CHECKPOINT BRITAIN

The dangers of digital ID and why privacy must be protected







BIG BROTHER WATCH

NAME	KEIR STARMER
AGE	63
IMMIGRATION STATUS	LEGAL
RIGHT TO WORK	CLEAR
RIGHT TO RENT	CLEAR
EXPIRY	08/2029

Checkpoint Britain: The dangers of digital ID and why privacy must be protected

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaigning organisation, fighting for a free future. We're determined to reclaim our privacy and defend freedoms at this time of enormous change.

We're a fiercely independent, non-partisan and non-profit group who work to roll back the surveillance state and protect rights in parliament, the media or the courts if we have to. We publish unique investigations and pursue powerful public campaigns. We work relentlessly to inform, amplify and empower the public voice so we can collectively reclaim our privacy, defend our civil liberties and protect freedoms for the future.

Contact

Rebecca Vincent
Interim Director, Big Brother Watch
Email: rebecca.vincent@bigbrotherwatch.org.uk

Matthew Feeney
Advocacy Manager, Big Brother Watch
Email: matthew.feeney@bigbrotherwatch.org.uk

Jasleen Chaggar
Legal and Policy Officer, Big Brother Watch
Email: jasleen.chaggar@bigbrotherwatch.org.uk

Published 11 September 2025

CONTENTS

Introduction....1

What is Digital ID?....5

- What are digital identity systems?....6
- History of ID cards in the UK....7
- Digital ID in other countries....8
- Calls for digital IDs....9

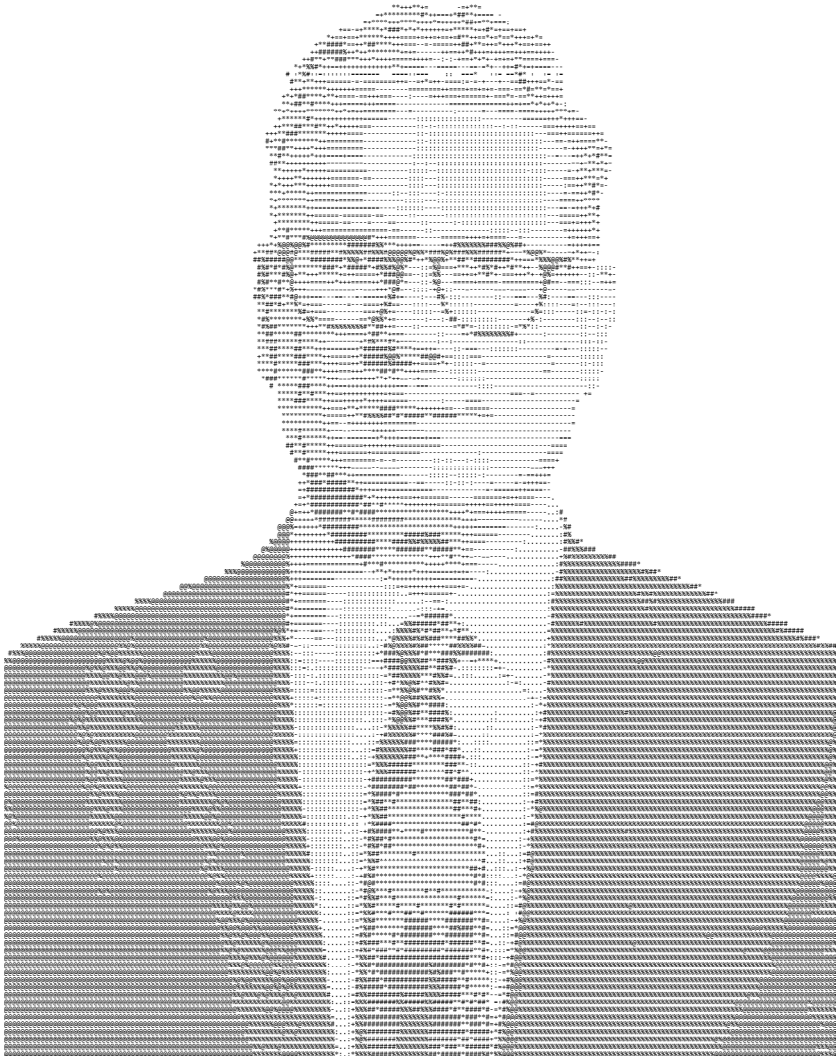
Will Digital ID work?....12

- Immigration....13
- *Commentary from Dr Shabna Begum, CEO of The Runnymede Trust*....21
- Education....23
- Welfare....26
- Healthcare....27
- National Data Library....29

What are the Risks of Digital ID?....32

- Privacy....33
- Surveillance, monitoring, and profiling....36
- Function creep....37
- Security....38
- Lack of choice in mandatory systems....40
- Inaccuracies and exclusion....40
- Abuses of power....41
- Changes the relationship between the population and the state....43

Conclusion....45



Checkpoint Britain:

The dangers of digital ID and why privacy must be protected

"I believe that the requirement of an internal passport is more objectionable than an external passport, and that citizens ought to be allowed to move about freely without running the risk of being accosted by a policeman or anyone else, and asked to produce proof of identity."

Aneurin Bevan MP, House of Commons, 1947

"Better a little evasion and inefficiency than too much petty bureaucratic interference with the individual. The Labour party ought to know this characteristic of its countrymen by now, sad as it is for zealous planners to bear with."

The Guardian, Editorial on the abolition of identity cards, 22 February 1952

"Those who support the introduction of such a card would reduce every man, woman and child in this country to a number to be programmed at will. The idea that every individual would have his or her life story on a little metal strip on a little plastic card is objectionable."

Alistair Darling MP, National Identity Cards Bill, 10 February 1989

"Instead of wasting hundreds of millions of pounds on compulsory ID cards, as the Tory Right demand, let that money provide thousands more police officers on the beat in our local communities."

Tony Blair, Labour Party Conference in Brighton, 1995

"If I am ever asked, on the streets of London, or in any other venue, public or private, to produce my ID card as evidence that I am who I say I am...then I will take that card out of my wallet and physically eat it in the presence of whatever emanation of the state has demanded that I produce it."

Boris Johnson, The Telegraph, 2004

"I felt listening to the Home Office ministers, and others proposing an ID card, that it has become part of the excuse culture. We've got a problem in terms of our asylum policy, we've got a problem in terms of violent crime, we've got a problem in terms of benefit fraud. Here's this one catch-all solution, which as I've said when you really look at it, it's really not a catch-all solution...and that only makes me more sceptical."

David Cameron, LSE event on Identity cards, 2004

"We have no hesitation in making the national identity card scheme an unfortunate footnote in history. There it should remain – a reminder of a less happy time when the government allowed hubris to trump civil liberties."

Theresa May, Identity Documents Bill, 9 June 2010

INTRODUCTION

INTRODUCTION

The question of mandatory ID has been a controversial topic throughout modern British history, ultimately being considered and rejected time and again in favour of preserving civil liberties. The modern-day version of this debate is now digital, and is no longer about physical ID cards but about a wide range of personal data being centrally held and accessible by the state and required for many aspects of modern life.

