LIBERTY

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

May 2026

About Liberty

Liberty is an independent membership organisation, founded in 1934. We challenge injustice, defend freedom and campaign to make sure everyone in the UK is treated fairly. We are campaigners, lawyers and policy experts who work together to protect rights and hold the powerful to account.

Contents page

Introduction

Liberty welcomes the opportunity to respond to this consultation on the Government's proposal to establish a digital ID system. The organisation has a long history of campaigning on questions of identification, state data collection, and civil liberties, most notably through its participation in the No2ID campaign during the 2000s.

The context for this debate has shifted considerably since the last time a Labour government proposed a national identity scheme. The volume of personal data collected and retained by both state and commercial actors has expanded dramatically. Yet, the fundamental principle remains unchanged: in a democratic society, the Government's power over citizens demands counterbalances of consent, transparency, and accountability. The aggregation and analysis of personal data by government creates a significant power asymmetry between citizen and state that makes strong, enforceable safeguards essential.

Liberty's digital ID principles

For a digital ID system to be rights-respecting and safe, it must include the following features:

- **Voluntary, always** – The law must prevent mission creep. Digital ID must never quietly become compulsory.
- **Privacy is not a feature, it's the foundation** – The whole system is built around protecting your data from day one, which means no database linking and no tracking where and when we use digital ID.
- **Clear purpose, hard limits** – Digital ID must be for proving who you are securely – not as an enforcement mechanism for immigration, not for policing, and not for surveillance. There must be limits on when you can be asked for digital ID.
- **No digital ID? No problem** – You must always have the right to choose a non-government provider or show a physical document instead.
- **State-of-the-art security** – It must be protected with the strongest cryptography and a decentralised design so there's no honeypot for hackers.
- **Open to scrutiny, accountable to you** – It must be built with an open-source code which can be audited, overseen by a regulator with real teeth and independence, and with a complaint mechanism we can all use easily.

These principles are the minimum conditions for a system that is lawful, trustworthy, and worthy of public confidence. A digital ID system that does not meet these requirements must not be built.

The consultation outlines three interconnected digital public infrastructure projects. The first is the digital ID itself, a digital credential, stored locally, that will include personal information including name, age, nationality, right-to-work, and a biometric photo. The second is a new right-to-work digital checking system that will record where those checks have been completed which can be audited by border enforcement. The third is a digital transformation project to connect different government data systems and give everyone a unique ID to be used across these systems.

The first proposition could be done well, in a privacy-protective way that allows users to gain more control over how their data is stored and shared. This goal is undermined when connected to the second project, where the ID becomes a mechanism for border enforcement. It is further undermined by the third project – a 'radical rewiring of the state' –

and the introduction of a unique, persistent identifier that would follow us around our use of public services.

It is important that this proposal is understood not as an incremental administrative reform, but as a substantive reconfiguration of how the Government collects, stores, and shares our sensitive personal information. These proposed changes would have major implications for our privacy and data protection rights in an arena where they are crucial: public services.

Our consultation response focuses on highlighting the human rights risks raised by the proposed system, with particular concern regarding the foundational government IT systems on which it will be built, the universal identifier, the inclusion of biometric data, the insufficient data protection regime, and specific risks that could arise in the technical build. We also suggest safeguards to foster trust and inclusion in any future system and mitigate harm.

Twenty years on from the No2ID campaign, the human rights risks of a national identity system are greater than ever. A digital ID system could be useful and privacy-protective, or it could become part of a powerful surveillance infrastructure. This consultation response sets out Liberty's assessment of where this proposal falls short, and what a rights-respecting alternative would require.

Liberty's recommendations

Voluntary participation and accessibility

- Digital ID must be voluntary and free of charge.
- The primary legislation should limit all ID demands outside of specified circumstances, for example, no conditioning access to a good or service on presentation of a digital or government ID, except where required by law (e.g. buying alcohol). It must be unlawful to refuse, penalise, or charge more for a good or service on the basis that a person has not used a digital ID.
- The right to not use digital ID must be protected in primary legislation, and alternative, non-digital methods of proving identity must be accessible and affordable.

Privacy and surveillance prevention

- The ID must not include a phone home functionality and must operate offline only to ensure authorities cannot track where, when, and how a digital ID is used.
- The system must not contain unique persistent identifiers and credentials should be unlinkable across different uses and databases.
- Users must have the right to pseudonymity and selective disclosure – with the ability to share only strictly necessary information.
- There must be no remote revocation capability, and instead digital IDs should be updated or renewed via a remote "appointment" system at the user's prompting.
- Police must be banned from requesting any ID, including a digital one, and this must on the face of the bill.

Data protection

- Biometric information should not be included in a digital ID, and police must not have access to any biometric database connected to a digital ID system.
- No special category data as defined by UK GDPR, nor protected characteristics as defined by the Equality Act 2010 should be included on a digital ID, except for date of birth. There must be an explicit prohibition of including this data in primary legislation.
- A robust privacy and data protection regulatory regime must be established via the primary legislation and not be left to existing data protection frameworks alone.

Oversight and accountability

- The digital ID system must be built on free and open-source software, so the code can be independently audited by regulators, civil society, and technologists.
- The digital ID must include a privacy dashboard showing a full transaction history of all data requests and disclosures, with the ability to request data deletion.
- A robust, properly resourced independent regulator must oversee the scheme with real enforcement powers to ensure adherence to data protection requirements.
- The Government must learn from eVisa failures and ensure redress mechanisms are swift, effective, and include access to a human helpline.

Digital ID scheme aims

Q1. What do you think the main benefits will be, if any, for the Government's new national digital ID system?

Q2. What do you think the main drawbacks will be, if any, for the government's new national digital ID system?

Q3. One of the government's aims for the new national digital ID system is to make it easier for people to prove who they are. To what extent do you agree or disagree that the proposed system could help achieve this aim, and why?

A well-designed digital ID system could deliver genuine benefits for UK residents. Liberty sets out below both the potential advantages of such a system and the significant risks that the current proposals, if adopted without amendment, would create.

Benefits

If truly designed with the privacy and data protection of the user in mind, a digital ID could provide a more privacy-protective option for identity verification than currently exists. Through selective disclosure, we might be able to verify certain attributes about ourselves like the fact we are over-18. It might also give us greater control over who we share our data with and how much we share, if the system includes a functionality like the EU wallet's "privacy dashboard".

This all depends on the Government designing the ID with the user's privacy and human rights in mind. The proposal put forward in this consultation does not do this.

Impact on privacy

The right to privacy is fundamental and is protected by Article 8 of the European Convention on Human Rights, enshrined in British domestic law by the Human Rights Act 1998. Our data protection rights are guaranteed by UK GDPR and the Data Protection Act 2018.

