protest by eliminating spaces for anonymous participation and private organizing. Emerging age verification laws, coupled with digital ID systems like mobile drivers' licenses and the rapid growth of bots and

---

[117] "In contrast to the inorganic thereness of lifeless matter, living beings are not mere appearances. To be alive means to be possessed by an urge toward self-display which answers the fact of one's own appearingness. Living things make their appearance like actors on a stage set for them." Hannah Arendt, *The Life of the Mind*, vol. 1: Thinking

[118] *Universal Declaration of Human Rights*, art. 21 (protecting the right to a secret vote).

[119] Hernández, Marianne Díaz. "Venezuela: Digital ID As a Tool of Oppression." Tech Policy Press, September 10, 2024. https://techpolicy.press/venezuela-digital-id-as-a-tool-of-oppression.

[120] Chimhangwa, Kudzai. "How Zimbabwe's Biometric ID Scheme (and China's AI Aspirations) Threw a Wrench into the 2018 Election." Global Voices Advox, January 30, 2020. https://advox.globalvoices.org/2020/01/30/how-zimbabwes-biometric-id-scheme-and-chinas-ai-aspirations-threw-a-wrench-into-the-2018-election/.

[121] Nyabola, Nanjala. Without Trust, Politics Is Reduced to Spectacle. August 26, 2020. https://www.thenation.com/article/politics/democracy-postal-service-kenya/.

[122] Fifield, Jen. "DHS Agreement Reveals Risks of Using Social Security Data for Voter Citizenship Checks." ProPublica, October 30, 2025. https://www.propublica.org/article/dhs-social-security-data-voter-citizenship-trump.

synthetic content driven by AI, are also creating a de facto expectation that identity will be continuously checked across the internet.[123] These systems create chilling effects for people seeking information related to reproductive healthcare, LGBTQ+ identity, sexuality, migration, labor organizing, and political dissent. In the United States, *Free Speech Coalition, Inc. v. Paxton* upheld Texas's digital age verification law for sexually explicit websites, narrowing longstanding First Amendment protections surrounding anonymous access to lawful online speech and signaling greater judicial tolerance for mandatory online identity checks.[124] These dynamics echo earlier censorship tactics including book bans, obscenity laws, McCarthy-era surveillance, and other moral panics in which stigmatized speech and political dissent were criminalized or suppressed.[125] Digital ID systems dramatically increase the scale, permanence, and enforceability of those controls by making identity-linked surveillance continuous, searchable, interoperable, and easier to automate across institutions and platforms.

Discriminating Against Targeted Communities

Digital ID systems reinforce discrimination through misidentification, erasure, and exclusion. As Ruha Benjamin and Virginia Eubanks have documented in adjacent contexts, automated systems often reproduce and legitimize existing inequalities under the appearance of technological neutrality. Facial recognition technologies disproportionately produce false positives for women and people of color, exposing them to arbitrary scrutiny, denial of services, and heightened policing.[126] Transgender people whose gender markers are incongruent with a government's rigid binary understanding of gender risk erasure from administrative systems altogether, while recent disputes over X gender markers on passports demonstrate how identities can be invalidated or rendered suspect.[127] Poor and working-class people without stable documentation, reliable internet access, or digital literacy are similarly at risk of exclusion from systems increasingly requiring digital authentication. Immigrants also face heightened risks when identities are linked across immigration databases, exposing people to detention, deportation, or exclusion. Globally, these harms are already documented as human rights violations, particularly where digital ID systems determine access to healthcare, movement, or legal recognition. For example, in Uganda and India, mandatory ID systems have already blocked women and people living with HIV from accessing essential healthcare.[128]

---

[123] Emanuel Maiberg, "UK Users Need to Post Selfie or Photo ID to View Reddit's r/IsraelCrimes, r/UkraineWarFootage." 404 Media, July 29, 2025. https://www.404media.co/uk-users-need-to-post-selfie-or-photo-id-to-view-reddits-r-israelcrimes-r-ukrainewarfootage/

[124] *Free Speech Coalition, Inc. v. Paxton*, No. 23-1122.

[125] Andrea Friedman, Prurient Interests: Gender, Democracy, and Obscenity in New York City, 1909-1945, Columbia Univ. Press, 2000.

[126] "Live Facial Recognition in Scotland: A Threat to Race Equality and Human Rights." *CRER*, https://www.crer.org.uk/blog/lfr-in-scotland-a-threat-to-race-equality-and-hr. Accessed 17 Sep. 2025.

[127] Erwin Chemerinsky, "The Shadow Docket Fails Again." November 20, 2025. https://www.scotusblog.com/2025/11/the-shadow-docket-fails-again/.

