

Joint Briefing on the “Do not introduce Digital ID cards” Parliamentary Petition Debate



Introduction

The 13 NGOs backing this briefing all oppose the Labour government’s plans for a mandatory digital ID, representing the vast numbers of people whose interests we represent. This position is informed by our varied expertise spanning privacy and data protection rights, equality rights and anti-discrimination, and immigration and migrants’ rights. This joint briefing for the 8th December 2025 debate on the digital ID Parliamentary petition summarises the most significant concerns associated with the government’s mandatory digital ID proposal. **We urge you to attend the debate on Monday 8th December and ensure that the government hears these concerns.**

In September, Prime Minister Sir Keir Starmer announced plans for a new digital ID scheme to be introduced and made mandatory for ‘right to work’ checks by the end of Parliament.¹ Since the announcement, the “Do not introduce Digital ID cards” Parliamentary petition has accrued more than 2.96 million signatures, making it the fourth largest petition in British history and the second largest non-Brexit petition.

Key issues:

Mission creep: Although the Prime Minister proposed the latest digital ID scheme in the context of immigration enforcement for ‘right to work’ checks, we have already seen the government promoting an expansive array of potential use cases. Minister for Intergovernmental Relations Darren Jones, signalled the government’s intent for the digital ID proposals to “shut down the legacy state”.² Additionally Children and Families Minister Josh MacAlister MP in an interview on GB News stated the Government was “starting with this issue of right to work check first -but there are loads of other applications for Digital ID”. He explained,

¹ Seddon, P. (2025, September 25). *Keir Starmer to announce plans for digital ID scheme*. BBC News. <https://www.bbc.co.uk/news/articles/c4g54g6vgpdo>

² McKeon, C. (2025, October 28). *Labour must ‘shut down legacy state’ in drive for digital ID, says minister*. Yahoo News UK. <https://uk.news.yahoo.com/labour-must-shut-down-legacy-185822555.html>

"we're not saying we're going to boil the ocean in one go because the public would be really sceptical."³

The government's own guidance on the scheme states that the digital ID will "in time" be used across government and private sector services, from right to rent checks to accessing welfare and other benefits, childcare, education, banking, and voting.⁴

This confused and arguably misleading messaging has severely damaged trust in digital IDs –with polling showing that public support for digital ID has collapsed since Starmer's announcement.⁵ As a result, millions of members of the public do not want to and are unlikely to use a digital ID, making any mandatory application of it exclusionary rather than inclusive.

Because legislation in the UK can be changed or removed by a simple Act of Parliament, there is no durable safeguard against mission creep once the infrastructure for a digital ID has been built. A future government could, at any time, require digital ID to access essential services – including healthcare, education, childcare, tax payments, and accessing age-restricted services. A digital ID system will last far beyond this government, meaning that we risk building a mass surveillance infrastructure for a less rights-respecting future administration.

Privacy: It is unclear what information the government intends to require for inclusion on the digital ID. The government has stated that the digital ID will include, name, date of birth, nationality, and a photo as well as technology used for biometric authentication.⁶ Put simply, the proposed digital ID scheme would provide the infrastructure for a mass mandatory biometric system for tens of millions of people. But the digital ID could include much more, with the government stating in its digital ID explainer that the upcoming consultation will consider whether the digital ID should include other details such as addresses.⁷

In other jurisdictions, national ID systems mandate expansive categories of personal information to be included on ID cards, ranging from age, gender, marital status, health records, education records, and photographs to biometric data. As the mandatory ID would be digital, it is a living identity document that could be updated and changed in real-time. Each time an individual uses their digital ID – whether in the public or private sector – that use may be recorded in government database, allowing vast amounts of information to be amassed, searched, and sorted to offer insights through data analysis and profiling. The public should not be forced to bare their lives to the state in order to access basic services.

The digital ID would also allow an individual's data across government departments to be linked up using a single unique identifier meaning that data shared for one purpose could be repurposed for use in a different context. For instance, personal health data shared with one's GP could potentially be linked up with an individual's welfare applications, criminal record, education history, giving the state a comprehensive view of an individual's life.

³GB News interview with Josh MacAlister <https://x.com/silkiecarlo/status/1972624076771582133>

⁴Department for Science, Innovation & Technology. (2025, September 26). Digital ID scheme: Explainer. GOV.UK. <https://www.gov.uk/government/publications/digital-id-scheme-explainer/digital-id-scheme-explainer>

⁵Courea, E. (2025, Oct 1). 'Reverse Midas touch': Starmer plan prompts collapse in support for digital IDs. The Guardian. <https://www.theguardian.com/politics/2025/oct/01/keir-starmer-labour-collapse-public-support-digital-id-cards>

⁶Department for Science, Innovation & Technology. (2025, September 26). Digital ID scheme: Explainer. GOV.UK. <https://www.gov.uk/government/publications/digital-id-scheme-explainer/digital-id-scheme-explainer>

⁷Ibid.