The proposed digital ID system poses a major risk to privacy in a variety of ways. Some of them are related to the digital ID itself and could be mitigated with a privacy-by-design approach to the technical build. Some of the risks are associated with the wider project to join up state databases via a single unique identifier.

Observability: The key difference between a digital ID and a physical ID is the ability to track where, when, and how a digital ID has been used. This tracking can reveal the most sensitive information about a person, depending on how the system is designed, including how much alcohol they consume, which websites they visit, and whether they watch pornography. It is therefore essential that the digital ID is not designed to "phone home" (outlined further below) and no entity can track where the ID is used.

Aggregation: This information becomes even more sensitive when correlated with other data points about a person. Indeed, consider the impact of the NHS, DWP, or a private insurer being able to access information about what we buy, what we eat, or where we go. There are serious rights risks to companies collecting data about the most private aspects of our lives. This can include discrimination through opaque profiling, such as feeding our data into dynamic pricing (e.g. using tax information to charge someone more for a product if they make more money). There are also risks to the Government having an unfettered ability to connect these data points about us, particularly as various departments increase their use of AI and automated decision making in government systems.

Purpose creep: In countries that have already introduced digital IDs, what began as relatively limited systems have gradually become effectively mandatory for everyday life. We have seen this in India, where Aadhaar is necessary to buy a house, get a job, open a bank account, pay tax, receive benefits, buy train tickets, and sign their children up for school. Indian people cannot function without a digital ID, even though it is "voluntary". This becomes even riskier if the Government uses digital ID to achieve age verification gating, where the scope for digital ID could expand to tracking who we are and what we do across the internet. Particularly online, there is a serious risk of government-certified identity checks proliferating in areas of life where anonymity was previously accepted, which would be a serious threat to freedom of speech and association.

Biometrics: Biometric data carries unique sensitivities that would significantly amplify the dangers of a digital identity scheme because, unlike other personal information, it cannot be reissued or changed if compromised. People can change a password or get a new email

address if their information is breached and used by hackers, but they cannot get new eyes, fingerprints, or a new face. We are also deeply concerned about the section about police access to digital ID's biometric data for facial recognition searches. Once this capability exists, the scheme ceases to be a tool to make UK residents' lives easier or give us more privacy protective identification options and becomes a tool that can be used against us.

Impact on cyber security

In a digital world, strong cybersecurity protects the right to privacy. It is therefore highly concerning that the Government intends to build a digital ID system on the shaky foundations of pre-existing digital projects that have been marred by technical failures and cyber security risks.

Successive governments have a bad track record of keeping our data safe and secure, and cyber incidents are increasingly common and damaging. Significant cyber incidents have increased by 50% from 2024 to 2025 according to the National Cyber Security Centre (NCSC).[1] A 2025 DSIT survey found 283,000 British businesses have been the victim of a cybercrime in the past 12 months.[2] Key British institutions including the Legal Aid Agency and the British Library have been crippled by severe cyber-attacks in the past few years. In 2017, the WannaCry cyber-attack on the NHS led to disruption in 34% of trusts in England and an estimated 19,000 appointments being cancelled.[3]

The NCSC warned in September 2023 that the One Login system – one of the systems that will underpin digital ID – had 'serious data protection failings' and 'significant shortcomings' in information security that could increase the risks of data breaches and identity theft. In December last year, whistleblowers in the One Login team warned of significant cybersecurity issues in the system. They told *ITV* that One Login failed to meet the mandatory minimum government cybersecurity standards, 'Secure by Design' and the 'Cyber Assessment Framework'.[4] In a red-team exercise, a remote attacker was able to introduce malware and gain access to sensitive parts of the system without triggering an alert in the security monitoring. The whistleblower noted it was theoretically possible that a hostile state actor had already gained access to the system without the Government knowing. The NCSC found One Login carried the risk of bulk theft of personal data, identity theft, the Government being defrauded, economic damage, and people in witness protection, intelligence agents, and dissidents being identified.

This is particularly concerning in this geopolitical environment. The 2024 MI5 threat lecture noted that hostile state actors have been investing heavily in cyber operations and 'their targets include sensitive government information, our technology, our democracy, journalists

[1] National Cyber Security Centre, 'NCSC Annal Review 2025', 14 October 2025.
[2] Department for Science, Innovation & Technology and Home Office, 'Cyber security breaches survey 2025', 19 June 2025.
[3] National Audit Office, 'Investigation: WannaCry cyber attack and the NHS', 27 October 2017.
[4] Sam Holder, 'Whistleblowers raise "extreme" concern about security of government's Digital ID', ITV, 18 December 2025.

and defenders of human rights."[5] The Government must improve its cybersecurity and data integrity practices if it is going to build high risk digital systems and connect public service access to them. It is deeply concerning that a highly sensitive system such as digital ID is being built upon existing digital infrastructure that, according to whistleblowing civil servants, suffers from extensive cybersecurity weaknesses. In this environment, maintaining offline access capabilities is also more important than ever to safeguard essential state functions.

Risk to freedom of expression and association

Digitalising ID could trigger an avalanche of identity verification demands, both online and offline. This could have a major impact on freedom of expression and association.

The rights to freedom of expression and assembly are important not only in themselves, but also as enabling rights that allow societies to ensure the peaceful enjoyment of other rights. As the UN Human Rights Committee put it, freedom of assembly 'constitutes the very foundation of a system of participatory governance based on democracy, human rights, the rule of law and pluralism."[6] Freedom of assembly is a positive right, requiring authorities to actively facilitate its exercise.

The key threat to freedom of expression and association posed by digital ID is the erosion of anonymity in public spaces, on and offline. Anonymity is not a shield for wrongdoing; it is a structural condition that makes participation in democratic society possible for many marginalised people. There are important reasons that a person might choose to be anonymous in an interaction.

- LGBTQ+ people, particularly those in unsupportive families or communities, or hostile workplaces, depend on anonymity to explore their identities, access supportive community, and organise politically.
- Political dissidents rely on anonymity to organise, communicate, and express opposition to foreign governments that may seek to target them on British soil. Anonymity is also important to allow UK political activists to organise freely.
- Disabled people and people living with mental illness frequently depend on anonymity to seek information, access peer support, and engage in public conversations without the stigma that disclosing their conditions could attract.
- Survivors of domestic abuse and violence rely on anonymity to access support, legal information, and community without detection by their abusers.
- Whistleblowers and journalists rely on anonymity to expose wrongdoing by powerful people and organisations.

