Big Brother Watch's response to the Cabinet Office consultation on digital ID

Key recommendations summary:

- Users must retain full control over what data is shared, when and with whom.
- A national digital ID must not have phone home functionality, nor keep a digital audit trail recording uses of the digital ID
- A national digital ID must not have a single unique identifier
- There must be a legal right for people to use non-digital means of identification

Questions on Part 1: Our ambition

The implementation of a national digital ID system threatens to bring in a mandatory scheme by stealth.

Despite the assurances that digital ID will be a voluntary scheme, absent an enshrined legal right to non-digital methods of proving one's identity, there is nothing to prevent it from becoming mandatory in future. Given the initial introduction of the scheme as a requirement to enforce penalties, it is understandable that the public will be sceptical about the inevitability of this outcome.

The UK government frequently refers to India's digital ID scheme to highlight the purported benefits of national IDs. However, in India, an ostensibly voluntary digital ID scheme has become "an infrastructural prerequisite for participation in everyday civic and economic life."[1] The system has become so embedded that Indians cannot even buy a train ticket, get a SIM card or admit their children to school without showing their digital ID.[2] The consultation envisions a similarly ubiquitous take up of digital ID in the UK, explaining "the range of ways people can choose to use their digital ID will grow over time."

Where digital ID systems become the single point of entry for accessing basic state services, failures have been catastrophic. People can be excluded and locked out of benefits. System failures are most likely to impact the most marginalised in society, including those living on low incomes, older people, people with disabilities and ethnic minorities. For example, in India, the Aadhar ID card system has led to deaths in cases where grain subsides were denied due to the lack of an Aadhaar number, failure to link biometrics to ration cards, or an inability to authenticate fingerprints.[3] Similarly, eVisa users in the UK have reported GPs wrongly rejecting their credentials, and recognised refugees being unable to connect their passports to their eVisas, making it impossible to set up a bank account or rent housing.[4] These problems would undoubtedly replicate in a population-wide digital ID system.

[1] The Aadhaar Paradox – Domestic Failures and Global Success, 17 February 2026, https://www.techpolicy.press/the-aadhaar-paradox-domestic-failures-and-global-success/.

[2] The Guardian, 'Your basis to live is checked at each and every step': India's ID system divides opinion, 14 October 2025, https://www.theguardian.com/world/2025/oct/14/india-id-system-divide-opinion.

[3] Human Rights Watch, 'India: Identification Project threatens rights,' 13 January 2018, https://www.hrw.org/news/2018/01/13/india-identification-project-threatens-rights.

[4] The Independent, 'UK rollout of eVisas hit by problems facing foreign nationals and refugees just two weeks in,' 14 January 2025, https://www.independent.co.uk/news/uk/home-news/evisa-uk-immigration-status-help-b2678643.html.

The consultation provides an assurance that access to public services will not be made dependent on having the digital ID. The government must also consider how it will ensure that digital ID will not become a prerequisite for accessing services in the private sector. It is also imperative that the public do not suffer any detriment from relying on paper-based forms of ID. Without an enshrined right to use physical forms of ID, the government's reassurances will not be watertight.

Recommendation: the Government should introduce a legal right to use non-digital verification services.

Questions on Part 2: Our approach

The potential revocation of digital IDs is a significant concern, particularly if such IDs become a prerequisite for accessing essential public services. Where a national digital ID functions as the primary means of proving entitlement, there is a risk of creating a system in which individuals' access to rights can be withdrawn with relative ease. For example, in February 2026, a law passed in Kansas immediately invalidated state-issued driver's licenses, identification cards and birth certificates for holders whose gender marker does not match their sex assigned at birth.[5] In 2022, the Canadian government froze the bank accounts of truckers suspected of taking part in COVID-19 restriction protests without a court order.[6] A national digital ID would be susceptible to similar instances of revocation in politically sensitive circumstances. Although the consultation states that revocation would occur only in strictly controlled circumstances, any such powers should be clearly defined in law and subject to robust parliamentary scrutiny.

