Digital Identity in the UK:

Promise and Peril

The UK government is once again considering the introduction of digital identity systems. Advocates argue that such systems can modernise public services, enhance security, and reduce fraud. Yet the experience of other countries — and Britain's own history with identity schemes — shows that digital ID carries significant risks that demand careful scrutiny.

The Case for Digital ID

Proponents highlight several potential benefits:

- **Efficiency and convenience:** Digital ID could simplify access to healthcare, banking, and government services, reducing paperwork and streamlining verification.
- **Fraud reduction:** By providing secure verification mechanisms, digital ID might help reduce identity theft and welfare fraud.
- **Economic potential:** A trusted digital identity system could support innovation in financial services and e-commerce.

These arguments resonate in a digital age where transactions increasingly occur online. However, the costs, risks, and unintended consequences must be weighed against these potential gains.

Lessons from the UK's Past

Britain has already been down this road more than once:

- **Identity Cards Act (2006):** Introduced a national ID scheme with a centralised register. Concerns over surveillance, cost, and civil liberties led to its repeal in 2010.
- **Connecting for Health (2002–2011):** The NHS's national IT programme sought to centralise patient records at huge scale. It cost more than £10 billion before being abandoned, proving how vulnerable large, centralised databases are to cost overruns and technical failure.
- **COVID-19 Vaccine Passport (2020–2021):** The government nearly introduced a nationwide digital credential system to regulate access to venues and services. Public debate quickly revealed this was, in effect, a form of digital ID. It was abandoned amid strong resistance, but it shows how easily digital ID can be introduced under another name.

These episodes underscore two recurring themes: the **public's mistrust** of government handling of sensitive data, and the **difficulty of justifying vast expenditures** for systems that are technically complex and politically unpopular.

International Experience

Denmark: A Qualified Success

Denmark is often cited as a digital identity success story. Its NemID system, launched in 2010, became integral to banking, tax filing, and public services. In 2021, it began transitioning to MitID to address security and usability concerns.

The Danish experience demonstrates that digital ID can achieve high levels of adoption and trust when:

- Systems are integrated seamlessly into everyday life.
- Strong legal and institutional safeguards are in place.
- Rollouts are accompanied by significant investment in digital literacy.

Yet the transition has not been without difficulty. Elderly citizens and those less digitally literate have struggled to adapt, highlighting risks of exclusion even in a digitally advanced society.

India and China: Cautionary Tales

India's Aadhaar system, the world's largest biometric ID project, has faced persistent issues, including individuals being denied food rations due to fingerprint mismatches. China's use of digital ID infrastructure within its social credit system shows how identity tools can be repurposed for political and social control.

These examples highlight the spectrum of outcomes: digital ID can enhance convenience, but without safeguards, it risks deepening inequality or enabling authoritarian overreach.

Key Risks for the UK

- **Privacy and surveillance:** Centralised ID systems create the potential for routine activities to be tracked and recorded, raising concerns about government overreach.
- **Cybersecurity:** A national digital ID database would be a high-value target for cyberattacks. Unlike passwords, biometric data cannot be changed if compromised.

- **Cost:** Past UK initiatives — from ID cards to Connecting for Health — consumed billions before being scrapped.
- **Exclusion:** Roughly 10% of Britons lack digital skills or reliable internet access, with disproportionate effects on the elderly, rural populations, and low-income households.

Policy Considerations

If the UK revisits digital ID, policymakers must consider:

1. **Voluntary vs. mandatory adoption** — Citizens should not be compelled into a system that risks exclusion or coercion.
2. **Decentralised design** — Minimising centralised data storage can reduce surveillance risks and limit the fallout of breaches.
3. **Robust legal safeguards** — Strong privacy protections and independent oversight are essential to prevent misuse.
4. **Inclusive access** — Any rollout must ensure support for those lacking digital skills or connectivity.
5. **Transparent costs and benefits** — Public trust requires clear evidence that digital ID offers net benefits compared to existing systems.

Conclusion

Digital identity is neither a panacea nor an inevitable step forward. International experiences show both the promise and peril of such systems. Denmark demonstrates that, with safeguards and careful integration, digital ID can deliver efficiency gains. India and China warn of the risks of exclusion and authoritarian misuse.

For the UK, the debate should not be framed as “digital ID or nothing.” Instead, policymakers must ask whether the benefits truly outweigh the risks, and if so, how systems can be designed to protect privacy, inclusion, and trust. Freedom and security are not mutually exclusive — but digital ID, implemented carelessly, could undermine both.

This is a paper published for discussion, please feel free to contact us with your thoughts, criticisms, observations and suggestions.