[5] Ken McCallum, 'Director General Ken McCallum gives latest threat update', Security Service MI5, 8 October 2024.
[6] United Nations Human Rights Committee, 'General comment No.37 (2020) on the right of peaceful assembly (article 21)', 17 September 2020.

- Religious and ethnic minorities might require anonymity to organise collectively without becoming targets – particularly in this moment of increasing intolerance to some religions and communities in Britain.

Indeed, any one of us who do not belong to the above communities and groups has the right to exercise our anonymity simply because it is our preference. Article 8 of the European Convention protects this choice.

The erosion of anonymity on and offline would pose a risk to the freedom of expression and association of all the above groups, and to us all. If the Government requires increasing identification online, we could all lose resources and access to community.

Our democracy has unusually limited checks and balances on parliamentary sovereignty. It is therefore particularly important that governments design digital systems with regard to how they could develop in the future and build them with technical and legislative rights safeguards baked in from the beginning.

Risk of discrimination

Digital ID could lead to discrimination by disadvantaging people who are digitally excluded, removing access to public services from vulnerable people, and expanding the hostile environment.

Risk of digital exclusion

The Government's research ahead of bringing in voter ID requirements found more than 2 million UK voters lacked appropriate photo identification.[7] This would be compounded by digital exclusion in the case of digital ID. 4% of Britons, 2.1 million people, are offline according to a report by the House of Lords Communications and Digital Committee.[8] Their report cited lack of affordable internet access, lack of connectivity and coverage, and lack of skills and motivation as barriers to digital participation.

Liberty welcomes the commitment for digital ID to be voluntary. International precedent nonetheless demonstrates that without explicit legislative restrictions on expanding use cases, a nominally voluntary scheme risks becoming effectively compulsory over time. As digital ID becomes the default way to access essential public services, or to prove the right to work or rent, those unable to participate in digital life risk being excluded by the back door.

This risk falls hardest on those who are already the most marginalised. Poverty and older age are among the strongest predictors of digital exclusion. A report on digital ID systems by the Centre for Human Rights and Global Justice at NYU notes, these exclusionary 'impacts are not necessarily linked to the digital aspects of such systems, but instead are manifestations

[7] Cabinet Office, 'Photographic ID Research – Headline Findings', IFF Research, 31 March 2021.
[8] Sarah Tudor, 'Digital exclusion in the UK: Communications and Digital Committee report', House of Lords Library, 30 January 2024.

of underlying dynamics of social exclusion, economic inequality, and marginalisation.'[9] It is therefore essential that digital ID does not become mandatory by default and there are explicit limitations on when a person can be asked to show a digital ID; that there is explicit protection for using physical documentation to access public services and the workplace; and that additional barriers to accessing essential services are not erected.

Risk of exclusion from public services and the workplace

There is a high risk of discrimination if the Government chooses to use digital ID to regulate access to public services. We have seen how this can go disastrously wrong in India's Aadhaar system. One of the key use cases of Aadhaar was establishing Indian people's identity for the purpose of distributing welfare benefits. The Indian Government has used digital ID to revoke access to subsidised food, pensions, and wages for public projects, sometimes for months or years at a time.[10]

This was not because they were ineligible for these benefits, but because they failed to satisfy Aadhaar's rigid digital conditions. Whilst the Indian government has claimed that the Aadhaar system has saved billions in welfare system, research by economist Reetika Khera suggests that much of the reduction in beneficiary numbers came from the removal of people who were eligible for benefits, but whose records could not be verified.[11] In Jharkhand, an 11-year-old girl reportedly died from starvation after her family's access to food rations were cancelled for not being linked to Aadhaar.[12] Again, digital ID can compound exclusion; if you do not have the paperwork to prove you have access to a service, digital ID can quickly remotely revoke it and leave people cut off from healthcare, money, or food that they need. Digital ID enables instant, remote, and potentially automated revocation. A flag in a database could lock someone out of public service access across the state in a frictionless way.

Hostile environment

In 2016, David Bolt, Independent Chief Inspector of Borders and Immigration, noted that there was 'insufficient hard evidence to say whether [the hostile environment surveillance regime was] achieving what the government intended.'[13] He added the justification for extending data sharing and search and seizure powers in 2016 was 'based on a conviction that they are "right" in principle, and enjoy broad public support, rather than on any evidence that the measures already introduced are working or needed to be strengthened'.[14]

---

[9] Center for Human Rights and Global Justice, 'Paving a Digital Road to Hell? A Primer on the Role of the World Bank and Global Networks in Promoting Digital ID', NYU School of Law, June 2022.
[10] Rebecca Ratcliffe, 'How a glitch in India's biometric welfare system can be lethal', The Guardian, 16 October 2019.
[11] Reetika Khera, 'Aadhaar and the creation of barriers to welfare', ACM Digital Library, 2 November 2020.
[12] Soutik Biswas, 'Aadhaar: Is India's biometric ID scheme hurting the poor?', BBC News, 27 March 2018.
[13] David Bolt, 'An inspection of the hostile environment measures relating to driving licenses and bank accounts', Independent Chief Inspector of Borders and Immigration, 2016.
[14] Ibid.

Indeed, research from the Migration Observatory at Oxford University found migrants who stay in the UK despite hostile environment restrictions are often able to adapt their strategies and lifestyle to avoid detection.[15] Migrants would adapt to the more expansive data-sharing environment that a single unique identifier would create, but it would push them into more precarious and dangerous situations to do so – avoiding reporting crimes, accessing life-saving healthcare, and removing their children from schools.

Cost

Liberty questions the Government's cost-benefit analysis of the proposed scheme. The history of such schemes offers a sobering precedent. In the 2000s, the cost of the ID scheme soared to £5.75 billion before it was scrapped.[16] This figure kept rising throughout the scheme's development. That scheme was abandoned precisely because the Government could not account for runaway implementation costs, and there is no reason to assume that the structural challenges which drove that cost explosion – complex cross-departmental IT integration, data security infrastructure, legal compliance, and public administration – have become simpler.

These factors have arguably become more complex as the public sector has accelerated digitalisation in the intervening years. The ambition of the consulted proposal arguably exceeds that of its predecessor scheme in that as well as being an ID system, it is a substantial reimagining of the data sharing processes of the state and an overhaul of legacy IT systems. Additionally, any credible cost-benefit framework must account for the substantial litigation risk outlined in this response from human rights and discrimination claims.

Revocation

Are there any ethical factors government should consider that relate to an individual deleting their digital ID?

Are there any ethical factors government should consider that relate to revoking (i.e. cancelling) an individual's digital ID?

Yes, Liberty is deeply concerned about the human rights risks of revocation, or "kill switches".