Recommendation: any enacted policy must contain safeguards to prevent the scheme being used as a tool of coercive control by a future government. In particular, revocation of the ID itself must not be a grounds on which to deprive citizens of services to which they are entitled.

[5] What can Canadian truckers teach us about CBDCs?, Jason Deane, 17 February 2022, https://medium.com/original-crypto-guy/what-can-canadian-truckers-teach-us-about-cbdcs-11e968a0d8cf.

[6] The Conversation, Kansas revoked transgender people's IDs overnight – researchers anticipate cascading health and social consequences, 1 March 2026, https://theconversation.com/kansas-revoked-transgender-peoples-ids-overnight-researchers-anticipate-cascading-health-and-social-consequences-277052?ref=404media.co.

Questions on Part 3: Useful

The proposed national digital ID would require individuals to submit a current, high-resolution biometric facial image as part of their core information. This turns an intensely personal and immutable aspect of identity into the key for accessing official records. Without an alternative option for accessing those records, this would amount to a requirement to share biometric data just as unique as fingerprints or DNA.

The risks inherent to this type of system have been borne out elsewhere. In India, there have been reports of Aadhaar records, including photographs, being sold online for as little as £6.[7] The proposals also suggest that, in addition to the core identity information, the digital ID may also need to store and share additional information or metadata, which has the potential to be highly revealing.

The consultation presents the digital ID, underpinned by the single unique identifier, as the foundation for joined up public services. The government argues that this system would ensure consistency of personal data across government and enable to the delivery of 'proactive personalised services.' Whilst government data profiling and analytics may enable more tailored public services, it would also have wider consequences on both the societal and individual level in terms of resource allocation and targeted interventions. Data processing and insights derived from the digital ID data could be used to determine where public funding goes, which communities and individuals are targeted for state intervention, and which neighbourhoods are observed, surveilled and investigated.

More data does not automatically lead to better decisions, particularly where data is used decontextualised and operated under “black box” systems. Individuals may be flagged simply for matching the characteristics of known offenders, even where they have done nothing to arouse suspicion. In practice, this can subject entire groups to heightened scrutiny based on generalised risk profiles. It marks a shift away from monitoring individuals based on specific behaviour to placing large segments of the population under surveillance in an effort to anticipate and manage potential threats.

The profiling and data mining associated with a national digital ID also threatens to affect those who do not elect to have one. Even if an individual does not consent to their data being used, they may be subject to decisions made on the basis of other people’s data. For example, if your child goes to a school where many children are found to be underperforming on the basis of data from other parents’ unique identification numbers, your child may also be subject to intervention measures despite not consenting to data sharing themself.

The consultation envisages a wide range of everyday uses for a national digital ID from joining a gym and collecting parcels to purchasing alcohol, accessing age-restricted products or websites, gambling, and verifying eligibility for discounts. Depending on how the system is designed, this could enable the state to collect detailed data on individuals’ private-sector transactions. If the ID includes “phone home” functionality, where each use triggers a check with the issuer or an intermediary, it could create a record of every instance in which a person verifies their identity, even outside government services. Without protection against such capabilities, a central record could expand far

[7] The Guardian, ‘Personal data of a billion Indians sold online for £6, report claims,’ 4 Jan 2018, https://www.theguardian.com/world/2018/jan/04/india-national-id-database-data-leak-bought-online-aadhaar.

beyond public-sector interactions to include credit histories, transaction data, and even browsing activity, raising serious concerns about the scope of state visibility into everyday life.

The government should reject proposals to impose a legal duty on individuals to report errors or updates to the personal information held in their digital ID. While applicants for entitlement-based public services may reasonably be required to demonstrate their eligibility, it is neither proportionate nor appropriate to compel people to continuously account for themselves to the state.