[128] Cynthia Conti Cook, Sawyeh Esmaili, and Rebecca Williams, "Digital IDs Put Health Care Privacy at Risk." Article Convergence Magazine, August 4, 2025, https://convergencemag.com/articles/digital-ids-put-health-care-privacy-at-risk/.

Eroding Privacy and Exposing Sensitive Information

Digital ID systems create central repositories of sensitive data that act as attractive targets for hackers, fraudsters, abusive actors, and foreign adversaries. Failures like the AU10TIX exposure, which leaked identity records connected to users of TikTok, Uber, and X, demonstrate how easily these systems can expose highly sensitive information.[129] Other recent breaches involving identity verification vendors, credit reporting systems, and platform contractors have exposed driver's licenses,[130] financial records,[131] and other personal information affecting millions of people.[132] Women using safety-focused applications have similarly faced harassment and doxxing after identity verification records were leaked online.[133] ID verification requirements can also create cascading cybersecurity risks. For example, several security and privacy developers reportedly lost access to critical publishing and signing infrastructure after Microsoft enforced government ID verification requirements for developer accounts, temporarily preventing security updates and software patches from being distributed to users.[134]

At the same time, many of the protections used to justify digital ID systems remain highly vulnerable to circumvention and failure. Face spoofing, manipulated liveness checks,[135] synthetic identities, and fraudulent credentials continue to bypass identity verification systems, while fake accounts and automated abuse remain widespread online. The systems themselves are also complex and error-prone. Biometrics routinely misidentify individuals, multi-factor authentication locks people out of critical services, and inaccessible interfaces disproportionately burden disabled people, elderly people, and communities with limited digital literacy or internet access. What is marketed as secure identity verification too often delivers insecurity, exclusion, surveillance, and risk instead.

IV. What We Must Demand

Digital ID systems are often framed as inevitable modernization efforts, but the United States remains in a relatively unusual position to resist a national digital identity system. Rather than passively accepting these developments, advocates, lawmakers, researchers, and communities

[129] Joseph Cox. "ID Verification Service for TikTok, Uber, X Exposed Driver Licenses." *404 Media*, 26 Jun. 2024, https://www.404media.co/id-verification-service-for-tiktok-uber-x-exposed-driver-licenses-au10tix/.
[130] Jay Peters. "Discord Blamed a Vendor for Its Data Breach — Now the Vendor Says It Was 'Not Hacked.'" The Verge, October 14, 2025. https://www.theverge.com/news/799274/discord-security-breach-5ca-vendor-blamed-not-hacked.
[131] Zack Whittaker. "Data Breach at Credit Check Giant 700Credit Affects at Least 5.6 Million." *TechCrunch*, December 12, 2025. https://techcrunch.com/2025/12/12/data-breach-at-credit-check-giant-700credit-affects-at-least-5-6-million/.
[132] Sead Fadilpašić. "Massive Global Data Breach Sees over a Billion Records Exposed." Yahoo Tech, February 26, 2026. https://www.techradar.com/pro/security/massive-global-data-breach-sees-over-a-billion-records-exposed-heres-what-we-know-so-far.
[133] Emanuel Maiberg and Joseph Cox. "Women Dating Safety App 'Tea' Breached, Users' IDs Posted to 4chan." 404 Media, July 25, 2025. https://www.404media.co/women-dating-safety-app-tea-breached-users-ids-posted-to-4chan/.
[134] Zack Whittaker, Developer of VeraCrypt encryption software says Windows users may face boot-up issues after Microsoft locked his account, *TechCrunch,* Apr. 8, 2026, https://techcrunch.com/2026/04/08/veracrypt-encryption-software-windows-microsoft-lock-boot-issues/
[135] Daniel Sims, "Brits Are Circumventing UK Age Verification with VPNs and *Death Stranding* Photos," *TechSpot*, July 26, 2025, https://www.techspot.com/news/108736-brits-circumventing-uk-age-verification-vpns-death.html.

must act now to shape how identity systems evolve to protect and better serve those most vulnerable to overpolicing, surveillance, and state separation–including homeless, formerly incarcerated people, gender non-conforming people, youth, disabled people and undocumented immigrants.

Unlike many countries with centralized national identity infrastructures, state and local governments have more control over identity governance. That fragmentation creates meaningful opportunities, particularly at the state and local levels, for public intervention, legislative guardrails, democratic participation, and resisting digitization before digital ID systems become deeply entrenched and difficult to unwind. State and local governments still retain significant authority over how identity is administered and recognized, creating critical opportunities to preserve non-digital alternatives, limit interoperability mandates, regulate vendor influence, and resist the normalization of continuous identity verification across daily life.

