Understanding the Risks of Digital IDs
Community FAQs

IMMIGRANT DEFENSE PROJECT

Governments are increasingly relying on corporate technology and massive database systems to identify, categorize, and track people. Digital IDs are one of these tools.

While digital IDs may seem convenient (like a driver's license on your phone or an online ID), they also increase state power and systems of control. Government-issued IDs must prioritize our security and rights—but digital IDs more often compromise our rights and put our identification systems at further risk.

Biometrics

Biometrics are physical measurements of different body parts (iris, fingerprints, face, DNA) used for identification purposes. They are typically unique characteristics that can be used to verify identities.

Biometrics collection has been used as a tool to increase the power of police, government, and private companies to identify, monitor, and track people.

Data sharing

Data sharing is the often automated sharing of vast datasets on people's identities and lives. Local, state, and federal agencies increasingly share data between their systems. Private companies also collect, sell, and share data with government agencies.

What's behind the push for digital IDs?

Digital IDs are part of larger systems of surveillance, biometrics collection, data sharing, and control. They function as massive databases that collect, store, and track sensitive info about our identity and actions. Governments and private companies use digital IDs to identify and track us—and then allow or deny us access to rights and resources.

Digital IDs are increasingly an example of **"smart-city" projects**, where governments and corporations claim that "smart," tech-based "solutions" can fix problems like access to banking and inefficient social services. However, what digital ID proponents don't tell us is that digital IDs and smart-city projects often increase inequity and hurt the communities they supposedly aim to help.

Communities are rarely consulted about these projects before they happen. Digital IDs are often driven by **"public-private partnerships,"** where governments contract private companies to provide what is typically a public service. This gives companies control of our personal information, government institutions, and resources with little accountability. Decisions are made to increase corporate profits, not to meet community needs.

Digitizing city systems is not necessarily a bad thing—but digitizing sensitive information and tying it to our identities can easily lead to increased surveillance and deny people access to basic rights and resources.

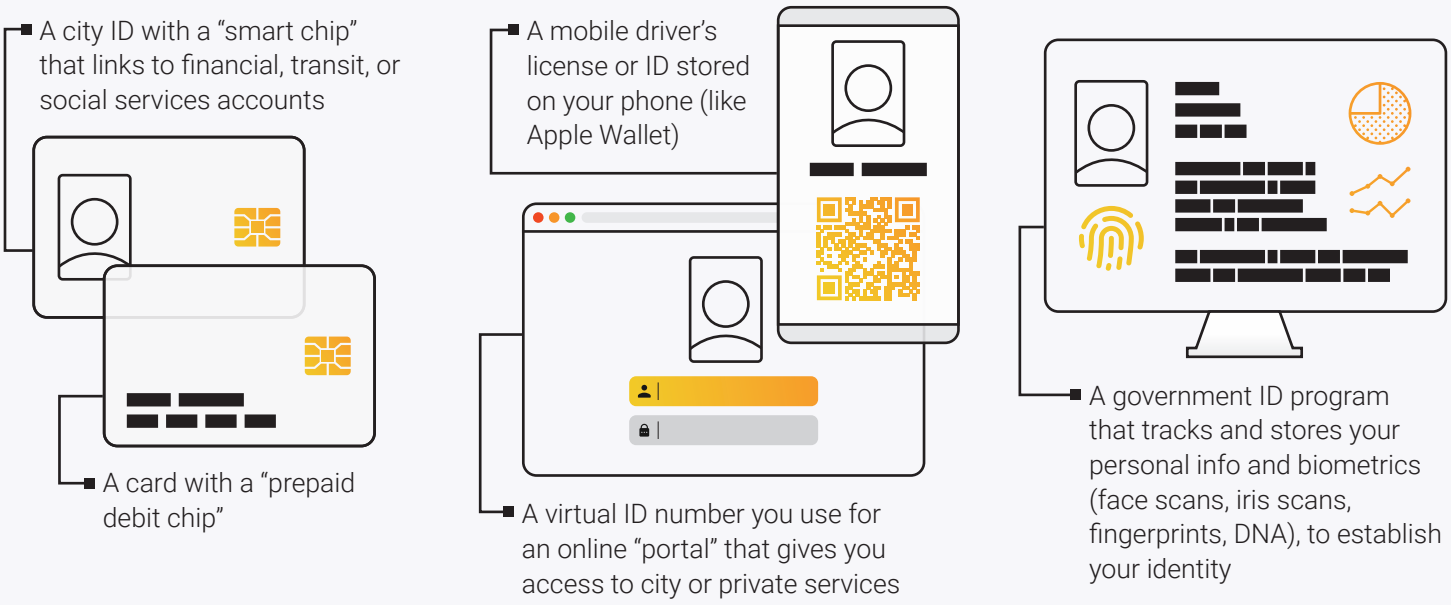
Learn more in IDP's Digital ID resources

Credits: This resource was created by the Surveillance, Tech & Immigration Policing Project, at the Immigrant Defense Project, and designed by Objectively.