Just days after the new Labour government was elected in July 2024, ministers publicly claimed there were no plans to introduce digital ID cards.[1] However, in the face of pressure from a group of backbenchers and proposals from Labour Together and the Tony Blair Institute for Global Change (TBI), and a steady push from those quarters to reframe the narrative surrounding digital ID in the context of combatting unauthorised immigration, the tide is rapidly shifting.

In April 2025, a group of 40 Labour MPs signed a letter calling on ministers to introduce a digital ID programme, claiming it would "transform public services" and help the government "get a grip of illegal immigration."[2] In early June, the government was reported to be actively considering a proposal for the introduction of a digital ID card for every adult in Britain, framed as part of efforts to combat unauthorised immigration.[3] The proposal, drawn up by think tank Labour Together, advocates for a universal and mandatory digital ID scheme under the name 'BritCard.' In the same month, the House of Commons Home Affairs Committee launched an inquiry into the potential benefits and dangers of a government-issued digital ID.[4]

On 4 August, civil servants were reported to be secretly drawing up plans for a national ID scheme codenamed 'Operation Kelp.'[5] In early September, Prime Minister Kier Starmer confirmed in a Cabinet meeting and then to the BBC that he was indeed considering a digital ID scheme.[6] Just two days after being appointed

1 BBC, 'Labour rejects Tony Blair's call for ID cards,' 7 July 2024, https://www.bbc.co.uk/news/articles/c87rgj4e0rzo.
2 The Guardian, 'Labour MPs launch campaign for digital IDs to crack down on illegal migration,' 8 April 2025, https://www.theguardian.com/politics/2025/apr/08/labour-mps-launch-campaign-to-introduce-digital-ids.
3 The Times, 'No 10 examines plan for digital ID card to cut illegal migration,' 5 June 2025, https://www.thetimes.com/uk/politics/article/no-10-examines-plan-for-digital-id-cards-to-cut-illegal-migration-3fqst2dl5.
4 Home Affairs Committee, 'New Inquiry: Harnessing the potential of new forms of digital ID,' 12 June 2025, https://committees.parliament.uk/committee/83/home-affairs-committee/news/207446/new-inquiry-harnessing-the-potential-of-new-forms-of-digital-id/.
5 The Times, 'Secret Project examines nationwide digital ID scheme,' 4 August 2025, https://x.com/breeallegretti/status/1952336075902390727/photo/1.
6 BBC, 'Starmer considering digital ID scheme to tackle illegal migration,' 4 September 2025, https://www.bbc.co.uk/news/articles/c5y5379djl3o.

Home Secretary, on 8 September Shabana Mahmood also announced that she is personally in favour of digital ID and reiterated that her department was considering their introduction.[7] These developments mark the first time in over a decade that a government appears to be on the brink of introducing a mandatory national ID system.

The question of digital ID has now fully re-entered public discourse in the UK, and is predominantly being proposed as a means of tackling unauthorised immigration. Mandatory digital ID could be swiftly rolled out in the near future. But insufficient consideration has been given to the valid concerns over the privacy and civil liberties implications of a mandatory digital ID, nor the fundamental reversal such a scheme would pose to the very nature of the population's relationship with the state. This report scrutinises the rationale behind the digital ID proposals and sets out a critique from a privacy perspective.

Further, public opinion remains more nuanced than what proponents of digital ID would suggest. Independent polling commissioned by Big Brother Watch via YouGov shows that the British public has concerns about privacy and cyber security when it comes to digital ID, and a clear majority – 63 percent – do not trust the government to keep their digital ID data safe.[8] At the time of publication, more than 90,000 people had signed Big Brother Watch's petition urging Starmer to reject plans for a mandatory digital ID.[9] And while Starmer's government barrels ahead, Parliament's views have not yet been heard, with the Home Affairs Committee's inquiry into the matter still ongoing.

This report scrutinises the rationale behind the digital ID proposals and sets out a critique from a privacy perspective. Although digital IDs may bring some administrative benefits and could be helpful in providing different methods to verify identity when necessary, digital ID systems can be implemented by states and private companies in ways that are uniquely harmful to privacy, equality and civil liberties. At their worst, digital ID systems can enable population-wide surveillance; infringe on civil liberties; monitor, predict or influence individuals' decisions; identify individuals or groups for targeted interventions; and facilitate the tracking, persecution, or differential treatment of marginalised groups. Rather than achieving a utopia state of digital inclusion, as is sometimes claimed, a digital ID system could significantly further digital exclusion.

---

7 Sky News, 'UK could suspend visas from countries that do not agree migrant returns deals, says home secretary,' 8 September 2025, https://news.sky.com/story/uk-could-suspend-visas-from-countries-that-do-not-agree-migrant-returns-deals-says-home-secretary-13427109.

8 All figures, unless otherwise stated, are from YouGov Plc. The total sample size was 2,153 adults. Fieldwork was undertaken between 20-21 August 2025. The survey was carried out online. The figures have been weighted and are representative of all GB adults (aged 18+).

9 38Degrees, 'Reject plans for a mandatory BritCard (digital ID)', accessed 8 September 2025, https://you.38degrees.org.uk/petitions/reject-plans-for-a-mandatory-britcard-digital-id.

Digital ID systems facilitate the collection of vast quantities of personal information into population-wide databases which can be amalgamated, searched, and analysed to monitor, track and profile individuals. Although the promise of tailored governmental services is offered, the risks of nudging, predicting outcomes and shaping decisions in the public sector have been underreported.

At a fundamental level, the introduction of a mandatory, national digital identity system would change the nature of the relationship between the population and the state. Where we have previously existed as free individuals, a mandatory digital ID system would turn us into a 'Papers, please' society, operating on licence. We would increasingly be required to present ourselves for identity checks in order to go about our daily lives – like visiting the GP, opening a bank account, or sending our children to school. We risk having to share excessive amounts of information about ourselves as a prerequisite for accessing basic services.

A list of potential benefits often accompanies proposals for a universal, mandatory digital ID system. However, with little evidence that digital ID would achieve these wide-ranging stated aims, it is difficult to justify the human rights and civil liberties infringements that would ensue. Subjecting the entire population to constant identity checks is not a proportionate approach. Rather than providing a silver-bullet solution for unauthorised immigration or other societal issues, a mandatory digital ID system is far more likely to put an additional burden on already law-abiding people to adapt to an online system that may be prone to system failures and inaccuracies, as has been the case with the widely criticised eVisa system. It would also put the population's personal data at unprecedented risk of security breaches – the scale and consequences of which could be devastating at both the individual and societal level.

Each living former Home Secretary has become convinced of the need for a digital ID and yet on each occasion, the British public has reliably pushed back against this incursion on their civil liberties. It is Big Brother Watch's view that the latest digital ID proposals must be similarly rejected and that more rights-preserving methods of streamlining governmental services or tackling issues such as unauthorised immigration must be explored. Most importantly, any use of digital ID mechanisms must never be made mandatory, and a legal right to non-digital ID must be introduced.

WHAT IS DIGITAL ID?

WHAT IS DIGITAL ID?