Below we recommend strategies to resist digital ID systems, to protect dignity, human rights and democracy, and questions to rethink identity. To assess whether your state has initiated an administrative or legislative effort related to mDL systems, CRCR's website hosts a "Toolkit for Navigating Your State's Digital ID System" and a spreadsheet with state-by-state administrative action or legislation related to mDLs.[136]

Resisting National Digital ID

Block Expansion

Popular resistance to centralized identity infrastructure already exists across the United States. Efforts to stop digital ID systems have evolved alongside the technologies and uses themselves. Earlier advocacy and legislation often focused broadly on restricting facial recognition systems. Individuals have pushed back against REAL ID expansion by choosing not to register for them[137], advocates have pushed for legislation banning facial recognition systems, communities have pressured lawmakers to place moratoriums of data center construction,[138] and some city workers have even placed garbage bags over surveillance cameras.[139] Advocates should pressure lawmakers to halt expansion of digital IDs until human rights-based guardrails, meaningful democratic oversight, and enforceable accountability mechanisms are in place.

---

[136] "Toolkit for Navigating Your State's Digital ID System" *theCRCR.org,* https://thecrcr.org/wp-content/uploads/Toolkit-for-Navigating-Your-States-Digital-ID-System_Print.pdf and "Digital ID Systems - Policies, Tech, Uses, Protections" (2025) https://docs.google.com/spreadsheets/d/1EKzZqsLUG_r_H7lby06US4aURRl7-r4D0ixdgq4p-2g/edit?gid=1286523486#gid=1286523486 (updated May 2026).

[137] WABI News Desk, "29% of Mainers have their Real ID as requirement goes into effect", *WABI*, May 7, 2025, https://www.wabi.tv/2025/05/07/29-mainers-have-their-real-id-requirement-goes-into-effect/

[138] French, Marie J., "New York lawmakers plan to approve one-year data center moratorium", *POLITICO*, June 2, 2026, https://www.politico.com/news/2026/06/02/new-york-one-year-data-center-moratorium-00946477

[139] Tangalakis-Lippert, Katherine, "Why Cities Are Putting Trash Bags Over Flock's License Plate Readers", *Business Insider*, June 1, 2026, https://www.businessinsider.com/cities-putting-trash-bags-over-flock-license-plate-readers-2026-6

As digital ID systems become increasingly intertwined with specific forms of identity-linked surveillance and coercion, so has legislation blocking its uses. For example, in 2026, Syracuse, New York, passed legislation prohibiting businesses from using biometric surveillance technologies in places of public accommodation.[140] At the state level, lawmakers in California have advanced proposals targeting surveillance pricing practices that use personal data, behavioral profiling, or identity-linked information to shape prices, services, or opportunities.[141] These developments reflect growing public concern that digital ID systems are becoming embedded across our lives.

Ensure people can…	Pass mandates that…
Refuse to enroll in optional programs like CLEAR or mDLswithout punitive long lines. Organize local campaigns for moratoriums and bans on biometric rollouts. Support lawsuits, ballot measures, and union demands against ID-linked surveillance.	Impose moratoriums on all new digital ID deployments pending enforceable safeguards. Sunset existing vendor contracts (e.g., IDEMIA, ID.me) unless renewed with public hearings and enforceable safeguards. Mandate risk-benefit reviews that weigh civil liberties and equity alongside efficiency claims. Defund pilots (such as mobile driver's license rollouts) unless paired with non-biometric alternatives and community consultation.

Preserve Human and Real-World Alternatives

We must call for policymakers to not only block harmful expansion, but also preserve meaningful non-digital alternatives. Digital IDs should never erase the right to live, pay, and interact in the physical world. People must retain meaningful access to paper IDs, cash, and staffed services to ensure equity, dignity, and resilience.

Experiences with inaccessible digital systems highlight how exclusive reliance on digital ID can undermine accessibility, equal access, labor protections, and meaningful participation in public life. Existing disability rights, labor, and consumer protection frameworks were not designed to fully address identity systems operating at this scale and level of automation. Preserving human and real-world alternatives is therefore essential to protecting dignity, accessibility, and democratic participation.