One of the key differences between a physical ID and a digital ID is the power it places in the issuer's hands to revoke it at any time. This is especially acute when the scope of the digital ID scheme creeps and it becomes necessary to access public services, to verify your identity to access websites or apps, and to prove who you are to get a job. This situation would give the Government enormous power to paralyse a person's ability to engage in society and move about the world freely.

[15] Mihnea Cuibus and Peter William Walsh, 'Briefing: Unauthorised migration in the UK', Centre on Migration Policy & Society, 2025.
[16] Alan Travis, 'Cost of national ID card scheme soars by £840m in six months', *The Guardian*, 11 May 2007.

We have seen examples of identity and service revocations, and the huge harms they have caused. In South Africa, the High Court ruled the practice of 'ID blocking' was unconstitutional. The Government had blocked around 1.8 million people it deemed 'suspicious' in an effort to curb irregular migration and identity theft.[17] Being blocked left people unable to access healthcare, education, and travel. As outlined above, excessive use of revocation has had a deleterious effect on Indian people using Aadhaar. Overuse of a revocation functionality has plunged millions of people in India into poverty and destitution and has even killed people.[18]

Liberty urges the Government to consider how this power could be used by a future government. If, as we have seen in other countries with digital ID systems, identity checks proliferate and become ubiquitous, it would be incredibly dangerous for the Government to have a "kill switch" over someone's identity and ability to access public services, the workplace, and the internet. The high risk of building such a system is why Liberty urges the Government to put strong guardrails around expanding digital ID use cases to avoid scope creep and to not build the ability to remotely revoke a digital ID into the system.

Revocation also creates technical risks within an ID system. The common approach for revoking a digital ID requires the holder or verifier to contact the issuer during the presentation of the ID to do a live check of the revocation status of the credential. This is a form of "phoning home", outlined further below, that creates dangerous risks for data collection and tracking.

It would also expose the Government to significant legal liability. Where access is wrongly revoked, whether to employment, welfare, or another essential service, those affected would have strong grounds for a legal challenge. The Government could face substantial litigation arising from errors that, in a federated system, have the potential to cause serious and cascading harm to individuals. We have seen such harms arise in other digital ID systems that facilitate public service access, such as Indian Aadhaar.

Revocation is not necessary for a digital ID system to work. The Government does not need the ability to run a live check on someone's information. Information contained within a digital ID could be updated or renewed via a remote "appointment" system at the user's prompting. A privacy-protective digital ID system must not have remote revocation capabilities and should be designed to operate offline only.

Private sector uses

Do you think people should be able to choose to store their national digital ID directly in holder services (sometimes known as 'digital wallets') other than the GOV.UK Wallet, that are certified to meet government standards?

[17] Institute on Statelessness and Inclusion, 'South Africa's High Court declares ID blocking unjust and unconstitutional', 2024.
[18] Rebecca Ratcliffe, 'How a glitch in India's biometric welfare system can be lethal', The Guardian, 16 October 2019.

To what extent do you agree or disagree with the proposed government checker service being made available for use in the private and third sectors, at low or no cost?

We are considering several limitations to the government checker service, by design. Are there any specific limitations you think we should set for the government checker?

The national digital ID would be useable across the private and public sectors, alongside other options like physical documents and other appropriate digital identities from third parties. To what extent do you agree or disagree that the private sector and third parties should be able to use the digital ID alongside other options?

Any digital public infrastructure that facilitates private sector access to personal data must be underpinned by robust and enforceable safeguards. It is essential that sensitive information about our health, welfare, and wider public service use is not made available to the private sector via the digital ID scheme's government data system overhaul.

This risk is especially acute where digital public infrastructure is made accessible to data-intensive industries (for example, social media, e-commerce, healthcare, and financial services) whose commercial interests are not aligned with the privacy rights of citizens. The scheme's legislative and technical framework must therefore explicitly prohibit data aggregation across relying parties and prevent private companies from data mining using the ID system.

A digital ID system should be regarded as digital public infrastructure; it is therefore essential that the build is not outsourced to a private company who can exercise proprietary control over any aspect of the system and whose commercial interests may not align with the long-term public interest in an open, accessible, and rights-respecting system.

However, the existence of a private sector digital identity ecosystem also provides UK residents with a choice about how they verify their identity and prove attributes. It is important that people have the option to select an alternative identity provider to the Government that meets their privacy requirements. This pluralistic approach is a welcome aspect of the consultation, as long as our public sector data is properly safeguarded in both the legislative framework and the technical build.

<u>Open wallet ecosystem</u>

Liberty recommends the Government adopt open and private wallets, transparent code, and regulates the market with a robust trust framework, as is proposed here.

People should have a choice about whether to download and run government software on their phone, or choose to use a verified business, or choose not to use digital ID at all. People need to have a meaningful choice about engaging with digital ID, and an open and regulated marketplace would help facilitate this.

The Government must provide the regulatory conditions for an open wallet marketplace that allows open-source providers focused on offering the maximum security and privacy to offer

alternatives to the Government system. The Government's trust framework, which sets standards for privacy, cybersecurity and inclusivity which a company must meet to gain access to government-held data for identity verification, provides a good basis for this. The list of trusted services and the UK CertifID trust mark are good ways to help people identify safe identity services. Liberty suggests educating the public about the trust mark and widely disseminating the list of trusted providers will be an important part of the digital ID rollout.

Users should always know who is asking for our data, how much data they are asking for, and whether they have the right to do so. Therefore, there must be technical mechanisms for people to authenticate and record where our data is being accessed and used, including full visibility over what data fields are requested, what is actually sent, and what verifiers have shared – as is proposed by the EU's privacy dashboard. Verifiers must provide people with as much assurance and information as users provide them in the verification process.

There should also be a functionality for users to report suspicion of unlawful behaviour to the Government, which could lead to the company's trust certification being revoked.

Information included in the digital ID

The national digital ID will include a person's full name, date of birth, nationality, and a biometric facial image (photo). What further information, if any, should the digital ID also include?

Businesses and organisations accepting the national digital ID need to trust that the information on it is up to date and accurate. We are exploring whether people with a digital ID should be legally required to inform the government within an appropriate timeframe of certain changes (such as a name change) or errors to their personal information, so that their digital ID can be updated. To what extent do you agree or disagree with a legal requirement to inform the government of changes or errors within an appropriate timeframe?

Protected characteristics

No data about protected characteristics, nor special category data should be included on the digital ID, apart from age. It is essential that the digital ID does not include information about sex, gender, sexual orientation, gender reassignment, race, disability, religion or belief, marriage, and pregnancy. Liberty strongly recommends that this stipulation be put on the face of the bill as a safeguard against such information being added in the future without parliamentary consent. If such information were included, Liberty would outright oppose that digital ID because that system would make it easier for future governments to target minority and marginalised communities in the UK. Digital ID would risk becoming a social register.