Almost every feature of our modern lives involves verifying our identities or revealing identifying information, whether it is online banking, booking a train ticket, shopping on Amazon, or scheduling a GP appointment. Login screens and the seemingly constant prompts to enter our addresses and names are an ubiquitous part of the modern world.

But while digital identification is an ordinary part of everyday life, mandatory digital ID systems are not. An individual's digital identity is an online representation of personal information that is capable of identifying them, such as their name, usernames, passwords, age, address or even biometric information. Digital identity verification is the process by which an individual can remotely prove their identity or entitlement to a service by cross-referencing their personal data against an official dataset, such as government records. A range of institutions from private companies to governments can issue and manage digital IDs.

As more services are increasingly delivered online, having remote ways to prove we are who we say we are can be useful. However, when digital ID is required to access all public services, it becomes a mandatory digital identity system that, depending on its design, links individual user data to national databases.

What are digital identity systems?

Importantly, digital ID systems are linked to databases. They often operate by creating a unique, permanent identifier for each user. This identifier links personal information held on databases across government departments, as an individual can be identified through their unique number. Each time an individual uses their digital ID, that use is recorded in these databases, which are updated in real-time. These databases can hold huge amounts of information, which can be aggregated, searched and sorted to offer insights through data analysis and profiling.

The government is already developing various digital identity systems. Currently, individuals are able to access over 40 government services using the same email address and password through the Gov.uk One Login digital identity system. One Login is currently optional and is not operational across all government services.

Additionally, the government has announced the launch of a digital wallet which will allow users to store government-issued documents, such as passports and driving licences, on an app on their phones. Individuals can show documents to government agencies and private companies to prove certain attributes, such

as age identity or eligibility for certain services.[10] It is not yet widely available. It is unclear how the digital wallet will function and what data it will collect and store, however, the One Login system and digital wallet are being proposed as the infrastructure of a mandatory, multi-purpose digital ID system.

Under the Data (Use and Access) Act 2025, the government also introduced a digital verification services trust framework ('DVS framework'), which is a set of standards that digital identity service providers must meet in order to be certified.[11] The DVS framework has cultivated a new digital identity market in the private sector, which is likely to play a significant role in the government's potential roll-out of digital ID systems.[12] This rapid expansion of digital identification ecosystems and indications of public-private collaboration in national digital ID provisions underscores the urgent need for greater scrutiny.

History of ID card systems in the UK

Fortunately, the UK's history of national ID schemes is relatively short. Governments have often proposed universal registers as responses to moral panics or at times of war.[13] The UK only instituted mandatory ID cards during the two world wars. Britain introduced its first identity cards, accompanied by a National Register, during World War I to support conscription, but the scheme quickly became redundant once it enabled the War Cabinet to ascertain how many men were still available to serve in the army.[14] During World War II, the government instituted a second National Register linked to mandatory population-wide ID cards as an emergency measure. Despite the initially limited purpose of ID cards for administering rations, conscription and national security, they continued to be used in peacetime, particularly for policing purposes.

In 1950, Harry Willcock, a 54-year-old dry cleaner and former Liberal councillor, was stopped by the police who demanded to see his ID. He refused, explaining, "I am a liberal and I am against this sort of thing." His resistance sparked a movement; the British Housewives' League protested the scheme by setting fire to their ID cards outside Parliament and Willcock established the Freedom Defence Committee.[15]

10 Gov.uk, 'GOV.UK Wallet,' https://www.gov.uk/wallet

11 Gov.uk, 'Guidance: Enabling the use of digital identities in the UK,' 13 February 2023, https://www.gov.uk/guidance/digital-identity.

12 Computer Weekly, 'Government starts private sector engagement on digital ID and Gov.uk wallet,' 15 May 2025, https://www.computerweekly.com/news/366623927/Government-starts-private-sector-engagement-on-digital-ID-and-Govuk-Wallet.

13 Jon Agar, 'Identity cards in Britan: past experience and policy implications,' https://historyandpolicy.org/policy-papers/papers/identity-cards-in-britain-past-experience-and-policy-implications/

14 Ibid.

15 Mark Egan, 'Harry Willcock: The Forgotten Champion of Liberalism,' Journal of Liberal Democrat History, 17: Winter, 1997-1998, https://www.liberalhistory.org.uk/wp-content/uploads/2014/10/17_

On 21 February 1952, the government led by Winston Churchill scrapped ID cards.

From 1993, the Conservative government toyed with the idea of ID cards when they were proposed by Home Secretary Michael Howard. However, the proposals were obstructed by other ministers.[16] In 2004, the last Labour government proposed a national identity card scheme linked to a centralised database called the National Identity Register. The proposal was unlike any other government ID scheme in the world in that it relied heavily on biometric enrolment and verification, proposed the use of a single identification number, and recorded every use of the ID system in a centralised database.[17] The plans quickly became highly controversial. A coalition of civil rights groups formed the 'No2ID campaign' which fought the proposals on a broad range of concerns, including privacy, security, ineffectiveness, human rights and cost. The Conservative and Liberal Democrat coalition government scrapped identity cards when it came into power in 2010.

The current Labour government is reportedly considering a range of mandatory digital ID schemes amid pressure to crack down on unauthorised immigration, improve efficiency and restrict unauthorised access to public services.

Digital ID in other countries

Many supporters of mandatory digital ID schemes will cite European countries as examples of liberal democracies where digital ID works well. While countries such as Spain and Estonia have much better civil liberties track records than authoritarian countries with mandatory ID cards such as China, it is still the case that British policymakers should be wary of international digital ID comparisons.

The UK stands out as being one of the few European countries that does not provide some form of national ID card, whether optional or mandatory. But it is worth comparing the UK to countries with which it enjoys close shared history and cultural ties.

Many of the UK's closest allies such as the USA, Canada, Australia, and New Zealand do not have any form of national ID card. Canada, Australia, and New Zealand are Commonwealth countries whose legal systems were inherited from Britain, which has a common law legal system very different to the legal systems found

egan_harry_willcock.pdf.

16 Blue Sky, Jon Agar, Thread on recent (1980s-2010s) UK ID Card History, 30 July 2025, https://bsky.app/profile/jonagar.bsky.social/post/3lv6ir2csnc2l; The Telegraph, Howard fights to hear off Tory revolt over ID cards,' 20 December 2004, https://www.telegraph.co.uk/news/1479364/Howard-fights-to-head-off-Tory-revolt-over-ID-cards.html

17 Edgar A. Whitley, Aaron K. Martin and Gus Hosein, 'From surveillance-by-design to privacy-by-design: Evolving identity policy in the United Kingdom,' 27 February 2014, https://personal.lse.ac.uk/whitley/allpubs/hos2014.pdf, 207.

in continental Europe. The USA similarly shares much of Britain's civil liberties heritage.

Far from the UK establishing a mandatory digital ID system being a sign of the UK catching up with European trends, such a move would represent a huge departure from the UK's historic liberal principles that have influenced legal systems around the world.

Calls for digital ID

Labour Together proposes a digital identity system called 'BritCard' which would be "mandatory, universal and free of charge."[18] It would comprise of a set of digital credentials that could be downloaded onto a user's smartphone and instantly verified using a verifier app. The BritCard would be used in 'Right to Work' and 'Right to Rent' checks and later expanded to other public sector uses.