[140] Deryn, Alexandra "'The Right Thing to Do': Syracuse Lawmakers Unanimously Pass Bill Banning Biometric Surveillance." May 19, 2026. https://www.yahoo.com/news/articles/thing-syracuse-lawmakers-unanimously-pass-101500641.html.
[141] Johnson, Khari. "Why Surveillance Pricing Bans Are Suddenly Gaining Traction This Year (and Not Just in California)." Technology. *CalMatters*, May 15, 2026. https://calmatters.org/economy/technology/2026/05/why-surveillance-pricing-bans-are-suddenly-gaining-traction-this-year-and-not-just-in-california

People should retain the ability to access public services and participate in society using physical identification documents, cash, and staffed in-person services without penalty, coercion, or exclusion.[142] Essential services and transactions should not require exclusive reliance on smartphones, biometric systems, digital wallets, automated kiosks, or app-based identity verification systems. When governments and businesses eliminate physical credentials, cash payments, or human staff in favor of automated identity and payment systems, people with disabilities, language barriers, limited internet access, unstable housing, low digital literacy, or heightened privacy concerns face increased risk of exclusion. Some jurisdictions have already begun preserving physical credentials and limiting mandatory reliance on digital ID systems through legislation protecting access to non-digital alternatives.[143]

From both human rights and labor rights perspectives, preserving human-mediated systems protects workers and the public alike by maintaining spaces for contextual judgment, accessibility, discretion, and meaningful recourse. Staffed public services, cash access, and physical credentials help prevent essential aspects of daily life from becoming fully dependent on exclusionary digital identity infrastructures and automated decision-making systems.

Ensure people can…	Pass mandates that…
Request physical IDs and challenge denials. Choose cash and push back against cashless-only businesses. Request staffed services when kiosks fail or exclude. Report failures of kiosk-only systems. Access equitable in-person help regardless of digital literacy.	Require states and federal agencies to issue physical ID cards on demand. Prohibit penalties, excessive friction, secondary screening, or retaliatory treatment for individuals who choose physical credentials or opt out of digital ID systems or biometric verification. Ban digital-only ID requirements. Ban cashless-only retail. Prohibit credit card fees, surcharges, or incentives that privilege digital payment. Protect ATMS, limit ATM fees, and ensure functional ATMs are available in every neighborhood. Require minimum clerk-to-kiosk staffing ratios. Prohibit full replacement of human staff with kiosks in essential services.

[142] Universal Declaration of Human Rights, art. 21 ("Everyone has the right of equal access to public service in his country"); see also International Covenant on Civil and Political Rights, arts. 19, 21, 22 (protecting rights of expression, assembly, and association).
[143] See, e.g., Oklahoma SB 1231 (2024) (defining digital identity data as personally identifiable information rather than merely a "digitized identification card" and prohibiting denial of government services based on refusal to use digital ID systems); West Virginia HB 5551 (2024) (preserving access to physical identification documents and non-REAL ID credentials).

	Enforce labor standards that protect staffed roles and prevent kiosk-driven layoffs.

Unwind Digital ID Systems that Facilitate Harm

Digital ID systems are often framed as inevitable modernization efforts, but many programs have stalled, failed, been deactivated, or faced significant legal and operational challenges. In the United States, for example, mDL programs have been deactivated in Florida, Missouri, and Oklahoma, while other programs have stalled, paused, or struggled to launch in Indiana, Kentucky, Nevada, North Carolina, Wyoming, and Washington, D.C.[144] Accessibility failures, procurement controversies, implementation barriers, public opposition, and shifting political priorities have already disrupted digital ID deployments across multiple jurisdictions. These examples demonstrate that digital ID systems are neither inevitable nor irreversible. They also illustrate that maintaining meaningful protections, human oversight, accessibility, and parallel non-digital systems requires substantial public investment and administrative capacity, issues explored further in the report's discussion of rethinking identity systems and resourcing meaningful protections.

Ensure people can…	Pass mandates that…
Challenge and reverse harmful digital ID systems through litigation, public pressure, accessibility complaints, procurement oversight, and legislative advocacy. Preserve access to services when digital ID programs fail, stall, or are withdrawn. Demand transparency around failed, suspended, or abandoned digital ID deployments and vendor contracts. Advocate for the sunset, repeal, or dismantling of systems that create exclusion, surveillance, accessibility barriers, or privatized control over public infrastructure.	Require periodic legislative review and sunset provisions for all digital ID programs. Create clear public off-ramps and termination procedures for harmful or nonfunctional digital ID systems. Mandate independent audits of accessibility, civil rights impacts, security failures, procurement practices, and vendor influence. Require public reporting on stalled, suspended, deactivated, or abandoned digital ID deployments and the reasons for their failure. Prohibit agencies from making digital ID systems mandatory when equivalent physical or human-mediated alternatives remain available. Restrict sole-source procurement and long-term vendor lock-in agreements for identity infrastructure.