What are Digital IDs?

Digital IDs are massive databases that track and store sensitive info about you and your actions. They combine your identifying information with a mobile tracking device, which could be your smart phone or ID card.

Digital IDs can look like:



In this FAQ, we're talking about digital IDs issued or used by local or national governments. You may have many other virtual IDs (like a social media account).

The Four Big Risks of Digital IDs—and Digitization of City Services

Real-life experience across the world and the US show that digital ID systems:

1	**Exclude residents from government services.** This is an increased risk when governments mandate that people use a digitized service to access benefits or resources. People with disabilities, elders, and low-income communities are often left out.	**Example:** When Ireland created a digital ID and used it to distribute social benefits, working-class and disabled people were excluded.
2	**Expose governments and residents to massive data breaches and privacy risks** from hacks, data sharing, and abuse by third-party companies.	**Example:** Baltimore lost control of its government services for weeks after a 2019 "ransomware" attack, which cost the city over $18 million in recovery spending and lost revenue.
3	**Increase surveillance, monitoring, policing, and data collection without consent** on Black, brown, and immigrant communities already subject to discriminatory policing and invasive surveillance.	**Example:** The Los Angeles digitized financial aid card puts undocumented residents at risk, by sharing data with companies that sell people's information to ICE.
4	**Take away resources for community-led initiatives, and redirect funds to corporations** that don't fix what they claim to solve.	**Example:** Instead of expanding banking access, Oakland attached a prepaid debit card to its city ID that charged high fees to low-income people.

How do Digital ID Systems Work?

Digital identity systems are massive databases that collect, store, and track sensitive info about people's identity and actions. They use technology to establish and prove your identity, often by collecting and linking your sensitive personal information, and to track you. This data can include your biometrics, health records, travel, and purchases. There are very few data protections against sharing this information with corporations and police.

IDENTIFY → AUTHENTICATE → AUTHORIZE

IDENTIFY

Attributes are pieces of your personal information or data that connect to your identity. They can be **biographic** or **biometric**.

Biographic

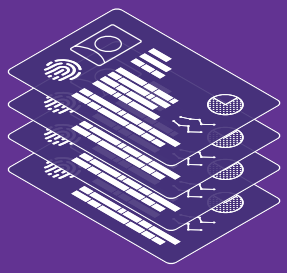
- Name
- Age
- Location
- DOB
- Gender

Biometric

- Face scan
- DNA
- Iris scan
- Fingerprints

AUTHENTICATE

Digital ID systems collect and store our information and use that to check or verify our identities.



AUTHORIZE

Digital IDs can introduce bias into the core of benefit systems, including algorithms to determine who is eligible.

Allowed
You're granted access to government benefits.

Excluded
You're denied access to your government benefits.

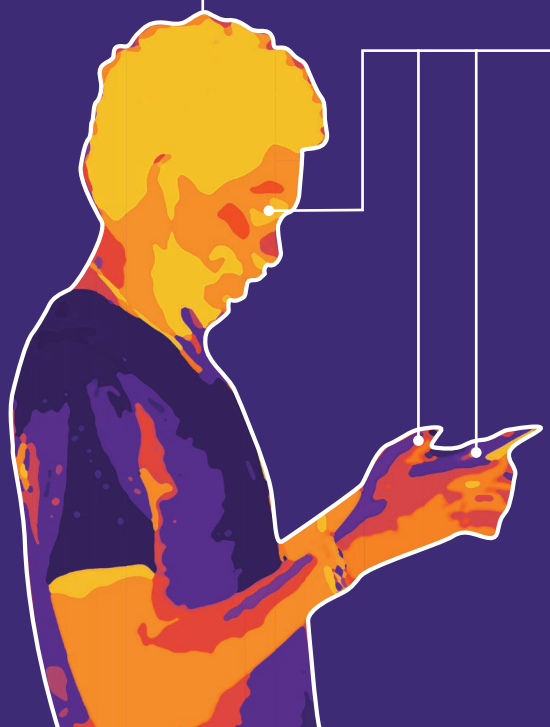
How does the digital ID system track you?