The system would function as a dual credential issuing and verifying process. A user would request their 'Right to Work' credential by inputting their One Login password, which would be shared with the 'Right to Work' credential service. The 'Right to Work' credential service would then verify the user's right to work by reference to authoritative sources (i.e., the passport or eVisa database) and issue the credential which is stored in the Gov.uk Digital Wallet.

The user could then present the credential stored in the Gov.uk Digital Wallet to the person verifying it (i.e., a landlord or employer) who would use a free to download 'verifier app' to check the credential. The verification service would confirm the validity of the credential and store the check in an event log. The app showing the individual's photo and eligibility status would then be presented to the person verifying it who would confirm likeness.

It is not only Labour Together which is promoting digital identity systems. In April this year, 40 Labour MPs wrote an open letter calling for the "development of an ambitious digital ID programme," listing a range of use cases, including making the NHS more efficient, tailoring education services, tackling benefit fraud and offering more targeted support.[19]

The Tony Blair Institute for Global Change (TBI) has also been a consistent proponent of digital ID systems. TBI sees a role for digital ID in almost every aspect of public

18 Labour Together, 'BritCard: A Progressive Digital Identity for Britain,' June 2025, https://www.labourtogether.uk/all-reports/britcard, p14.
19 Letter from 40 Labour MPs, Labour Growth Group, X, 3 April 2025, https://x.com/LabourGrowth/status/1909499797112844511/photo/1.

life: a NHS ID for every citizen; a unique pupil identifier in schools, widespread use of digital-ID in the public and private sectors to tackle illegal migration; and digital-ID enabled data-sharing across government departments for targeted welfare interventions.[20] The proposed scheme seeks to integrate data across departments using "harmonised personal identifiers," meaning that all of the information we share with government bodies will be logged in an interoperable database. TBI advocates using AI to analyse data collected by digital ID in order to identify patterns, assist decision-making and make targeted interventions.[21] It also suggests that data collected through digital IDs could all be fed into a 'National Data Library' – anonymously at first, of course, but eventually linked to digital ID – for researchers and private companies to use and for AI models to be trained on.[22] According to media reporting, the government is considering a digital ID plan proposed by the TBI.[23]

The Times Crime and Justice Commission, which was established to consider the future of policing and the criminal justice system, also advocates for a universal digital ID system administered through the provision of a unique code given at birth.[24] It argues that such a system would facilitate the prevention of welfare fraud, unauthorised immigration and identity theft and would enable stringent age verification both in-person and online.

Make no mistake: despite Labour Together's recommendation against a singular, centralised database,[25] the aforementioned proposals would create an ecosystem of databases linked by digital ID that are capable of producing continuous, real-time insights about people living in the UK. They would fundamentally alter the population's relationship with the state and make access to public services contingent on surrendering vast quantities of personal information beyond its specific intended purpose.

These proposals are underpinned by the assumption that more data necessarily leads to better insights. As journalist Virginia Eubanks puts it, "these perspectives

---

20 Tony Blair Institute for Global Change, 'The Great Enabler: Transforming the future of Britain's Public,' 15 June 2023, https://institute.global/insights/tech-and-digitalisation/great-enabler-transforming-future-of-britains-public-services-digital-identity

21 Tony Blair Institute for Global Change, 'Creating Value for Users and Governments: How AI can enhance Digital ID solutions,' https://institute.global/insights/tech-and-digitalisation/creating-value-for-users-and-governments-how-ai-can-enhance-digital-id

22 Tony Blair Institute for Global Change, 'Governing in the Age of AI: Building Britain's National Data Library,' https://institute.global/insights/tech-and-digitalisation/governing-in-the-age-of-ai-building-britains-national-data-library.

23 The Observer, 'This is serious: Starmer orders move towards digital ID system,' 3 August 2025, https://observer.co.uk/news/politics/article/this-is-serious-starmer-orders-move-towards-digital-id-system

24 Times Crime and Justice Commission, 'A report into the state of the criminal justice system,' https://embed.documentcloud.org/documents/25881132-tcjc-full-report/?embed=1, p60.

25 Labour Together, 'BritCard: A Progressive Digital Identity for Britain,' June 2025, https://www.labourtogether.uk/all-reports/britcard, p27.

assume that complex controversies can be solved by getting correct information where it needs to go as efficiently as possible."[26] However, the problems that digital ID is being proposed to solve are not merely informational; they are political questions that require a debate on values and trade-offs. As we will show, it may do more harm than good.

Moreover, as these data disclosures will provide a detailed record of an individual's private life, they also engage privacy rights. Under Article 8 of the European Convention on Human Rights, any interference with privacy rights by a public authority must be necessary and proportionate. The UK GDPR also enshrines principles of data minimisation and purpose limitation, meaning that organisations and public bodies must only collect data for a specified, explicit and legitimate purpose and process only as much data as necessary to fulfil that purpose.[27] Clearly, proposals to collect any and all data for ill-defined, ambiguous aims are unlikely to comply with the UK's human rights or data protection obligations.

The following section explores some of the proposed use cases of a digital ID system and examines the dangers of adopting this approach in each context.

26 Virginia Eubanks, High-tech Homelessness, American Scientist (July-August 2018) 106(4), https://www.americanscientist.org/article/high-tech-homelessness.

27 ICO, 'A Guide to the Data Protection Principles,' https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/purpose-limitation/.

WILL DIGITAL ID WORK?

WILL DIGITAL ID WORK?

When the last Labour government brought forward proposals for an ID card scheme in the early 2000s, officials suggested it could variously be used to tackle illegal employment, unauthorised immigration, organised crime, terrorism, identity and welfare fraud, and make access to public services more efficient. It seems that over two decades later, little has changed. Much like the original proposals to introduce an ID scheme, a digital ID is touted as somewhat of a panacea for all societal problems.

Should the government decide to pursue a universal digital ID system, it must provide evidence that such a scheme is necessary and proportionate to the purpose for which it is designed – and, importantly, that it will actually achieve its stated aims. In the case of the digital ID proposals the Government is reportedly considering, it is unlikely that they would achieve the most often cited goal of reducing unauthorised immigration. These proposals would also pose significant civil liberties risks if applied to public services such as education, welfare, and healthcare.

Immigration

Many supporters of digital ID systems suggest that digital ID would help the government tackle unauthorised immigration by deterring people from crossing the channel or staying in the UK once their visa has expired or their asylum claim has been rejected. Setting out the case for digital ID, 40 Labour MPs wrote an open letter in April 2025, arguing that such a system would help to tackle "off the books employment, which is a major draw for migrants entering the country unlawfully."[28] Elsewhere, proponents of digital ID systems have suggested that digital ID would reduce the "pull factor" by making it impossible to access public services and find work or housing.[29] However, this argument rests on flawed assumptions and fundamentally misunderstands what the ID would be able to achieve and the factors behind migration to the UK.