[144] "Digital ID Systems - Policy, Tech, Uses, Protections." Spreadsheet. Accessed May 25, 2026. https://docs.google.com/spreadsheets/d/1EKzZqsLUG_r_H7lby06US4aURRl7-r4Doixdgq4p-2g/

Protecting Dignity, Human Rights, and Democracy

As demonstrated, digital ID systems increasingly facilitate harm across dignity, human rights, and democracy. Existing constitutional, civil rights, disability rights, labor, administrative, consumer protection, and privacy frameworks contain important protections intended to safeguard these values, but many were not designed to fully address interoperable digital ID systems operating at this scale. Protecting dignity, human rights, and democracy therefore requires both enforcing existing legal protections and developing new safeguards responsive to digital ID systems.

Democratic Participation

Democratic governance principles include the right of people to participate meaningfully in decisions about systems that govern them, yet digital ID systems are expanded through technical and administrative processes that largely bypass public input, exposing gaps that require new statutory protections. Governance must be open, participatory, and accountable. Otherwise, IDs entrench surveillance without the consent of the governed.

How corporate sale of data, mergers, and acquisitions of technology vendors serving governments create security crises around the world are foreseeable yet often ignored consequences of tech companies' entanglement with governments globally.

Ensure people can…	Pass mandates that…
Participate in consultations, hearings, and advocacy campaigns. Demand transparency and collective control over technology procurement and ID policies. Organize collectively to challenge opaque or harmful ID practices.	Require open rulemaking and community consultation before any deployment of a digital ID system. Create statutory public oversight boards with authority to review and veto contracts, standards, or procurements. Prohibit "buried legislation" by requiring standalone bills for major ID expansions. Mandate transparent public briefings on identity system contracts, vendors, and data sources. Incentivize open-source, auditable tools in procurement. Fund public education programs on risks and rights.

Free Expression and Association

Free expression and association depend on the ability to speak, read, organize, explore ideas, and participate in civic life without constant identity verification or monitoring. Digital ID systems increasingly threaten these freedoms by making participation in online forums, protests, public meetings, platforms, and access to information contingent on persistent identity

checks, biometric verification, or behavioral monitoring. As identity verification expands across digital and physical spaces, people may avoid seeking information, joining communities, attending protests, or expressing dissent out of fear that their activities will be tracked, profiled, or later used against them.

Ensure people can…	Pass mandates that…
Access information, online platforms, and public spaces without mandatory identity verification or biometric enrollment. Participate in protests, political organizing, mutual aid, religious communities, and civic associations without pervasive surveillance or identity tracking. Read, browse, communicate, challenge, and explore controversial or sensitive topics without being forced to disclose their identity. Use pseudonymous, anonymous, and encrypted services for speech, organizing, and community participation.	Prohibit mandatory digital ID or biometric verification requirements for accessing lawful online speech, forums, or informational resources. Ban facial recognition surveillance at protests, religious gatherings, libraries, schools, and other protected spaces for speech and association. Restrict the use of identity verification systems for monitoring political activity, protest participation, immigration status, or ideological affiliation. Protect the right to anonymous and pseudonymous participation online and in civic life. Require strict scrutiny, transparency, and public debate before implementing identity verification systems that affect free expression or association rights.

Privacy

Existing privacy and consumer protection laws and constitutional frameworks did not anticipate cross-context digital ID systems. Privacy is the foundation of freedom. International human rights frameworks recognize that no person should be subjected to arbitrary interference with their privacy, family, home, correspondence, honor, or reputation.[145] Without privacy protections, digital ID systems risk becoming tools of constant tracking, profiling, and surveillance. People must have the ability to shield their data, and legislators must ban invasive defaults. Some jurisdictions have already begun establishing privacy protections for digital ID systems, including limits on data collection, retention, sharing, mandatory use, and device searches.[146]

[145] Universal Declaration of Human Rights, art. 12 ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.")
[146] See, e.g., New Jersey A3518 (2025) (establishing privacy protections for digital driver's licenses, including limits on data collection, retention, device searches, and mandatory use of digital IDs); Utah SB 275 (2026) (establishing a "Digital Identity Bill of Rights" focused on consent, privacy, and user control protections for digital ID systems); Jay Stanley, "Utah Enacts Landmark Digital Identity Protections," American Civil Liberties Union, March 27, 2025, https://www.aclu.org/news/privacy-technology/utah-digital-id-law."