Biometric information

Additionally, Liberty strongly discourages the Government from including any biometric information in the digital ID system. Biometric authentication must not be a precondition of

using digital ID. Biometric systems create serious human rights risks that cannot be mitigated, as outlined above.

In this context, Liberty is deeply concerned about the point the consultation covers in 5.2: 'there is a legal basis for police use of facial recognition, which may include access to biometric data held by government.' Firstly, there is no dedicated legal basis for police use of facial recognition, as confirmed by the Bridges case in 2020. Liberty welcomes the Government's acknowledgement that the current legal situation for the use of facial recognition is confused and inadequate and has engaged with the consultation into a new legal framework. At time of writing, proposals have not been published, and it is concerning to see this consultation make reference to a 'legal basis' that is discredited and in the process of being replaced.

Secondly, this line suggests that there may be a biometric photo database as part of the digital ID system architecture which is extremely concerning. Most people interact with biometric verification via their smartphones, but these systems store biometric information for authentication only in the secure enclave of the device and never upload it onto the cloud or into a database. If the digital ID system includes this kind of database, it will never be privacy protective or data minimised.

Additionally, any digital ID system will rely on public trust to be a success. If police are allowed to access the biometric information in the digital ID system, people will rightly cease to trust the ID. Such a functionality would launder a surveillance capability through the legitimate aims of improving public service access.

Legal requirement to keep information up to date

Liberty strongly recommends that the Government does not introduce a legal requirement to keep your information up to date on a digital ID. Such a measure would place an excessive burden on the user. Indeed, it is unclear what the sanction for not meeting this requirement would be and the consultation provides no further detail on this front.

This proposal is especially risky when considering the data entanglement issues that eVisa users faced, and the difficulty in accessing pathways to fix these issues. Research by the 3million found eVisa users reported incidents of entangled status, where the incorrect name, photographs, visa type, nationality, and visa expiry date was displayed on accounts.[19] There was inadequate support for people seeking to fix these errors when they occurred. People were referred to automated webchats that rarely connected them to human operators; the 24/7 helpline was shut down a few months after the launch even though issues persisted; and automated responses cited significant delays in assistance due to 'high enquiry volumes.' This is one of the systems that will underpin digital ID.

The risks of data entanglement, through no fault of the user, and a legal duty that makes the user liable for such mistakes, will make for a dangerous system. Creating a legal duty to keep

[19] The 3 Million, 'The Digital Status Crisis', 28 October 2025.

one's information up to date in this context is irresponsible. It risks trapping individuals in a Kafkaesque bureaucratic loop, chasing accuracy in a system over which they have no meaningful control. Such a measure will likely have a disproportionate impact on users without digital literacy skills or who have other access needs. Liberty would encourage the Government to have due regard for the Public Sector Equality Duty and consider the potential impact on people with digital access needs.

Whilst we do not support a legal duty to keep one's information accurate, Liberty strongly encourages the Government to consider building a functionality that would allow people to update their information easily, without needing to go through webchats or helplines to correct mistakes on their ID. We have seen substantial issues with previous access and helpline programs (e.g. eVisa), so this is essential.

Public sector transformation

We know that people can struggle to access or claim the public services to which they are entitled. We want to identify key issues in these interactions, so that we can explore how the digital ID system could help address these, making people's lives easier. Are there examples of any barriers or inefficiencies that prevent you (or people you support) from interacting with public services, that you think the digital ID system could help with?

For those who opt for a digital ID, government would develop a method to securely identify and match people across different public services to simplify everyday interactions between individuals and the state. For instance, such an approach could help ensure changes in an individual's information are easily and quickly reflected across services, like a name change. This would reduce the need for people to update their information separately for each service. It could also let government move away from old-fashioned and bureaucratic processes, towards proactive, hassle-free services that are available at the point of need. To what extent do you agree or disagree with the adoption of such an approach to public sector transformation?

Liberty has profound concerns about the public service data sharing transformation proposed as part of the digital ID system.

Concentration of risk: A digital ID system which is built with public service access in mind would concentrate risk of system failure. A technical failure, outage, or a cyberattack from non-state hackers or a foreign adversary could result in a catastrophic service breakdown or stoppage. We already have examples of this dynamic in the impact of the WannaCry attack on the NHS in 2017 or the Jaguar Land Rover attack in 2025. In a world of geopolitical fracturing and rapidly improving AI capabilities which could facilitate more complex cyberattacks, these risks look set to only increase. If public service access is mediated by a government digital service, a cyberattack could have a huge impact on people's health, housing, and welfare. The Government must protect offline access to public services on the face of any digital ID bill to mitigate this risk.

Scope creep: In countries that have already introduced digital IDs, what began as relatively limited systems have gradually become effectively mandatory for everyday life. Again, we have seen this in India, where Indian people cannot function without a digital ID – even though it is "voluntary". The potential for this kind of scope creep poses a particular risk for digitally excluded people and their access to public services and the workplace.

Privacy concerns: A digital ID system would not necessarily address privacy concerns in public service data sharing. A system truly built with privacy-by-design principles, which allows us to share minimised data in a cryptographically protected way, could addressed existing privacy concerns arising from data storage and sharing in various public service and identity checking contexts. However, this is not the system which this consultation outlines. A system that is designed to connect all of our government data using a single unique identifier will create huge privacy and surveillance concerns.

Single unique identifier

What ethical issues, if any, can you think of when designing a way to identify and match people across services?

What technical issues do we need to think about when designing a way to correctly identify and match people across public services?

Liberty strongly disagrees with the introduction of a unique persistent identifier. Such a proposal would undermine every commitment to privacy-by-design and hand the Government unprecedented surveillance power. A unique identifier would act as a "super cookie" which would allow the Government to track users across all areas of life and daily interactions and connect otherwise siloed sets of data. This proposal could give rise to legal challenges, and it will reduce trust and uptake of the scheme.

The key problem of a unique identifier is architectural; it transforms many separate, siloed datasets into connected information sets about every UK resident. Indeed, a persistent number would not just link our record: it would change what those records mean. HMRC knows our income; the NHS knows our health history; DWP knows what benefits we have access to; the Home Office knows our immigration status. Each of these data points is collected for a proportionate reason and subject to UK GDPR restrictions about storage and use. However, a unique identifier would allow government to join all this information up into a single profile that would reveal a huge information about us via the mosaic effect. Each piece of information is a tile that when put together reveals who we are.