28 Letter from 40 Labour MPs, Labour Growth Group, X, 3 April 2025, https://x.com/LabourGrowth/status/1909499797112844511/photo/1

29 Guardian, 'Digital ID cards would be good for Britain – and a secret weapon for Labour against Reform,' 9 June 2025, https://www.theguardian.com/commentisfree/2025/jun/09/britain-digital-id-cards-labour-reform-borders-identity; Sky News, Digital ID cards would help to deter migrants from heading to UK, Harriet Harman says, 11 July 2025, https://news.sky.com/story/digital-id-cards-would-help-to-deter-migrants-from-heading-to-uk-harriet-harman-says-13395054https://news.sky.com/story/digital-id-cards-would-help-to-deter-migrants-from-heading-to-uk-harriet-harman-says-13395054; The Times, No 10 examines plan for digital ID cards to cut illegal migration, 5 June 2025, https://www.thetimes.com/uk/politics/article/no-10-examines-plan-for-digital-id-cards-to-cut-illegal-migration-3fqst2dl5; The Times Commission, https://www.documentcloud.org/documents/25881132-tcjc-full-report/?embed=1&q=ID&mode=document#document/p28, p60-61

Pull Factors

It is common to hear proponents of stricter immigration control cite a range of pull factors such as access to employment, public services, housing, and welfare benefits that supposedly attract unauthorised immigrants to the UK. However, the British informal economy is relatively small compared to those of other European countries.[30] Researchers have argued that existing social networks, community ties, and familiarity with the language or culture are stronger "pull factors" than access to public services or employment.[31]

Even if there is a perception among prospective unauthorised migrants that it is easy to access public services and find work or housing in the UK, there is little evidence that a mandatory digital ID would alter this view. Studies have shown that prospective migrants have a lack of awareness about the policies and practices of the UK and instead rely on the decisions of smuggling agents, who assure them of the high quality of life at their intended destination.[32] The Home Affairs Committee's inquiry into 'Migration and Asylum' cited misleading social media campaigns which lead young Albanians to believe "that it would be easier to disappear into the grey or black economies in the UK and to earn high wages."[33] In a 2024 interview with the BBC, an unauthorised Vietnamese migrant explained that smugglers had told him "there were lots of opportunities and the living conditions were good."[34] Upon arrival, he "found that wasn't the case."[35]

Former Home Secretary Yvette Cooper also acknowledged this reality, explaining that unauthorised migrants:

> "are sold a lie by the people smuggling gangs that they will be able to live and work freely in this country, when in reality they end up facing squalid living conditions, minimal pay and inhumane working hours."[36]

It seems highly unlikely that people smugglers would warn prospective migrants

30 BBC, 'Why do Channel migrants want to come to the UK?' 9 July 2025, https://www.bbc.co.uk/news/articles/cy9xyn30yj0o.

31 Jackline Wahba and Valentina Di Iasio, 'Hotels and employment aren't major 'pull factors' for refugees – here's what really draws people to move,' Electronic Immigration Network, 25 August 2023, https://www.ein.org.uk/blog/hotels-and-employment-arent-major-pull-factors-refugees-heres-what-really-draws-people-move.

32 The Migration Observatory, 'Unauthorised Migration in the UK,' 21 January 2025, https://migrationobservatory.ox.ac.uk/resources/briefings/unauthorised-migration-in-the-uk/; The Migration Observatory, 'People Crossing the English Channel in Small Boats,' 18 July 2025, https://migrationobservatory.ox.ac.uk/resources/briefings/people-crossing-the-english-channel-in-small-boats/.

33 Home Affairs Committee, Asylum and Migration: Albania, Second Report of Session: 2022-23, 12 June 2023, https://publications.parliament.uk/pa/cm5803/cmselect/cmhaff/197/report.html.

34 BBC, 'Illegal nail bar jobs offered despite clampdown,' 19 December 2024, https://www.bbc.co.uk/news/articles/c8dqeerd75mo

35 Ibid.

36 Gov.uk, 'Nationwide clampdown on delivery riders working illegally,' 5 July 2025, https://www.gov.uk/government/news/nationwide-clampdown-on-delivery-riders-working-illegally.

against coming to the UK if the Government introduces a mandatory digital ID that potentially makes it harder to work or rent.

Even though a digital ID would not deter unauthorised migrants from coming to or staying in the UK, proponents of a digital ID argue that it would nonetheless make accessing public services, work, and housing impossible. But this belief rests on weak foundations.

Right to Work and Right to Rent

The underlying assumption in proposals for mandatory digital ID is that it would facilitate the enforcement of 'Right to Work' and 'Right to Rent' checks so effectively that it would become untenable for unauthorised migrants to live in the UK. However, rather than encouraging them to leave, these increased checks would drive unauthorised migrants into unsafe housing and 'off the books' work, intensify scrutiny of well-intentioned businesses trying to comply with their obligations and have very little impact on criminal trafficking gangs.

Employers

There are two categories of employer which fail to comply with 'Right to Work' checks. The first group skips the checks altogether, knowingly hires workers without the right to work, or turns a blind eye to the wrong documentation. The second group is well-intentioned but may be presented with fake documents, misunderstand or misapply the rules, or have poor record-keeping processes.

Certain sectors are notorious for employing high numbers of unauthorised migrants such as the construction industry, car washes, care work, hospitality, barbers, vape shops, restaurants, and takeaways.[37] A 2022 report found that more than 90 percent of car washes were likely to be employing workers who do not have the right to work in the UK, and less than half were registered companies at all.[38] In a report documenting case studies from workers in the car wash industry, an employee recalled, "pay was always cash in hand and there were no payslips, nor written contracts."[39] When the Home Office visited, his employer would produce

37 BBC, 'Illegal nail bar jobs offered despite clampdown,' 19 December 2024, https://www.bbc.co.uk/news/articles/c8dqeerd75mo; The Week, 'How many people are working illegally in the UK?' 11 July 2025, https://theweek.com/business/jobs/how-many-people-are-working-illegally-in-the-uk

38 Nottingham Trent University, New research reveals hand car wash sector is awash with exploitation, 9 May 2024, https://www.ntu.ac.uk/about-us/news/news-articles/2024/05/exploitation-in-the-hand-car-wash-sector; The Guardian, More than 90% of hand carwashes in UK employing workers illegally, study finds, 26 December 2022, https://www.theguardian.com/uk-news/2022/dec/26/more-than-90-of-hand-carwashes-in-uk-employing-workers-illegally-study-finds.

39 IFF, Worker Voices in Hand Car Washes, April 2020, https://assets.publishing.service.gov.

payslips with false records of the number of hours he had worked.[40]

In these circumstances, a digital ID system would not have any positive effect. Proponents of a digital system argue that the checks could be cross-referenced against company employment records held by HMRC and Companies House, but these shadow businesses would not even show up on those records.[41]

Similarly, there is reportedly a sizeable population of unauthorised migrants working as couriers in the gig economy by renting accounts from approved riders. Food delivery apps such as Deliveroo and Uber Eats allow riders to elect a substitute to make deliveries on their behalf. It is the official account holder who is responsible for conducting the 'Right to Work' check for the substitute rider.[42] Although couriers are prompted to verify their identity periodically, approved riders renting out their accounts to unauthorised migrants easily circumvent these checks by logging into the app, verifying their identity and then allowing the renter to log back in.[43] Unless the gig economy companies themselves became responsible for conducting checks, rather than the 'self-employed' account holders, the introduction of digital ID checks would not prevent these practices.