Ensure people can…	Pass mandates that…
Opt out of biometric enrollment and use non-invasive alternatives. Mask or anonymize themselves in public spaces to reduce surveillance. Challenge discriminatory ID practices through protest, litigation, and public campaigns. Limit their digital footprint by using encrypted tools, avoiding oversharing, and adopting privacy-preserving platforms.	Ban mandatory biometric enrollment, especially in sensitive areas like immigration, policing, healthcare, and education. Prohibit warrantless law enforcement access to ID systems or related databases. Limit the collection, retention, sharing, and cross-context use of identity data for compliance, fraud prevention, or eligibility verification purposes. Require organizations to use the least invasive identity verification methods possible, prioritizing contextual, in-person, or non-persistent verification over universal identifiers and interoperable tracking systems. Require independent third-party audits of all retention, linkage, and data-sharing practices. Enact data protection laws based on contextual integrity[147]. Reduce reliance on universal persistent identifiers such as Social Security numbers and prohibit the unnecessary expansion of biometric identification systems. Support decentralized, open-source, privacy-preserving ID models. Promote international safeguards against biometric surveillance, interoperability mandates, and cross-border identity tracking.

Autonomy and Self-Determination

Human rights principles recognize legal identity and recognition before the law as foundational to autonomy and participation, including the right to a nationality[148], yet digital ID systems increasingly fix identity in rigid, invasive and expensive ways that existing law only partially constrains. Identity is not static. Systems must allow people to self-determine and update how they identify themselves without undue barriers or fees. Otherwise, digital IDs harden categories that erase individuality and deny agency.

[147] Nissenbaum, Helen. "Privacy as Contextual Integrity." *Washington Law Review* 79, no. 1 (2004): 119. https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10.
[148] Universal Declaration of Human Rights, art. 15 ("Everyone has the right to a nationality" and "No one shall be arbitrarily deprived of his nationality nor denied the right to change his nationality.").

As identity and reputation become increasingly machine-readable, interoperable, and commercially valuable across platforms, these systems also create new opportunities for exploitation. Grammarly, for example, capitalized on their collection of identity plus programmatic data it collected from subscribers and began offering AI-generated 'editor' personas modeled on professional writers and editors, including journalists like Julia Angwin, without their consent, prompting a proposed class action lawsuit that may test how courts address emerging harms around identity, labor, and AI-generated likeness.[149]

Ensure people can…	Pass mandates that…
Assert control over names, gender markers, and attributes. Correct errors and update records without undue barriers. Give or withhold meaningful consent before data is collected or shared.	Require systems to allow self-identification and attribute updates (e.g., name, gender, address) without excessive documentation or cost. Mandate informed, revocable consent for all collection and sharing of identity data. Establish judicial oversight of disputes involving errors, exclusions, or denials. Restrict ID requirements to necessary contexts only, enforcing a "least privilege" principle. Abolish reliance on discriminatory identifiers (SSNs, mandatory biometrics). Support decentralized, auditable, non-biometric ID alternatives.

Equity

Human rights principles of equality and non-discrimination require equitable access in practice, a standard that digital ID systems routinely fail to meet, and that existing civil rights law has not yet adequately enforced in digital identity contexts. Digital ID systems often exclude those already marginalized. Equity means fair access for everyone regardless of income, housing status, gender, age, immigration status, or documents. Without it, digital ID systems become gates of exclusion.

Ensure people can…	Pass mandates that…
Challenge exclusionary practices that block access. Use flexible, non-biometric alternatives when standard documents are missing or expired.	Require equity impact assessments for all digital ID programs before launch, with results made public. Mandate multiple verification pathways (non-biometric, community-based, in-person) as a condition of funding.

[149] Klee, Miles. "Grammarly Is Facing a Class Action Lawsuit Over Its AI 'Expert Review' Feature." *Wired*, n.d. Accessed May 10, 2026. https://www.wired.com/story/grammarly-is-facing-a-class-action-lawsuit-over-its-ai-expert-review-feature/.

Secure equal opportunities to verify identity regardless of circumstances.	Prohibit exclusion based on expired, missing, or nontraditional documents (community attestations, letters from service providers). Establish oversight to monitor disparate impacts and halt deployments that exacerbate inequity. Guarantee accessible enrollment (multilingual options, disability accommodations, fee waivers).