Digital ID systems typically assign each person **a unique number or identifier** and link your biometric and biographic attributes to that number.

Your number and information is linked to your "**access key**" or "**credential**," which you use to prove your identity. **This credential is a digital or physical tracker that you carry with you:**

A digital credential can be on your **smartphone** or linked to your **face**, **iris**, or **fingerprint** data.

A physical credential can be a card with a "**smart chip**" that tracks its use or location.



This information in this graphic is partially based on: Nyst, Carly, Steve Pannifer, Edgar Whitley, and Paul Makin. "Digital Identity: Issue Analysis." Consult Hyperion, June 8, 2016. https://chyp.com/wp-content/uploads/2020/06/PRJ.1578-Digital-Identity-Issue-Analysis-Report-v1_6-1.pdf.

Why should I be concerned about Digital IDs?

Digital IDs aren't far away: they're here. We don't need more public-private partnerships to develop them. We need proactive policy and action to limit and regulate digital IDs now.

Here are six reasons why you should be concerned about Digital IDs:

1 **Digital ID systems threaten our physical and digital safety, privacy, and access to constitutional rights and basic resources.** Companies sell digital IDs as a "solution" to a wide range of problems like government inefficiency—but in reality they have rarely solved these issues and instead create more dangers.

2 **Digital ID systems gather billions of data points of our private information, often without our consent or knowledge.** This data can include our intimate biographic info (date of birth, location, SSN), biometrics (face scans, fingerprints, DNA, iris scans), banking info and transactions, and real-time location if IDs are used for public transit.

3 **All this data has been used to surveil us and monitor our every move.** This always hits communities targeted by racially-biased policing the hardest—like unhoused and undocumented people in Los Angeles.

4 **Digital IDs often do not keep us or our data safe, and rarely improve government efficiency.** This data collection exposes us to cybersecurity attacks and data breaches—like in Baltimore and South Korea.

WARNING
Digital ID systems can increase the threat of surveillance, policing, and exclusion from government services!

5 **Digital IDs can exacerbate inequality.** Governments increasingly use digital IDs and automated AI systems to decide who is eligible for social services. This sounds convenient but can cut off people's access to essential benefits. When Indiana automated its public benefits systems in 2007, more than 700,000 people were unjustly denied benefits like Medicaid. In the US and globally, digital ID systems can most harshly impact low-income and unhoused people, people with disabilities, the elderly, trans and non-binary people, heavily-policed groups, and non-citizens.

6 **Digital ID systems take away our control of our own communities.** Tech-driven services often offer misguided and damaging "solutions" that make problems worse. Corporations sell digital ID systems and keep the profits, redirecting essential government resources away from community initiatives and long-term urban planning.

"The State is forcing me to trade my private data in exchange for access to services to which I am legally entitled."

An Irish teacher denied welfare benefits after she refused to get the Irish digital ID

Breaking Down the Myths of Digital IDs

Governments and companies claim they solve a range of problems—but a decade of research shows that they hurt the communities they seek to help. Let's break down these myths to understand how.

Myth: Digital IDs are more secure than paper systems.

Fact: Digital ID systems are not more secure. They expose us to identity theft, massive data breaches, and major privacy concerns.

Many ID systems are implemented without adequate data protection legislation or security. In these cases, to "prevent fraud," governments and corporations are instead establishing invasive surveillance networks, with little oversight, and exposing themselves and residents to security breaches and increased fraud. Even Estonia, the poster child of digital identity, has had security issues, with an encryption incident in 2017 putting 760,000 people at risk of identity theft.

In the US, the digitization of city services has led to severe security breaches. This includes over 400 recorded "ransomware" attacks on US city and county governments since 2016—where hackers lock users out of their accounts and demand a ransom to return their data or restore access. After a 2019 attack, Baltimore lost control of its government services for weeks, costing the city over $18 million in recovery spending and lost revenue.

Fact: Digital ID systems give control of our data to private companies, which profit off our information and use that data to try to modify our behavior.

There are huge privacy concerns related to sharing personal information with private companies, like financial institutions. Companies profit off our data, and the way it is used for surveillance and policing.

For example, Mastercard—a huge player in the digital ID market—has based part of its business model on expanding credit card use and data collection. While the company insists it values privacy, they often collect and sell people's data without users' consent and knowledge. In 2018, the Electronic Privacy Information Center filed a complaint with the US Federal Trade Commission over a secret data-sharing agreement between Mastercard and Google, which affected the company's 2 billion cardholders.