Human rights risks

Liberty is highly concerned about the human rights risks associated with establishing a unique persistent identifier; we believe that this proposal could create major legal risk for the Government. The human rights risks of a universal persistent identifier are systemic rather than incidental: the architecture itself, not merely its potential misuse, threatens the right to private life, freedom of expression, and the equal protection of the law.

UK GDPR's purpose limitation principle constrains how data collected for one function can be used for another, and Article 8 of the ECHR protects the right to a private life. But these protections operate at the level of specific uses and specific decisions. They do not address, and were not designed to address, the structural privacy harm created by the existence of a linkable identifier: the modification of behaviour that occurs simply because people know, or suspect, that their interactions with the state are being assembled into a single picture. This chilling effect on help-seeking, rights assertion, and free expression is a privacy harm in itself, and one that no regulatory framework has yet proved adequate to prevent.

The human rights risk of a unique persistent identifier is particularly acute considering the increased prevalence of AI across public services. Once the Government can build a detailed profile on every UK resident, the risk of this data being fed into predictive technology to try and predict our behaviour is acute. The recent Policing White Paper promised to massively scale predictive policing technology and DWP is using automated decision making to profile Universal Credit claimants. A unique persistent identifier could give the state access to every interaction we have to feed into predictive systems. We have seen scandals across the world where this has gone wrong, including the Dutch childcare benefits scandal where a risk scoring algorithm flagged dual-nationality families, a discriminatory proxy. 26,000 families were wrongly accused of fraud and driven to financial hardship by the demands to repay their rightful benefits.

A unique identifier raises the risk of discrimination by proxy in the UK. Collection and analysis of special category data is strictly protected under UK GDPR. However, a unique identifier would allow for those characteristics to be inferred from linked administrative data. For example, GP practice location + children's school choice + last name = reasonable proxy for religion or ethnicity. This harm materialises when our profiles are used to make key decisions about our lives which are based on neutral criteria on paper, but in practice are shaped by discriminatory inferences.

Such a proposal undermines the Government's promise to deliver greater user control over data and improved privacy via a digital ID scheme.

Legal and trust risks

The introduction of a unique persistent identifier would expose the Government to substantial legal liability on several fronts. The architecture of a linkable identifier risks systemic breach of Articles 8 and 10 of the European Convention on human rights, opening the door to human rights claims where individuals can demonstrate that comprehensive government profiling has chilled their speech or movement, suppressed rights-assertion, or led to the wrongful withdrawal of their access to a public service. UK GDPR's purpose limitation principle (Article 5(1)(b)) would be structurally undermined by a system designed to aggregate data collected under distinct lawful bases. The integration of linked profiles into automated decision-making and predictive systems used across the state would be particularly risky here. This could

also trigger challenges under the Equality Act 2010 where discriminatory proxies (as in the Dutch child benefit scandal) lead to loss of access to public services.

Additionally, given the above risks of racial profiling and discriminatory loss of public services via the digital ID scheme's database connections, such a proposal is likely to undermine trust in the scheme itself and depress uptake of any ID, especially among marginalised communities.

Right-to-work checks

Are there any additional challenges not captured in the consultation that businesses would face in carrying out fully digital right to work checks for all new workers?

Would any additional support not captured in the consultation be required for business to comply with fully digital right to work checks?

What information would your organisation require to have confidence that a digital right to work check has been completed?

It is particularly concerning that the only digital ID use case the Government has committed to deliver this Parliament is a right-to-work digital checking system. Liberty strongly discourages the Government from building a digital ID system with immigration enforcement in mind. The Government should be clear about a digital ID system's purpose and ensure it is designed to improve people's interactions with public services or as a trusted form of identity verification, not to extend the hostile environment.

Successive governments' commitment to the hostile environment means that there is already expansive data-sharing occurring between the Home Office and frontline services. Liberty would urge the Government to reduce data sharing between the Home Office and essential services, rather than allowing the Home Office access to disparate government databases via a digital ID system.

Innovations in data processing are ostensibly deployed to support legitimate and important policy objectives such as keeping the public safe from serious violence and the prevention or detection of crime. The Government frequently makes reference to 'safeguarding' in its rationale for sharing data from essential public services with immigration enforcement.[20] However, when immigration enforcement is integrated into goals such as the protection of public health, the prevention of trafficking and domestic violence, and promoting children's education, the former risks undermining the latter.

For example, a 2023 report from the Domestic Abuse Commissioner revealed that all police forces in England and Wales share migrant victims' data with Immigration Enforcement, a practice which the Commissioner concluded deters victims and witnesses of crime from

[20] 'Memorandum of Understanding Between Health and Social Care Information Centre and the Home Office and the Department of Health', Gov.uk, 2016.

coming forward.[21] Between 2020 and 2023, the Immigration Enforcement National Command and Control Unit made 537 immigration status enquiries to the police for victims of domestic abuse.[22] This pattern of data sharing poses a serious safeguarding risk to migrant women and children, and is a deterrent to reporting abuse, enabling perpetrators to use victims' immigration status as a tool of coercion and control.

Inclusivity

Which of the following ages do you think is most suitable to access the digital ID system from?

Some people may face barriers to creating or using the national digital ID. This may be due to difficulty accessing traditional proofs of identity (like passports) or due to a lack of digital access, skills or confidence. Are you aware of any other barriers not captured in the consultation?

Is there any particular support not captured in the consultation or the Digital Inclusion Action Plan that would help you or other people to use the national digital ID?

Are there any groups not included in the list that you believe could also be at risk of ID or digital exclusion?

What kind of support should be made available to people who do not have a digital device (like a smartphone or tablet) to enable them to create and access the digital ID?

We are considering dedicated accessible support for those who are digitally excluded, delivered locally, in-person and by trusted organisations. Are there any other ways you think the government should consider supporting those who are digitally excluded?

We are exploring alternative ways to access the national digital ID for those who cannot use a device. What do you think are the most important barriers for government to address when designing alternative access routes for the national digital ID?

Risk of digital exclusion

As outlined above, the risk of scope creep increases the risks of digital exclusion cascading into a wider exclusion from public services, which would have a major impact on the most marginalised people in society. It is therefore essential that our right to not use digital ID is explicitly protected in primary legislation, and that alternative, non-digital methods of proving identity are accessible and cost efficient.

The EU's digital ID legislation explicitly protects people who decide not to use the EUID Wallet, noting they must not suffer a negative consequence for opting out such as being refused a service or being asked to pay a higher price for it. These provisions ensure that the rights of

[21] Domestic Abuse Commissioner, 'Safety Before Status: How to ensure the Victims and Prisoners Bill meets the needs of all victims', Domestic Abuse Commissioner's website, 2023.
[22] Ibid.

all are protected, and not determined by their income, age, digital or legal literacy, legal residency or other status. We recommend a similar legislative provision is included on the face of the digital ID bill.