Access to Justice

Without explicit remedies tailored to digital identity harms, existing legal protections often fail to provide meaningful recourse, reinforcing the need for new statutory rights and enforcement mechanisms. Without enforceable remedies, rights are empty. People need courts and regulators empowered to punish those responsible for violations and compensate for harms so that governments and corporate officials are held accountable for digital ID harms. Recent proposed state legislation has begun to outline what these protections could look like, including bills that would limit law enforcement access to biometric information, require meaningful consent for digital ID systems, and create private rights of action for individuals harmed by misuse or abuse.[150]

Ensure people can…	Pass mandates that…
Pursue damages through courts; join or initiate class actions. Seek collective remedies for systemic violations.	Create a private right of action for harms caused by digital ID systems, covering economic, psychological, and reputational harms. Empower state attorneys general to enforce violations with escalating penalties. Permit class actions to secure remedies for communities, not just individuals.

Transparency and Accountability

Existing transparency and fairness obligations offer limited insight into how identity systems function in practice, leaving lawmakers to decide whether new statutory disclosure, audit, and accountability requirements are necessary. Transparency is essential for accountability. People cannot trust systems they cannot see into. Clear rules on disclosure and auditing ensure IDs are not black boxes of surveillance.

[150] Ill. H.B. 5521, 103d Gen. Assemb., Reg. Sess. (2024) (restricting law enforcement access to biometric identifier information and providing a private right of action); Mo. S.B. 921, 102d Gen. Assemb., 2d Reg. Sess. (2024) (establishing consent requirements for digital identification systems, creating a private right of action, and authorizing civil penalties for violations).

Ensure people can…	Pass mandates that…
Demand transparency in why ID is requested and how data will be used. Access clear information about error rates and failures.	Require vendors and agencies to publicly disclose all processes, data sources, and vendors. Mandate continuous public audits and publish identity proofing error rates.

Questions to Rethink Identity

Rethinking digital ID systems requires more than designing less invasive forms of identification. It requires questioning why so many institutions increasingly rely on continuous ID checks, behavioral monitoring, and individualized gatekeeping in the first place, both online and offline.

As digital ID systems become easier to spoof, automate, and scale, they also expose the limits of systems built around constant surveillance, suspicion, and proof of deservingness. Rather than expanding digital ID systems into more areas of life, advocates and policymakers should move through a series of threshold questions before introducing new ID checks. First, is an ID check actually necessary in this context, or has identification simply become a default administrative response to risk, liability, or convenience? Second, can the underlying harm be addressed collectively or structurally without relying on individualized surveillance or gatekeeping?

Only after those questions are exhausted should institutions ask whether ID checks can be implemented in ways that are narrowly tailored, rights-protective, accessible, and meaningfully resourced in practice. Systems that depend on constant monitoring, appeals processes, human review, accessibility accommodations, and parallel non-digital alternatives require substantial long-term public investment and oversight, not merely technical promises or policy language on paper.

Do We Actually Need ID Checks Here?

Long-standing free expression principles caution against unnecessary identification in civic contexts; services should not make identity proofing the default barrier to participation.[151] Many digital ID systems emerge from intentional efforts to sort, rank, monitor, and restrict access to goods, services, and participation, while others become normalized through bureaucratic expansion and routine administrative practice. For example, DHS has used identity verification systems for both Privacy Act and Freedom of Information Act (FOIA) requests, even though identity verification is generally only necessary for requests seeking personal records under the Privacy Act.[152] Extending these requirements to ordinary FOIA requests can delay access, deter requesters, and transform a right to know into another identity checkpoint. Reducing reliance on digital ID systems therefore requires questioning whether identity verification is necessary in

[151] *Universal Declaration of Human Rights*, art. 21 (protecting the right to a secret vote).
[152] Freedom of the Press. "You Filed a FOIA, Then the Agency Wrongly Demanded ID. What Now?" August 31, 2025. https://freedom.press/the-classifieds/you-filed-a-foia-then-the-agency-wrongly-demanded-id-what-now/.

the first place, whether systems actually need to operate at the scale they currently do, and whether public goods can instead be delivered through lower-surveillance, lower-barrier, and more trust-based models.

Ensure people can…	Pass mandates that…
Access public goods and services without unnecessary identity verification, surveillance, or digital tracking. Use alternatives to formal identity systems, such as community attestations, clerk-based discretion, trusted intermediaries, vouchers, or anonymous and low-data access pathways. Participate in civic and public life without ID checks becoming the default condition of access.	Prohibit ID requirements for routine civic participation (voting, attending meetings, receiving basic benefits). Require agencies to apply the principle of necessity before instituting ID checks. Fund pilot programs that provide universal or anonymous access models (e.g., lotteries, non-tracking tokens). Codify the right to non-biometric pathways for accessing all public services.

Can We Address Harms Collectively Without ID Checks?