The government will require businesses to conduct digitised right-to-work checks. The consultation suggests that the move to digital only checks will remove unreliable manual checks of varied paper documents making it harder for criminals to use forged documents. However, digital ID documents are not immune to falsification. A cybersecurity engineer demonstrated that Gov.uk One Login itself is susceptible to impersonation[8] and in September 2023, the National Cyber Security Centre warned that the design of One Login left it vulnerable to identity theft.[9] Additionally, the digital only checks will also create a audit trail of where checks have been carried out to support enforcement. This underlines how digital ID systems can also be used in a punitive way, supporting the imposition of sanctions as well as compliance.

Recommendations: ensure that the collection of biometric data is optional, with no de facto requirement to provide it in order to access services.

Require transparency as to the use of any data deriving from the scheme in relation to public policy, especially spending, decisions.

Remove from the design of any ID the capacity for the ID to be used to track transactions with third parties i.e. remove any phone home functionality, audit trail, and single unique identifier.

Reject proposals to impose a legal duty on individuals to report errors and updates to their personal information. Ensure an offline option for right-to-work checks remains.

[8] OneLogin, 'Many Issues: How I Pivoted from a Trial Tenant to Compromising Customer Signing Keys,' 10 June 2025, https://specterops.io/blog/2025/06/10/onelogin-many-issues-how-i-pivotedfrom-a-trial-tenant-to-compromising-customer-signing-keys/.

[9] ID Tech, 'Critical Security Flaw found in UK's Gov.uk One Login Identity System,' 16 May 2025, https://idtechwire.com/critical-security-flaw-found-in-uks-gov-uk-one-login-identity-system/.

Questions on Part 4: Inclusive

The suggestion that digital IDs could be issued from birth is deeply troubling. This would enable the state to accumulate and link data about individuals from infancy, creating a lifelong record of their lives, long before they are capable of consenting to such data collection.

The consultation suggests that children as young as 13 could be issued a national digital ID, noting that the primary use case at this age would be to verify access to age-restricted social media platforms. Big Brother Watch has consistently opposed the introduction of ID requirements for accessing online services. In positioning digital ID as the solution, the government risks addressing a problem created by its own policy approach.

Any rollout of digital ID should be accompanied by a legal right to use non-digital forms of identification, so that participation is not coercive, and to uphold equal access to opportunities. This is particularly important for those who cannot share their information digitally, whether for reasons of digital poverty, disability, age, or financial circumstances. Age UK has warned that "it will never be possible to get everyone online and trying to force the issue poses a real risk to older people's health, finances and ability to participate in society."[10] Those fleeing domestic abuse, whose records may be compromised, may depend on offline options to maintain their safety. Proposed alternatives, such as digitally signed QR codes, may also introduce practical challenges, as evidenced by issues encountered with the UK's e-visa scheme.

The government proposes providing dedicated, accessible support for those who are digitally excluded, delivered locally, in person, and through trusted organisations. However, this support will need to be sustained beyond initial onboarding and should be fully accounted for in the system's long-term costs. Ongoing assistance is also likely to be required whenever technical updates are introduced.

Recommendations: no digital ID should be issued without explicit consent from the individual or their parent/guardian.

Any rollout of digital ID should be accompanied by a legal right to use non-digital forms of identification.

Any support plan for a transition to digital ID must include planning, and cost analysis, for ongoing assistance following technical updates.

[10] Age UK, 'Offline and Overlooked: Digital Exclusion and Its Impact on Older People,' https://www.ageuk.org.uk/siteassets/documents/reports-and-publications/reports-and-briefings/offline-andoverlooked-report.pdf, p2.

Questions on Part 5: Trust

Data protection and privacy
5.1

The consultation makes some important gestures towards data protection principles, such as data minimisation, decentralisation and transparency. However, other aspects of the proposal undermine our confidence that these gestures are meaningful.

The government has repeatedly emphasised that the digital ID will be decentralised by design. However, it is still possible to collect vast amounts of data, monitor and profile citizens without building one centralised database. Provided the digital ID is built around a single, unique identifier – which is the government's proposal – it will not make a difference whether there is a centralised or decentralised database as the data will be linked in practice.