Requirements to check a prospective employee's 'Right to Work' documents would not deter unscrupulous employers. An unauthorised worker who was interviewed in a study explained that if "the job-seeker is a relative, the employer will hire them anyway, whether there is paper or not."[44] Employers may also choose to knowingly hire unauthorised migrants as it is more economical or because of co-ethnic solidarity among local networks.[45] It is not difficult to find posts on social media by unauthorised migrants openly sharing their immigration status and looking for work.[46] Rather than targeting these 'off the books' employers, a digital ID system would push unauthorised migrants into less secure work where the risks of crime and exploitation are higher. Indeed, the BritCard proposal acknowledges that a digital ID system would be ineffective in tackling unauthorised work in the shadow economy.[47]

---

uk/media/61b72b69e90e07043c35f586/worker-voices-in-hand-car-washes.pdf, p14.

40 Ibid.

41 Labour Together, 'BritCard: A Progressive Digital Identity for Britain,' June 2025, https://www.labourtogether.uk/all-reports/britcard, p15.

42 The Conversation, 'I'm Always Hungry Delivering Food while Hungry: How Undocumented Migrants Find Work as Substitute Couriers in the UK,' 4 May 2023, https://theconversation.com/im-always-delivering-food-while-hungry-how-undocumented-migrants-find-work-as-substitute-couriers-in-the-uk-201695

43 Ibid.

44 Bloch, Kumarappan and Mckay, 'Employer sanctions: The impact of workplace raids and fines on undocumented migrants and ethnic enclave employers, ' Critical Social Policy (2015) 35(1), 132-151. https://doi.org/10.1177/0261018314545600.

45 Ibid.

46 BBC, 'Illegal nail bar jobs offered despite clampdown,' 19 December 2024, https://www.bbc.co.uk/news/articles/c8dqeerd75mo

47 Labour Together, 'BritCard: A Progressive Digital Identity for Britain,' June 2025, https://www.labourtogether.uk/all-reports/britcard, p16.

But even law-abiding employers should fear a mandatory digital ID system. Most employers conduct right-to-work checks satisfactorily, but some make mistakes which lead to non-compliance. Labour Together proposes that digital ID could be an effective tool to combat fake documents.[48] But if the problem is predominantly "record keeping and rechecking documents," then having an easy way to prove the right to work is unlikely to actually solve that problem.[49]

Some genuine employers are duped by false documentation. Proponents of digital ID suggest that "it is relatively easy for a worker or tenant to present a document that belongs to someone else or to produce a fake document."[50] However, digital ID documents are not immune to falsification. A cybersecurity engineer demonstrated that Gov.uk One Login itself is susceptible to impersonation.[51] In September 2023, the National Cyber Security Centre warned that the design of One Login left it vulnerable to identity theft.[52] In Paris, a large criminal network was found to be conducting document fraud, including forged Belgian, Spanish and Italian identity cards.[53] Similarly, in India, a software fault meant that fake ID cards could be generated remotely without genuine verification.[54]

Despite the implementation of ID cards in Europe, unauthorised employment prevails. In 2019, The Nation interviewed an unauthorised migrant who continued to work in France "under the table for 550 euros per month as a window cleaner" and receives payment "unaddressed and endorsed by a friend with legal working status."[55] Despite Belgium having similar ID checks for most services, there were up to 150,000 unauthorised migrants in 2020.[56] The experience of foreign ID systems should dampen the enthusiasm of those hoping that a British digital ID system would make a significant difference to the rate of unauthorised employment.

---

48 Ibid, p15.

49 Home Office, 'Employer Awareness of, and self-reported compliance with, Right to Work checks,' 1 April 2025, https://www.gov.uk/government/publications/employer-awareness-of-right-to-work-checks/employer-awareness-of-and-self-reported-compliance-with-right-to-work-checks.

50 Labour Together, 'BritCard: A Progressive Digital Identity for Britain,' June 2025, https://www.labourtogether.uk/all-reports/britcard, p15.

51 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-pivoted-from-a-trial-tenant-to-compromising-customer-signing-keys/

52 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/

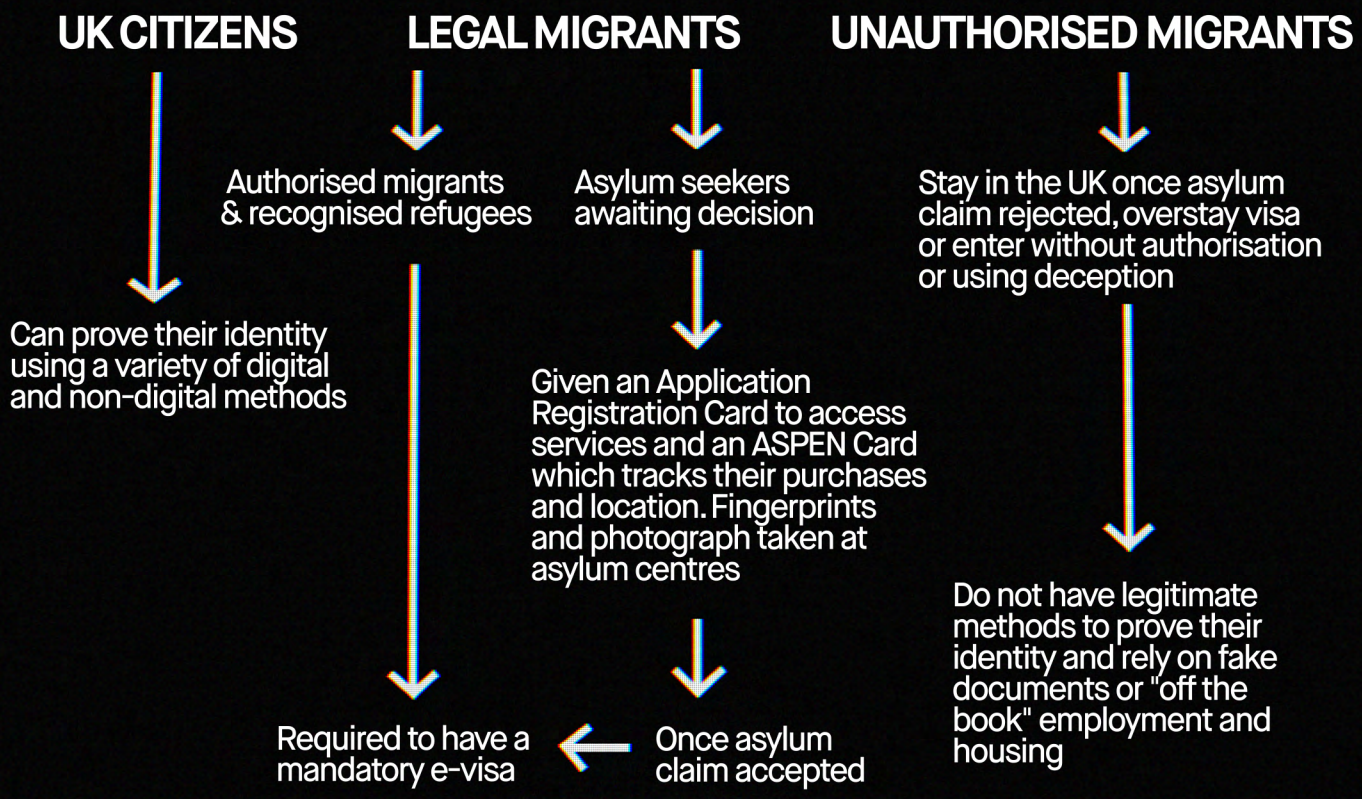
53 Europol, 'Two print shops producing fake EU documents dismantled in Paris,' 18 June 2020, https://www.europol.europa.eu/media-press/newsroom/news/two-print-shops-producing-fake-eu-documents-dismantled-in-paris

