Consultation Response: Making public services work for you with your digital identity

Respondent: Freddie New, Co-Founder and Chief Policy Officer, Bitcoin Policy UK.

Summary

We fundamentally oppose these proposals. While the consultation document is carefully worded to emphasise convenience and choice, the underlying architecture being proposed, namely:

- a centralised system of digital identity verification,
- operated by the state,
- linked to biometric data, and
- intended to become the primary means of accessing public services,

represents one of the most significant expansions of state surveillance infrastructure in modern British history.

One should never create a system, or give oneself a power, that one would not want one's worst enemy to have. Digital ID would be exactly that kind of system, and would give extraordinary power to government over people's lives. It should be rejected outright, and no more public money wasted on efforts that so many already oppose.

1. "Voluntary" systems do not remain voluntary

The government states "there will be no legal obligation for people to have or present the digital ID." History teaches us that this assurance is meaningless. Systems introduced as voluntary become compulsory through function creep and practical necessity.

For example:

- National Insurance was introduced in 1911 purely for social insurance. Having an NI number is now a de facto requirement for employment, banking, and benefit access.
- Right-to-work checks are explicitly referenced in this consultation as an early use case. Anyone starting a new job "will be able" to use digital ID for these checks "by the end of this Parliament." How long before employers refuse to process paper alternatives?
- Identity checks for employment already take place, via passports, residence permits, and the like. A Digital ID scheme does not introduce a new safeguard, but simply centralises and digitises a process that already exists.

Once the infrastructure exists and public services are redesigned around it, opting out of Digital ID will mean opting out of society. This is compulsion by design, not by statute, which is arguably worse, as it circumvents Parliamentary scrutiny.

2. Centralised data stores are honeypots and the UK government cannot be trusted to protect them

The consultation makes the disingenuous claim that the system "will not create a centralised database." Even if data is nominally distributed, a system that allows the state to verify identity across all public services necessarily creates a centralised point of correlation. Whether the database is technically "centralised" or federated is irrelevant if the state can query across it.

It is no exaggeration to say that the UK government's track record on data security is already catastrophic:

- 2007: HMRC lost two unencrypted CDs containing the personal details of 25 million child benefit recipients (effectively every family in the country).
- 2022: NHS software provider Advanced was hacked, exposing patient phone numbers, medical records, and home entry details for over 80,000 vulnerable care patients.
- 2022: Ministry of Defence - sensitive personal data of over 18,000 Afghan nationals eligible for UK relocation was exposed. An 18-month, "superinjunction" suppressed this information until July 2025.
- 2023: The Police Service of Northern Ireland accidentally published the personal data of all 10,000 serving officers, in a region where such disclosure can be a death sentence.
- 2024: The Ministry of Defence (again): a cyberattack on an external payroll contractor compromised the personal details (names, bank details, and some addresses) of a large number of serving UK military personnel and veterans.
- 2025: The FCDO itself was hacked (confirmed by Chris Bryant MP in December 2025).
- 2025: A Cabinet Office review of 11 major public sector data breaches (HMRC, Met Police, MoD, benefits system) found systemic failures across government.

This is not ancient history but merely the last few years. It appears that in the UK, even the Ministry of Defence cannot defend itself against data breaches and leaks; and this is the government that now proposes to create a single identity infrastructure linking names, dates of birth, photographs, nationality, and biometric data to every interaction a citizen has with the state.

When (not if) this system is breached, the consequences will be orders of magnitude worse than any previous incident. You cannot change your biometric data. You cannot get a new face. And bad actors will have access to a wealth of personal information far more extensive and more damaging than any they have accessed before.

3. The surveillance architecture is the point

The consultation frames digital ID as a tool for convenience: faster access to tax codes, driving licences, benefits. But the architecture being described is far from being a convenience tool and should more properly be considered as a surveillance tool masquerading under a veil of convenience.

A system that:

- links biometric data to a unique identifier;
- is used across all government departments;

- is required for employment verification;
- is designed to "consistently identify people" across services; and
- will be expanded to the private sector;

is, by definition, a system of mass surveillance. The question is not whether it will be used for surveillance, since it will be; the question is when, and by whom.

