Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Elise Quevedo

Safeguarding human dignity in a digital identity world

This one has been brewing for a while. For years, digital identity has been a conversation happening in closed rooms, among policymakers, legal experts, and a handful of tech innovators. But now, it is becoming mainstream. And whether we like it or not, it will affect every single one of us over the upcoming years.

In the UK, the topic recently reached a new milestone. The Data (Use and Access) Act received Royal Assent. This legislation is another step toward creating a trusted framework for digital identity verification. That might sound like bureaucratic jargon, but in plain language, it means the government has officially recognised that digital IDs are the future.

And the UK is not alone. Around the world, countries are moving fast, experimenting with digital ID systems designed to make our lives easier. At the same time, risks around privacy, scams, and security are growing louder.

So let us unpack what this means for us, the people behind the screens.

What Are Digital Identities?

At its simplest, a digital identity is an electronic version of your traditional identification. Think of your passport, driving licence, or national insurance number, translated into secure, encrypted, and verifiable digital form.

Instead of carrying multiple cards or submitting piles of documents every time you need to open a bank account, pass through airport security, or prove your age, you would use one secure digital ID.

> With every new door that opens, new vulnerabilities appear

It may sound like something out of a sci-fi movie, but it is reality. The US Customs and Border Protection (CBP) already promotes the Mobile Passport Control (MPC) app, which allows travellers to create a digital identity and speed up the customs process. Estonia has been living with a nationwide digital ID system for years. Singapore and India are also pioneers.

As always, there is a but. With every new door that opens, new vulnerabilities appear. And trust remains the biggest challenge.

The Trust Challenge

Why should you hand over your most sensitive personal data to a digital system? Who manages it? Who protects it? Who profits from it?

These are the questions governments and technology providers are scrambling to answer openly. For the public, scepticism is natural, and I raise my hand. I don't always jump onto the next digital trend as soon as it's out. I like to observe and analyse first.

> If trust is not addressed with transparency and accountability, the rollout of digital IDs will stall

Every headline about data breaches or identity theft makes us more hesitant. And when we talk about digital identity, we are talking about biometric data, fingerprints, facial recognition, and our most personal details.

If trust is not addressed with transparency and accountability, the rollout of digital IDs will stall.

The Leading Countries in Digital Identity

Some nations are already proving that digital identity can work when done right. Here are the top three leading the way:

Estonia

Estonia is often called the digital nation. Since 2002, every citizen has had access to a digital ID card. With this card, residents can access almost all government services, vote online, and pay taxes in a matter of minutes.

With the help of a solid legal system and public backing, trust has been developed over many years. A few years ago, I visited Tallinn and witnessed its level of development firsthand.

India

India's Aadhaar system is the largest digital ID programme in the world, with over 1.3 billion citizens enrolled. It makes use of biometric information, such as iris and fingerprint scans, connected to a distinct 12-digit ID number.

Aadhaar has drawn criticism for privacy issues as well as accolades for increasing access to services.

Singapore

Residents of Singapore can access over 2,000 public and private sector services through Singpass.

The system is respected, safe, and demonstrates how the public and private sectors may cooperate to guarantee successful implementation.

These countries are not perfect, but they offer important lessons for the rest of the world.

The Risks and Challenges

Every fresh opportunity has a drawback. Digital IDs carry with them the classic problems we hoped we could avoid.

First, privacy issues arise because digital IDs centralise personal information, making them a prime target for fraudsters. Second, exclusion, because access to technology is not universal. Vulnerable populations can be left behind if digital IDs are used without inclusive policies.

We must continue to raise awareness and have conversations about it

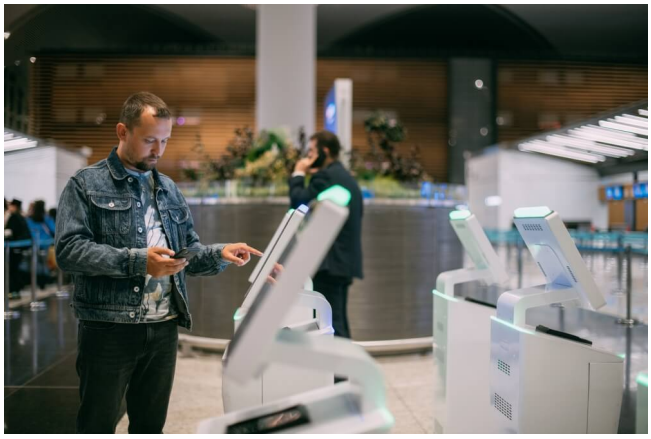
Third, government overreach, because detractors worry that digital IDs may be used as surveillance tools, granting governments excessive authority over people. And fourth, fraud and scams, because con artists are quick to adjust. Before safeguards are completely implemented, digital ID systems may be exploited by phishing, deepfake impersonations, and fake apps.

Nevertheless, the momentum is here in spite of these dangers. For this reason, we must continue to raise awareness and have conversations about it.

Why Governments Are Pushing Forward

Governments see digital IDs as a way to streamline bureaucracy, reduce fraud, and improve efficiency. For citizens, it is the promise of convenience: faster border checks, simpler access to healthcare, and smoother financial services.

Businesses also benefit. Banks, airlines, and online platforms all spend billions verifying identities. A standardised digital system would cut costs and boost customer satisfaction.



Identity verification is central to everything we do. Sticking with paper documents is no longer sustainable or safe

When I worked at one of the largest airports in Europe in my younger days, I was an authorised signatory, which meant I was someone nominated by the company to manage the application for and manage ID passes.

I was a gatekeeper of processing applications and verifying identities and references before someone would get access to the security airside areas. Back then, we did not have much digital processing. A lot of the processing was done manually and required a significant amount of person-hours.

The real driver now, though, is inevitability. Our lives are increasingly digital. Identity verification is central to everything we do. Sticking with paper documents is no longer sustainable or safe.

Predictions. What Comes Next?

I believe the UK's move with the Data (Use and Access) Act is only the beginning. Within the next few years, we will see the EU following suit.

The European Union is already working on its own digital identity framework, known as eIDAS. Once Denmark finalises its AI likeness protection bill, as I mentioned a couple of weeks ago, digital identity will become even more urgent to safeguard citizens.

> Once a few major countries prove it works, others will not want to fall behind

Expect big banks, airlines, and healthcare providers to integrate digital ID verification into daily services. Once a few major countries prove it works, others will not want to fall behind, as is the norm with any major change across the world.

We must demand transparency

Digital identities are about our lives, our privacy, and our freedom. So, we must demand transparency about how our data is stored and used.

Above all, we must stay informed, because ignorance is the biggest danger of all. The saying "out of sight, out of mind" will be our worst enemy otherwise.

As I wrote in last week's article on AI in banking, "With great power comes great responsibility." The same applies here. Digital identity has the power to simplify our lives and connect our world, but it also carries the responsibility to safeguard human dignity.

If digital identity becomes a global standard, what safeguards do you believe should be in place before you trust it with your life?