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

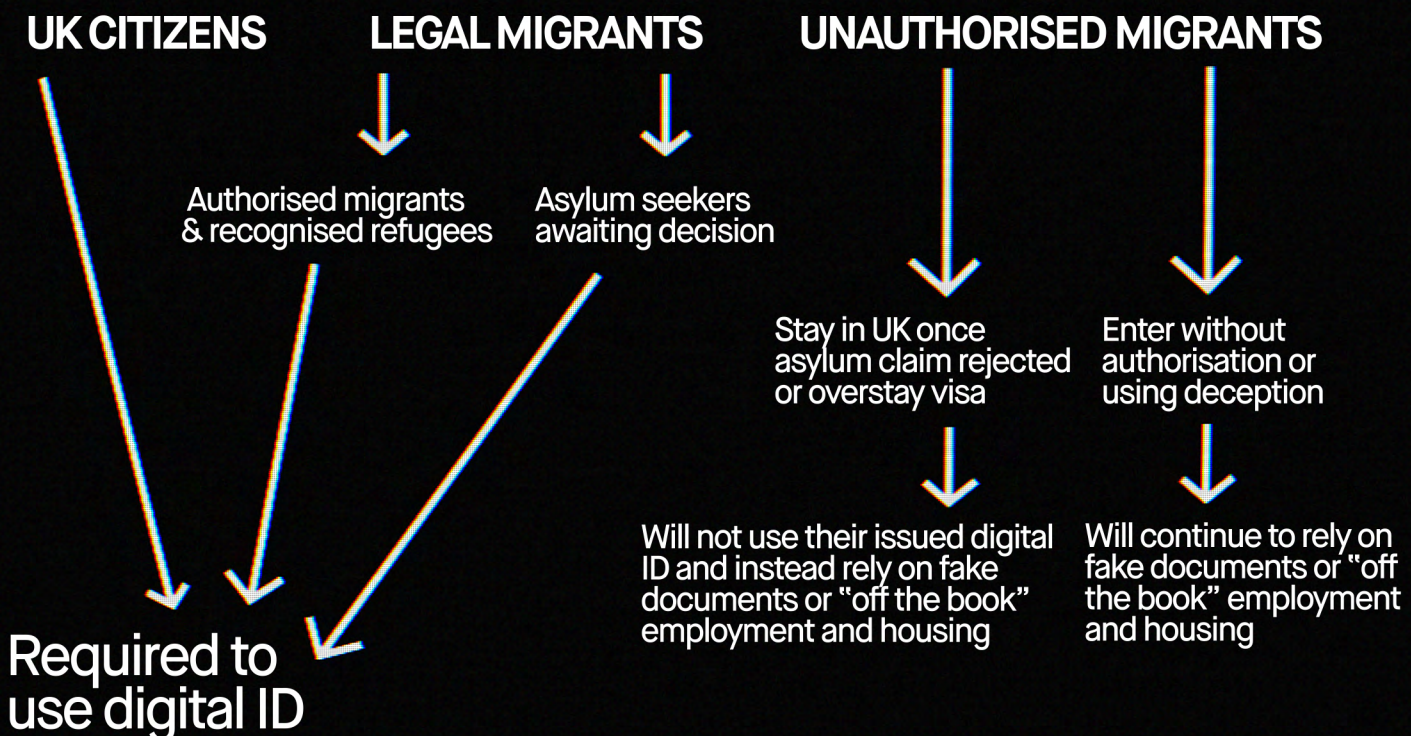
55 The Nation, 'France's Undocumented Migrants are Fighting for their Rights' 31 December 2019, https://www.thenation.com/article/archive/france-migrants-macron-refugees/

56 Middle East Monitor, 'Son of Iraq refugee takes office as Migration Minister in Belgium,' 20 October 2020, https://www.middleeastmonitor.com/20201020-son-of-iraq-refugee-takes-office-as-migration-and-asylum-minister-in-belgium/

CURRENT ID REQUIREMENTS



PROPOSED ID REQUIREMENTS



Landlords

Landlords would also be affected by the digital ID proposals, as they would have to use digital ID to verify 'Right to Rent' status. However, many unauthorised migrants stay with friends or landlords who do not conduct these checks. An unauthorised migrant from Vietnam recalled "carrying all of his possessions in a small black bag and had been sofa surfing around the UK for weeks."[57] It is unlikely that these 'unofficial' landlords would register in the first place, meaning that the Home Office would not be able to identify an absence of checks on their record – it simply would not exist. There are also reports of asylum seekers, who live in hotels while their application is processed, working without authorisation on food delivery apps. The use of digital ID in 'Right to Rent' checks would have little effect in tackling these instances of unauthorised employment because the Home Office already knows the immigration status of these individuals.[58]

Problems with digital ID in immigration

The Border Internalised

Under the proposed digital ID system, Britain risks becoming a checkpoint society. We could expect to have to prove our identities in order to use the NHS, access benefits, get a job, rent property, get a driving licence, open a bank account, and much more. It is not clear in the proposals exactly what data would be shared with governmental departments each time digital ID is used.

Burden on Businesses

Proponents of a digital ID system have argued that it would "support broader efforts to tackle modern slavery by enabling more effective targeting of checks and thus improve identification of victims."[59] However, as set out above, the Home Office is highly unlikely to identify unscrupulous employers and landlords acting unlawfully or those trafficking victims of modern slavery through digital ID checks. Instead, it would target enforcement towards those businesses and landlords who, for all intents and purposes, are doing their best to comply. In other words, instead of government resources being put towards trafficking and criminal gangs, it would be law-abiding citizens who are hit with heavy – and potentially reputation

57 BBC, 'Illegal nail bar jobs offered despite clampdown,' 19 December 2024, https://www.bbc.co.uk/news/articles/c8dqeerd75mo

58 BBC, 'Home Office to share asylum hotel data with food delivery firms,' 23 July 2025, https://www.bbc.co.uk/news/articles/cy4yjpv87v0o

59 Labour Together, 'BritCard: A Progressive Digital Identity for Britain,' June 2025, https://www.labourtogether.uk/all-reports/britcard, p17.

damaging – immigration raids.[60]

The 'BritCard' proposal would also impose additional burdens on employers. Currently, companies that employ self-employed contractors are not liable if the contractor is later revealed to be an unauthorised worker. However, if the BritCard proposal were implemented, "these employers would need to carry out checks on all individuals they engage regardless of employment status."[61]

Discrimination of ethnic minorities

Policy Exchange acknowledged the reality that "people who do not look and sound like the ethnic majority are more likely to be subject to status checks." To tackle this, it recommends "that, so far as possible, everyone is checked and everyone is subject to spot-checks."[62] Neither outcome is particularly reassuring: at best, the entire population would be subject to increased checks and at worse – and more likely – these increased checks would disproportionately target ethnic minorities.