The mass surveillance and profiling that digital ID systems facilitate mean that certain individuals and communities are likely to be subjected to excessive monitoring and targeted interventions. There is a significant disproportionality in the use of stop and search powers on Black and other racialised people, and digital IDs, given their likely mission creep, could facilitate extensive data sharing with the police and other authorities and be treated like internal passports for people of colour.⁸

Security Risks: Mandatory digital ID would put the population's personal data at unprecedented risk of data breaches by creating a honey pot for criminal hackers, and target for foreign adversaries. It is also less resilient than non-digital forms of ID to certain risks on the National Risk Register of Civil Emergencies such as those that impact the electricity or communications network.

In the past year alone, breaches of the legal aid database and Afghans relocating to the UK have resulted in the addresses, financial data, legal records, criminal histories, and political allegiances of hundreds of thousands of people, including members of the special forces and MI6, being leaked. The government's OneLogin system, which the proposed digital ID will be built on, is also reported to be suffering from "serious vulnerabilities" according to security experts.⁹

Unlike a password, it is impossible to change your biometric data, which uniquely identifies you. A breach of a biometrically-linked digital ID system could therefore leave an individual permanently susceptible to identity theft and privacy intrusions without recourse to protect themselves.

Security breaches are common in digital ID systems around the world. In Estonia – which is often held up as the poster child for digital ID, a hacker was able to obtain over 280,000 personal identity photos in 2021, following an attack on the state information system. The culprit had already obtained personal names and ID codes and was able to obtain a third component, the photos, by making individual requests from thousands of IP addresses.¹⁰ Similarly, in 2017, a flaw was identified in over 760,000 national identity cards which could have let attackers decrypt private data or impersonate citizens. The citizens at risk were banned from accessing online government services whilst the threat was remedied.¹¹ In India, which is home to the world's largest biometrically linked digital ID scheme, citizens' personal data was reportedly being sold for less than £6 online after the database was breached.¹²

Accuracy: The eVisa scheme for migrants has already caused a raft of failures, leaving people stranded at airports, missing job opportunities and excluded from health services.¹³

⁸ Kundnani, A. (2005, May 26). *ID cards: Implications for Black, Minority Ethnic, migrant and refugee communities*. Institute of Race Relations. <https://irr.org.uk/article/id-cards-implications-for-black-minority-ethnic-migrant-and-refugee-communities/>

⁹ Computer Weekly, (2025) Security tests reveal serious vulnerability in government's One Login digital ID system, <https://www.computerweekly.com/news/366623991/Security-tests-reveal-serious-vulnerability-in-governments-One-Login-digital-ID-system>

¹⁰ ERR (2021) 'Hacker downloads close to 300,000 personal ID photos,' *ERR* <<https://news.err.ee/1608291072/hacker-downloads-close-to-300-000-personal-id-photos>>

¹¹ BBC News (2017) *Security flaw forces Estonia ID 'lockdown.'*

<<https://www.bbc.co.uk/news/technology-41858583>>

¹² BBC News (2018) Aadhaar: 'Leak' in world's biggest database worries Indians, <https://www.bbc.co.uk/news/world-asia-india-42575443>

¹³ See ORG evidence submission to Home Affairs Committee -

<https://www.openrightsgroup.org/publications/harnessing-digital-id-evidence-on-evisas-share-codes-and-digital-immigration-status/> and the Digital Status Crisis Report by the3Million - <https://the3million.org.uk/sites/default/files/documents/t3m-report-DigitalStatusCrisis-28Oct2025.pdf>

These failures can stem from the digital records of someone's status being incorrect or entirely inaccessible. The government has failed at providing an accurate and reliable digital ID scheme for the 10 million eVisa holding migrants in the UK. Many of the problems digital ID schemes face will scale with population size. In March 2024, The Guardian reported that 76,000 records in the Home Office were corrupted, resulting in eVisas displaying incorrect photos, passport numbers and nationalities.¹⁴

Discrimination and exclusion: Many people risk being excluded by mandatory ID systems, including elderly people, the unemployed, disabled people, and those living in digital poverty or without digital skills.¹⁵ Young people are also a particularly affected group, being the second most digitally excluded group after the elderly.¹⁶

There should always be the right of people to use acceptable "functional" IDs such as passports and driving licenses rather than enrol in a mandatory foundational identity system; and there must also be the right to use non-digital methods for those who cannot or do not want to use digital means to identify themselves.

Changes relationship between population and the state: Our identity practices are built on a *multi-path, trust-based approach*. Because verification happens through different providers, documents, and social contexts, the system is more robust against failures and supports personal autonomy. Mandatory digital ID would essentially turn that dynamic on its head by creating a society on licence, where we could be required to seek permission every time we interact with the state.

¹⁴Dyer, H., Taylor, D., & Syal, R. (2024, March 14). *Home Office immigration database errors hit more than 76,000 people*. The Guardian. <https://www.theguardian.com/uk-news/2024/mar/14/home-office-immigration-database-errors-hit-more-than-76000-people>

¹⁵Deloitte LLP. (2023). *Digital poverty in the UK: Executive summary — A socio-economic assessment of the implications of digital poverty in the UK*. <https://digitalpovertyalliance.org/wp-content/uploads/2023/09/Deloitte-Digital-Poverty-ExecutiveSummary-29092023.pdf>

¹⁶Ibid.