Myth: Digital IDs are more effective and convenient.

Fact: Perceived "convenience" comes at a huge cost. Digital IDs often create new problems.

Even if the "goal" of the digital ID program is to do good, it is difficult to ensure that the system will be safe. Collecting large amounts of personal and biometric data always creates opportunity for abuse, even when the program's purpose seems to be positive.

Fact: Digital IDs are not necessarily more effective at cutting costs or tackling corruption.

For example, Apple has been criticized for pushing the costs of its US digital ID program onto taxpayers. Most digital ID programs rely on corporations like Apple or IDEMIA, and this redirects public funds and control of our private information to companies that are not accountable to us.

Fact: Digital IDs expose people to increased surveillance and policing.

Digital ID systems collect massive amounts of personal and biometric info and share that data with companies and government agencies. This threatens our digital and physical security, both from corporate surveillance and policing fueled by data sharing.

Digital IDs easily become another way of cataloging people—by police, welfare, immigration, refugee, or other databases—and centralizing and sharing this data. This increases the capacity of the state and companies to monitor, regulate, and punish us.

Myth: Digital IDs expand access to resources.

Fact: Digital ID systems and automation of benefits can increase marginalization and exclusion.

While digitization can have benefits, automating eligibility determinations for social services can introduce bias into the core of the benefits system, cutting off people's access to these essential resources. For example, more than 700,000 people were denied benefits when Indiana automated its welfare system. When governments make digital IDs mandatory to access rights or resources, exclusion gets worse.

> **"They gave me no reason [why my Medicaid was denied after 10 years]. To get a reason, I had to send a letter in to say I wanted a reason so I just re-applied. I just went in for an appointment to re-certify and the lady said, 'You're not going to get it.'"**
>
> **Teresa Ford, denied Medicaid after Indiana automated its benefits system**

Myth: Digital IDs help expand banking access.

Fact: Digital ID systems do not close wealth gaps and can reinforce systemic exclusion.

Governments and companies promote digital IDs with attached financial services as a way to address people's lack of access to banking. However, having an account doesn't mean people have money to deposit. In addition, these financial "inclusion" programs are often sold by financial technology ("fintech") companies that do not provide the same security and services as banks. Instead, they promote second-tier products for poor and working-class people, which reinforces economic injustice.

For example, prepaid debit cards are often promoted as a "solution" for people without bank accounts. But these programs, like in Oakland, have high transaction fees, and maintain a two-tiered banking system that increases marginalization.

> **"For decades, prepaid debit card companies have touted their product as a solution to "banking deserts" and, for decades, the rhetoric has failed to match the reality. There is no compelling reason for the City of New York to steer IDNYC cardholders to this service, much less to connect it to people's identity cards."**
>
> **New Economy Project**

What happens when digital IDs become mandatory?

After over a decade of digital ID implementation around the globe, the research shows that:

- **Requiring people to register for or use digital IDs excludes historically marginalized groups**—such as non-citizens, trans and non-binary people, rural communities, people with disabilities, and the elderly.
- **People may have trouble registering for digital IDs**, due to lack of documentation, fees, failures and bias in biometrics software, inaccessible registration facilities, and language barriers.
- **Non-citizens can be denied services or tracked** if they submit their personal and biometric data.
- **People may be coerced into submitting their sensitive data**, if it's the only way they can access basic services.

How can we fight for more equitable digital systems?

Digital IDs and smart-city projects aren't far away: they're here. We don't need more flashy new technologies. **We need proactive policy and action to limit and regulate digital IDs**. We need to redirect resources toward our communities' long-term demands to address systemic inequality and discrimination.

We must prioritize our communities over corporations and make sure the most marginalized are not left behind. Governments must ensure that policies to protect our rights are at the foundation of any data system. Since few laws protect our data—especially from corporations and police—any information that is collected can be used to fuel surveillance, policing, and other forms of abuse. This is a particular concern when our info is combined into massive databases.

For more ideas on how to engage, check out IDP's Digital ID resources.

IMMIGRANT DEFENSE PROJECT

@ImmDefense

immigrantdefenseproject.org

IDP's **Surveillance, Tech & Immigration Policing** project challenges ICE policing and migration control at the intersection of the criminal legal and immigration systems. This includes tackling the rapidly expanding role of tech corporations in local governance. The project supports organizing to build the collective knowledge and political infrastructure to end state violence and to grow a just digital future.

Learn more at: immigrantdefenseproject.org/surveillance-tech-immigration-policing