Identity-based risk scoring and fraud controls raise serious concerns under principles of equity and fairness, particularly when automated systems produce exclusion without clear accountability or recourse. More broadly, digital governance systems increasingly attempt to solve social problems through pervasive identity verification, behavioral monitoring, and continuous eligibility checks imposed on individuals. But many harms are better addressed structurally and collectively rather than through expanding surveillance infrastructures.

Fraud prevention, for example, should focus on organized abuse, corruption, labor and tax enforcement, and large-scale financial exploitation, not constant ID checks and behavioral profiling of ordinary people. Likewise, efforts to protect children online increasingly rely on age verification and identity checks that expand surveillance for everyone. Yet many online harms are better addressed through safer platform design, stronger protections for minors, limits on manipulative recommendation systems, advertising restrictions, interoperability, and meaningful platform accountability. When systems are made safer and fairer at the structural level, the pressure to impose pervasive identity checks on individuals diminishes.

Ensure people can…	Pass mandates that…
Access services without being subjected to pervasive surveillance, behavioral profiling, or automated suspicion in the name of fraud prevention.	Prohibit algorithmic risk scoring for benefits until proven non-discriminatory through independent equity audits. Require agencies to publish fraud-prevention rationales and conduct equity impact assessments before implementation.

Challenge unnecessary ID checks, document exclusion, and harms caused by risk scoring or automated fraud systems. Receive services through systems designed to address fraud structurally rather than by continuously monitoring individuals. Access safer digital environments created through structural safeguards rather than being subjected to pervasive age or identity verification.	Mandate macro-level anti-fraud strategies, such as beneficial ownership disclosure, anti-corruption enforcement, labor and tax enforcement, organized crime investigations, and oversight of large-scale financial abuse, over pervasive identity surveillance, behavioral profiling, and continuous ID checks of individuals. Enact public oversight boards to review fraud prevention strategies, with the authority to veto harmful systems. Require platforms and public agencies to prioritize structural safety measures, including safer platform design, stronger privacy protections, limits on manipulative recommendation systems, and meaningful human oversight, before imposing new identity verification requirements.

If ID Checks Cannot Be Avoided, How Do We Resource Meaningful Protections?

Many public institutions historically accepted a degree of ambiguity, anonymity, human discretion, and administrative inefficiency in exchange for accessibility, privacy, free inquiry, and democratic participation. Librarians, for example, are increasingly aware of the need to limit data retention, reduce punitive enforcement mechanisms, and minimize identity requirements in recognition that constant surveillance and verification can undermine public trust.[153] Public systems should not treat frictionless identity verification, interoperability, behavioral monitoring, and automation as inevitable or inherently desirable goals.

Ensure people can…	Pass mandates that…
Access public goods without continuous identity verification or surveillance. Maintain privacy, anonymity, self-determination, and meaningful human discretion when accessing public services. Use in-person, low-data, non-digital, and community-based pathways for accessing essential services. Participate in civic and public institutions without being forced into interoperable identity systems or persistent behavioral monitoring.	Require public institutions to absorb the administrative costs of protecting privacy, accessibility, and human rights, including maintaining in-person, low-data, and non-digital pathways for accessing services. Recognize privacy, anonymity, self-determination, and freedom from constant identity verification as public goods, even when preserving them introduces administrative inefficiencies or limits optimization. Require agencies to justify why identity collection is necessary rather than treating identification as the default condition of access.

[153] Wang, Tian, Chin, Chieh-Li, Benner, Christopher, M. Hayes, Carol, Wang, Yang, and Bashir, Masooda, "Patron Privacy Protections in Public Libraries" *The Library Quarterly,* Vol. 93, No. 3, July 2023, https://www.journals.uchicago.edu/doi/abs/10.1086/725069.

	Encourage low-data and low-retention service models in public institutions. Limit retention of identity and behavioral data when not strictly necessary for service provision. Preserve spaces for anonymous, pseudonymous, and low-barrier participation in civic and public institutions.

A Call to Halt Digital IDs

As they exist today, digital ID systems are flawed tools that unnecessarily exacerbate existing harms and introduce new threats to privacy, equity, and democracy.

They entrench exclusion and normalize invasive data practices rather than providing real security or public benefit. Passing new mandates for mobile driver's licenses, age verification, or other digital ID schemes without enforceable safeguards will only accelerate these harms: people denied services, youth blocked from online communities, sensitive data exposed, and public funds diverted into vendor contracts that fail at scale.

The choice is urgent and clear. Halting further digital ID expansion until enforceable rights and democratic safeguards are in place, preserving in-person and physical documents, and questioning identity are the only ways to protect dignity, equity, and freedom. The future of identity should not be built on more sophisticated surveillance but on systems that respect human rights and collective self-determination.