The government tout selective disclosure as a key benefit of a digital ID and use it to claim its proposals are privacy-preserving. Whilst selective disclosure is important, it is not the only aspect of privacy and control. True consent and control over data would mean that individuals are able to choose when and with whom their data is shared. A single unique identifier would make that control impossible, by linking our government records on the back-end of these systems. This also fundamentally undermines the notion of data minimisation as vast quantities of personal information will be collated as a result of the single unique identifier.

The government maintains that a digital ID would improve privacy by allowing users to see who their data is shared with and how it is processed. Whilst it is laudable to attempt to improve transparency over government-held data, it is not necessary to build a national digital ID to achieve this aim. It would be far more proportionate to improve existing transparency functions and ensure that government departments comply with extant requirements to a high level, for example by making privacy notices easy to understand and helping people to exercise their data rights.

National security, lawful access and police powers
5.2
The consultation acknowledges that the police will have a legal basis to access digital ID photos for the purpose of facial recognition searches. If adoption of a digital ID is expansive (as, indeed, the government hopes that it will be) this would result in an almost population-wide facial recognition database. Given the government's emphasis on building trust in a national digital ID system, the explicit possibility that the public's digital ID photos could become mugshots seriously, and perhaps fatally, undermines this objective. The government should expressly exclude digital ID photos from being repurposed for facial recognition in its new legal framework on facial recognition technologies.

Under the government's proposals, the personal data processed and retained by the digital ID could also be lawfully accessed in line with existing legislation. This means that law enforcement and intelligence agencies will have access to vast amounts of personal and uniquely identifying data, potentially without requiring warrants or having to make individual requests for information from governmental bodies. Building infrastructure capable of monitoring and analysing the data of millions in real time would hand the state powerful tools that could be used to suppress or censor

political dissent. While many in the UK may view such risks as remote, recent history shows how quickly human rights and democratic norms can erode once such capabilities are in place.

Routes of redress

5.4

The consultation acknowledges that there must be measures put in place to make sure people can resolve issues with their national digital ID. However, the experience of e-visa users indicates that the government's existing track record on providing routes to redress with digital systems is poor. In evidence given to the Home Affairs Select Committee, Monique Hawkins, Head of Policy and Advocacy at the 3million explained that since late 2023, individuals using the Home Office's reporting tool to raise problems with their e-Visa received an auto-reply with the message, "Due to the volume of reports we are getting, we are unable to reply within the normal two weeks."[11] The 3million also revealed, through a Freedom of Information request, that 483,000 calls were made to the e-Visa resolution call centre over a 12-month period. However, many of these calls went unanswered or involved such long waiting times that callers were unable to get through. A national digital ID system with similar issues would make it even more difficult for individuals to access public services, contrary to the stated aim of the scheme. The government should not push forward with the national digital ID, having been unable to demonstrate capacity for rectifying errors in the existing e-visa system.

Recommendations: do not create a single, unique identifier as this entails centralisation in practice.

Do not launch any scheme unless / until the government is confident that its ability to provide ongoing technical support, critically the rectification of errors, is assured.

The government should expressly exclude digital ID photos from being repurposed for facial recognition in its new legal framework on facial recognition technologies.

[11] Home Affairs Committee, Oral evidence: Harnessing the potential of new digital forms of identification, HC 986, 28 January 2026, https://committees.parliament.uk/oralevidence/17082/pdf/.

Questions on Part 6: Wider summary of impacts

6.1

The consultation cites several figures which explain the costs associated with societal problems, without establishing how a digital ID would solve it. For example, the government states that identity fraud costed individuals £1.8 billion in 2020 and suggests that "a small reduction in the amount of fraud would save households millions." However, it neglects to set out how a digital ID will contribute to this cost saving. The onus will be on the government to determine the cost benefit analysis, particularly when the scheme is voluntary, and uptake is unknown. It is insufficient to suggest "a good digital ID solution…may be able to make a significant dent in that problem."

Recommendation: do not launch any scheme until a return on investment assessment which recommends digital ID has been conducted, published for Parliamentary scrutiny, and accepted.