The consultation makes no mention of:

- Judicial oversight for government access to identity verification logs;
- Warrants required before cross-referencing identity checks across departments;
- Prohibition on sharing verification data with law enforcement without a court order;
- Time limits on data retention; or
- Independent audit of government access patterns.

Without these safeguards, which are not proposed, and which no UK government has ever voluntarily imposed on itself, this system will inevitably be used for purposes far beyond its stated scope, and which the system's victims (namely every UK citizen) will be powerless to overturn.

4. The right comparison is not online banking but the Chinese Communist Party

The consultation repeatedly compares the proposed system to private sector conveniences like online banking. This is a false equivalence. When I use online banking, I have a contractual relationship with a private institution. I can change banks, or I can close my account. The bank cannot arrest me, deny me healthcare, or prevent me from working.

The correct comparison is in fact with state-administered digital identity systems in authoritarian regimes. The PRC's social credit system began with precisely the same language of "convenience" and "modernisation." India's Aadhaar system, being the closest democratic parallel, has been plagued by data breaches, exclusion of vulnerable populations, and mission creep into areas never contemplated at its inception.

The UK does not need to follow this path. The absence of a national identity system has been a persistent feature of British liberty, not a bug. We should be deeply suspicious of any government, and of any party that seeks to change this, and any party which does so should be punished at the ballot box at the next available opportunity.

5. The real losers are the most vulnerable

The consultation claims digital ID will help the excluded, whereas in fact the very opposite is likely to be true. Digitally excluded populations, such as the elderly, the disabled, those without smartphones, or those without stable housing, will be the first to be locked out when services migrate to a digital-first model.

The consultation acknowledges that 25% of the population struggles to use digital services and 1 in 10 lacks photo ID. Rather than addressing these problems at their root (problems such as poverty, digital illiteracy, or bureaucratic complexity), the government proposes to solve them by creating a new digital

system that requires a compatible smartphone, biometric enrolment, and digital literacy; in other words by doubling down on the very problems and issues that lead to difficulties in using digital services in the first place.

This is circular reasoning. The people who most need help accessing services are precisely those least able to navigate a new digital identity system.

6. Alternatives exist and are ignored by the consultation

The consultation presents a false binary: either we build a national digital ID system, or we remain trapped in "call centres, paperwork and hours on hold." This is absurd. There are well-established alternatives:

- Federated identity verification without a central state-controlled system (as used successfully in the Nordic countries with BankID, which is private-sector-led)
- Zero-knowledge proofs that allow verification without disclosure (e.g., proving you are over 18 without revealing your date of birth. ZKP is a technology that exists today)
- Decentralised identity standards (W3C DID) that give individuals control of their own credentials without any central authority
- Simply improving existing services. The consultation's own examples (tax codes, driving licences) do not require a new identity infrastructure; they require better-designed individual systems

The government has not demonstrated why a centralised state identity system is necessary when privacy-preserving alternatives exist.

Conclusion

I urge the government to abandon these proposals. The recent E-petition debate[1] on the issue saw resounding and cross-party opposition to it.[2] The UK's lack of a national identity system is far from a failure of modernisation, but should properly be thought of as a deeply rooted constitutional inheritance that reflects a fundamental principle: that **the state serves the citizen, not the other way around**. The Prime Minister spoke early on in his premiership about 'treading more lightly on all our lives'. Digital ID is in fact more akin to the boot at the conclusion of Orwell's '1984', stamping on a human face, forever.

No government should be building infrastructure that makes it easier to track, profile, and ultimately control its own population, regardless of how many times it uses the word "convenient." People should not be afraid of their government; the government should be afraid of its people. It is only by our good grace that they hold and retain power; and any party that supports Digital ID has demonstrated they are unfit to hold that power.

The question this consultation should be asking is not "how should we build digital ID?" It is "should we build it at all?" My answer is, and always will be, no.

---

[1] https://x.com/DecentraSuze/status/2008089097324101638?s=20
[2] https://www.youtube.com/live/dCGWpaAfJIw

Freddie New

Co-Founder and Chief Policy Officer

Bitcoin Policy UK

12 March 2026