Digital ID access age

Digital ID poses a particular risk to the rights of children. Any future system must not be designed for children.

Recital 38 of UK GDPR recognises that children require specific protection in relation to their personal data, given their limited awareness of the risks of processing, and singles out profiling and data collection through services offered directly to children as areas of particular concern. A digital ID system that connects government data via a single unique identifier creates precisely the conditions Recital 38 warns against: the infrastructure for detailed, longitudinal profiling of children across public services. Where digital ID becomes the gateway to services children use directly, the heightened protections Recital 38 requires must be embedded in the system's architecture from the outset. The current consultation does not demonstrate that they would be.

The UN Convention on the Rights of the Child requires that all actions be guided by the best interests of the child, account for evolving capacities, avoid discrimination, and ensure children are heard on matters affecting them. A digital ID system that imposes adult-facing design on children, creates heightened data exposure risks for children, and is used to exclude children from essential services would fall short of each of these obligations, as would a system where children have had no meaningful input into its design.

Risk of record permanence: If digital ID becomes a vehicle to join up public service records, it will risk creating a permanent record that could follow children throughout their lives. This is particularly worrying for children who come into contact with safeguarding, mental health, or youth justice systems.

Safeguarding and risk of exposure: One of the greatest risks of including children in a digital ID system is the risk of children's personal information being exposed by a cyberattack. Data breaches, unauthorised access, or poorly secured systems can compromise children's sensitive information and create major safeguarding risks.

Exclusion: Like adults, children risk being excluded from essential public services because of authentication errors, or their parent or guardian does not enrol them in the system. These incidents would show up as technical errors or unmatched records, but they are rights violations and could manifest in significant disruptions to children's lives.

Trust and privacy

Are there any additional measures, beyond the principles and standards set out in the consultation, that we should consider to further protect user data?

Principles of data minimisation and empowering users to ensure they have greater control over how much data they share when using their national digital ID at point of use will be central to the design and implementation of the digital ID system. How should the government ensure transparency around how national digital ID data is used?

Are there any additional security safeguards to those named above that should be considered in relation to the national digital ID system?

We want to ensure these alternative access routes are secure. What do you think are the most important factors we need to consider in order to achieve this?

Below, Liberty sets out the minimum safeguards that must be incorporated into any digital ID system that is to be compatible with human rights law and data protection obligations.

Accessible and voluntary

Any digital ID system must be entirely voluntary and accessible. Every UK resident should have the right to access a digital ID, and it must be offered to people free of charge. We therefore welcome the Government's commitments to both. It must be unlawful to refuse, penalise, or charge more for a service on the basis that a person has not used a digital ID, and this protection must be on the face of the bill.

Unobservable

As noted above, the key difference between a digital ID and a physical ID is the ability to track where, when, and how a digital ID has been used. The digital ID system must be designed so that our use of a digital ID cannot be tracked – i.e. it is unobservable.

The digital ID system must therefore not include a "phone home" function. Phone home occurs when a digital credential is presented (in person or online) and the system sends a live check to the original issuer or a proxy to confirm validity. It allows the ID issuer to track every instance in which an identity is used: where, when, and for what purpose. A national identity system with this capability would give the Government an unprecedented surveillance tool. If, as the consultation proposes, digital ID is also used for age assurance online, this could extend to visibility of citizens' browsing activity.

Privacy protection must be built into the system's technical architecture. The system must be designed so that user interactions are unobservable by third parties, including the issuer. Modern cryptographic methods allow credentials to be verified and revoked without contacting a central server. However, protecting just the digital ID interactions is not enough – the whole data architecture must be designed with privacy and data minimisation in mind.

Unlinkable

To ensure a digital ID system is safe and privacy protective, it is essential that it is not built with unique and persistent identifiers. The digital ID, its technical architecture, and the

standards that govern the ecosystem should be designed to prevent the compilation of records of where people are presenting their digital ID on the verifier side.

Privacy-protective options here include single-use credentials, or cryptographic anonymous credentials which let the holder repeatedly prove they have an attribute (e.g. they are over 18) without having to share a unique, linkable identifier. The mandate for the ID to be unlinkable must be included in the primary legislation and must be unambiguous and unqualified from the outset. However, as noted above, this alone is not enough for a digital ID to be privacy protective.

Right to pseudonymity

To protect users from tracking, they should have a right to use freely chosen pseudonyms not linked to their real identity whenever there is no legal obligation that they have to identify themselves. This can be achieved with privacy-enhancing technologies, but only if the surrounding architecture does not collect and store data that undermines the privacy gains.

No requirement for biometrics and no police access

Liberty welcomes the Government's commitment to banning any police officer from asking for a digital ID. This commitment must be protected on the face of the bill.

Biometric authentication or identification should not be a precondition for using a digital ID and no biometric photograph should be included in the digital ID. As noted above, biometric systems carry unique risks that would make a digital ID system much more dangerous.

User control over data

As the consultation highlights, one of the key benefits of a digital ID system is that it gives users the ability to selectively disclose information about themselves. It is therefore essential that the digital ID system is built to facilitate attribute authentication.

However, Liberty also notes that "user consent" is impossible in many cases where a digital ID will be used. Acknowledging the power dynamics between a user that needs to access a service and the service asking for the user's permission to share a certain amount of data about themselves, how meaningful that choice actually is for the user is highly suspect. For example, would a person who needs a welfare payment really deny the DWP a data sharing request? It is therefore essential to build restrictions about when a digital ID can be asked for and what information can be handed over into the regulatory regime from the start.

Privacy dashboard

A digital ID system must include a full transaction history of every request for information the user has received, the identity of the party making the request, and the information the user shared with them. Moreover, the digital ID should offer the possibility to request the deletion of any personal data by the ID user to a verifying party.

This functionality is required in the EU digital ID regulation: the wallets must 'enable the user in a manner that is user-friendly, transparent, and traceable by the user, to: [...] (d) access a log of all transactions carried out through the European Digital Identity Wallet via a common dashboard enabling the user to: (I) view an up-to-date list of relying parties with which the user has established a connection and, where applicable, all data exchanged; (ii) easily request the erasure by a relying party of personal data pursuant to Article 17 of the Regulation (EU) 2016/679); (iii) easily report a relying party to the competent national data protection authority, where an allegedly unlawful or suspicious request for data is received.'

Use case regulation

One of Liberty's key concerns with the establishment of a digital ID system is the risk of over-identification and the loss of anonymity in public spaces. To avoid a large increase of identity demands, which would facilitate tracking and privacy invasions whilst intensifying equity implications for digitally excluded people, Liberty recommends that the primary legislation should limit digital ID demands outside of specified circumstances.

Legislative language that could achieve these protections would forbid conditioning access to a good or service on presentation of a digital or government ID, except where required by law (e.g. buying alcohol). We would also recommend restrictions on charging different prices for goods or services based on digital ID presentation. We would also suggest that there is an explicit legislative mandate to request the minimum data necessary to determine a transaction meets legal requirements.

Oversight and governance

What additional oversight mechanisms, if any, should be put in place for the national digital ID system?

What measures can you suggest, if any, that could be put in place to make sure people can resolve issues with their national digital ID?

What additional oversight mechanisms, if any, would help you to have trust in the national digital ID system?

What measures do you think should be in place to help you feel confident in resolving any issues with your national digital ID?

The consultation does not include nearly enough information about the system's potential oversight mechanisms. Existing oversight structures will provide no meaningful accountability or redress. Parliamentary oversight of a digital ID system alone will not be consistent nor efficient enough to be effective.

Strengthening the regulatory regime

During the passage of the EU's digital ID scheme, the EU legislator did not find that GDPR provided sufficient safeguards for their wallet scheme. A robust privacy and data protection

regulatory regime must therefore be passed as part of the primary legislation to establish any digital ID scheme.

The assurances regarding the robustness of UK data protection law within the consultation document are undermined by the Government's prior record. A 2020 ICO audit of the Department for Education found that the Department was not complying with the basic principles of GDPR, was over-relying on public task as a lawful basis for sharing, lacked formal information governance oversight, and was not providing data subjects with the privacy information the law requires.[23] Citing data protection law as a safeguard for a new and expansive identifier system, against this background, offers little reassurance.

If the ICO is required to regulate the digital ID scheme's data protection, it must be properly resourced and take a more proactive approach to protecting our rights. The ICO has a notably weak enforcement record compared to its international counterparts. In particular, its policy of not fining public bodies for significant data breaches risks making it an overly permissive regulator of digital ID. Taking a fundamental compliance incentive off the table hollows out its enforcement framework before digital ID has even been established. If the ICO will not fine public bodies, they need another strong enforcement option to provide a real check and balance to government and incentivise data protection compliance.

Free and open source

A free and open-source software license must underpin the digital ID system. This is be a fundamental governance requirement.

Without an open-source license, the software underlying a national identity system would be a black box; code that millions of UK residents are asked to download onto our phones with no meaningful ability to verify what it does, what data it collects, or whether its technical architecture reflects the Government's stated policy and human rights commitments. Scrutiny of the framework by Parliament, regulators, and civil society cannot substitute for scrutiny of the code itself. Policy commitments mean nothing if the technical build does not reflect them, and without access to the source code there is no way to know whether it does.

The EU provides a precedent here. Open-source licensing of the EU digital wallet has allowed independent technologists to audit the code, identify discrepancies between policy commitments and technical implementation, and hold governments publicly accountable.[24] This kind of independent technical scrutiny is an essential check on a system that would sit at the heart of how citizens interact with the state.

Open-source licensing also strengthens cybersecurity. Code that can be audited by independent researchers is code that can be tested for vulnerabilities before they are

[23] ICO, Letter regarding ICO Department for Education reprimand published on ICO website, 2 November 2022, https://ico.org.uk/media2/migrated/4022280/dfe-reprimand-20221102.pdf
[24] epicenter.works, 'Analysis of Privacy-by-Design EU Legislation on Digital Public Infrastructures', 29 February 2024.

exploited. Closed, proprietary systems concentrate both risk and knowledge, and security depends entirely on the integrity and competence of the vendor, with no external check.

Finally, a system built with public money should remain a public asset. Proprietary licensing of publicly funded code would allow private companies to exercise control over, and extract commercial value from, infrastructure that taxpayers have paid to build.

Additionally, Liberty is concerned about "open washing", which is the increasingly prevalent practice of presenting a system as open source while key components remain proprietary, or where commercial arrangements obscure who controls the infrastructure. A genuine open-source commitment requires that the entire system is licensed accordingly, and that a well-functioning open-source community is empowered to provide ongoing oversight of whether the Government's commitments to privacy-by-design and user empowerment are reflected in the technical build.

Learn from eVisa mistakes

Liberty encourages the Government to learn from the mistakes made in the eVisa system's implementation, outlined above. The Government's redress mechanisms, where users can get help when something goes wrong, must not be a chatbot or an error form. There must be a helpline that allows users to speak to a human person and get guidance. A digital ID error could lose someone a job, or leave them unable to prove their identity, so it is essential that recourse is quick and effective.

Summary of wider impacts

Do you think there are any other costs to businesses from introducing the national digital ID system that have not been considered?

Do you think there are any other benefits for households from introducing the national digital ID system that have not been considered?

Do you think there are any other costs to households from introducing the national digital ID system that have not been considered?

Do you believe there are any other wider impacts from introducing the national digital ID system that have not been considered in this consultation?

Digital ID is not inherently incompatible with a rights-respecting society. Designed well – with privacy-by-design principles, genuine user control, and robust technical and legislative safeguards – it could give people more control over how their identity and data are shared than the systems it replaces.

However, the proposal set out in this consultation is not that system. It bundles a potentially useful identity tool with a right-to-work enforcement mechanism and a sweeping public service data transformation via a unique persistent identifier that would hand the

Government an unprecedented capacity to profile every UK resident. These are foundational choices that will determine whether this system serves citizens or surveils them.

The human rights risks raised by this proposal are serious and compounding. A unique persistent identifier would allow centralisation of disparate government databases into a single profile of every person's interaction with the state, which represents a structural privacy harm that no regulatory framework has yet proved adequate to prevent. Phone-home architecture could give the Government visibility of where, when, and how an ID is used, extending, if the consultation's age assurance proposals are adopted, to citizens' browsing histories. Scope creep, as demonstrated in India, could render a nominally voluntary system de facto mandatory, with the heaviest consequences falling on those already most marginalised. Finally, the system would be built on digital foundations (One Login) that the NCSC has already identified as carrying serious cybersecurity risks.

Liberty's recommendations are the minimum conditions for a system that is lawful, trustworthy, and worthy of public confidence. The system must be voluntary in law and in practice, with the right to use physical documentation protected on the face of the bill; it must be unobservable and unlinkable by design, not by policy; it must not include biometric data or unique persistent identifiers; it must be underpinned by a free and open-source license and governed by a properly resourced, genuinely independent regulator with meaningful enforcement powers.

The Government has an opportunity to build something that demonstrably improves people's lives while respecting their rights. To do so, it must be willing to redesign what it is currently proposing.