Some digital ID supporters have suggested that a digital ID scheme could reduce discrimination by "introducing one simple way for everyone to prove their immigration status that is free, instant and convenient."[63] However, in reality, it is going to be ethnic minorities who are asked to show their ID by default. As The New Arab put it, "For minority groups, a small piece of plastic also allows for the questioning of your right to be in the country you call home. And that questioning... can be constant, violent and deeply traumatic."[64]

During the mid-1990s in France, young people of Algerian or Moroccan descent reported being asked to produce their ID cards several times a week, risking arrest and detention if they refused.[65] In Belgium, a 20 year-old citizen of African origin, Bicha Monkokole Kasembele, was stopped by the police and arrested, after they refused to believe that the identity card she produced was real.[66] Kasembele filed an official complaint against the police and the foreign affairs ministry, which acknowledged that this was not the only similar error.

60 BBC, 'Home Office issues apology over immigration raid," 22 May 2025, https://www.bbc.co.uk/news/articles/cm23m38vz78o.
61 Labour Together, 'BritCard: A Progressive Digital Identity for Britain,' June 2025, https://www.labourtogether.uk/all-reports/britcard, p29.
62 Policy Exchange, 'The Border Audit: Is the UK border now fit for purpose? A post-Windrush Review,' 2018, https://policyexchange.org.uk/wp-content/uploads/2018/07/The-Border-Audit.pdf, p63.
63 Labour Together, 'BritCard: A Progressive Digital Identity for Britain,' June 2025, https://www.labourtogether.uk/all-reports/britcard, p17.
64 The New Arab, 'Introducing Mandatory ID cards will threaten the civil liberties of minorities in the UK,' 24 November 2022, https://www.newarab.com/opinion/id-cards-will-threaten-minorities-civil-liberties-uk.
65 Institute of Race Relations, 'ID cards: Implications for Black, Minority Ethnic, Migrant and Refugee communities,' 26 May 2005, https://irr.org.uk/article/id-cards-implications-for-black-minority-ethnic-migrant-and-refugee-communities/.
66 Statewatch, 'Belgium: Women in Repatriation Blunder,' 28 March 2012, https://www.statewatch.org/news/2003/august/belgium-woman-in-repatriation-blunder/

THE RACIALISED HARMS OF MANDATORY DIGITAL ID

by Dr Shabna Begum, CEO of the Runnymede Trust

Mandatory digital ID schemes risk creating significant perils for communities of colour. Whilst currently proposals in the UK are marketed as improving efficiency, reducing fraud, enhancing national security and tracking undocumented migration, there is little attention to the unequal costs - and indeed increased harms that mandatory ID schemes will pose to racialised communities in the UK. In fact, given the very heated political environment where we have witnessed a rise in far-right racist politics, this policy can be seen to rely on and exploit heightened fears about 'illegal' migrants accessing public services, as a way to secure public support.

There are practical problems; the suite of technologies and information that digital ID systems often rely on - biometric systems and particularly facial recognition and fingerprinting technology, have been shown to disproportionately misidentify individuals from racialised communities. Research by Amnesty International indicates that these technologies are less accurate for people of colour, which in the context of institutional racism, will likely lead to increased surveillance and discriminatory outcomes for these communities.[1] In addition, there are also barriers around digital exclusion which we know apply to certain communities of colour at higher rates than for the wider population which will likely aggravate the inequalities and discrimination experienced.[2]

There is also considerable evidence that the mass collection of personal data through digital ID systems will worsen our increasingly aggressive surveillance culture. In our recent report 'A hostile environment: language, race, politics and the media' (2025), we highlighted how hostile environment immigration policies have effectively 'deputised' ordinary citizens to act as immigration enforcers; members of the public, education and healthcare professionals, as well as employers and a landlords are essentially obliged to surveil and assess the immigration status of the people they encounter and often the decisions they make are deeply racialised.[3] Mandatory digital ID will turbo-charge this surveillance culture where people of colour who are seen to be outside of the 'citizenship community' are more likely to be interrogated for their digital ID as a prerequisite to access to services.

1 Amnesty International, 'Automated Racism: How police data and algorithims code discrimination into policing', February 2025, https://www.amnesty.org.uk/files/2025-02/Automated%20Racism%20Report%20-%20Amnesty%20International%20UK%20-%202025.pdf?VersionId=JqCcTODw37yAXylNmAY6uAzrKEWucFF7

2 Ofcom, 'Exploring Digital Disadvantage', page 33, February 2025, https://www.ofcom.org.uk/siteassets/resources/documents/internet-based-services/technology/research-digital-disadvantage/exploring-digital-disadvantage-research-report.pdf?v=393692

3 The Runnymede Trust, 'A hostile environment: language, race, politics and the media', February 2025, https://www.runnymedetrust.org/publications/a-hostile-environment-language-race-politics-and-the-media

Whilst advocates argue that this would protect against the outcomes of the Windrush scandal, this represents a fundamental misdiagnosis of the root problem; the Windrush scandal was caused by a specific hostile environment policy that created a bureaucratic system requiring particular ID verification, and to which people of colour were more likely exposed. To advocate for further entrenching ID requirements is to renew and create more hurdles for people of colour and fails to address the real problems that come from our immigration system.

We also cannot ignore the fact that the timing of the proposals, coinciding with rising support for far right, anti-immigrant politics, suggests it is a reactionary move rather than a result of careful policy development or consultation with affected communities. We are witnessing an increasingly hostile environment towards migrants and people seeking asylum and as in the past, governments will often exploit fears around migration as a way to validate regressive and intrusive extensions of state powers. This has historically always impacted people of colour, particularly settled communities, the hardest.

There are too many technological imperfections and likely racialised harms posed by the current proposals, and so it is essential that the government resists the temptation to rush ahead with a policy that clearly has so many discriminatory implications and risks.

Education

Various Labour-leaning think tanks have suggested that a mandatory universal digital ID system could have a role to play in the education sector. Setting out its plan for 'The Future of Learning,' TBI suggests that it is possible to "provide each child with a personalised education" by making use of "the power to accumulate and analyse vast amounts of data."[67] In order to achieve this aim, TBI recommends introducing a digital learner ID for each student that would "contain all educational information, including formal test results, attendance records, week-by-week assessments, marked homework, records of non-academic achievement," and provide pupils and parents with "useful insights from the information."[68] The 40 MPs who called for the introduction of a digital ID for "more tailored education services," were likely drawing on this assessment[69]

Labour Together's BritCard proposal also suggests that the Department for Education could build on its existing "digital single pupil number," to deliver "the full potential benefits of digital identity."[70] The number Labour Together refers to is the unique pupil number (UPN), which identifies and remains with pupils throughout their school career. The UPN is linked to the National Pupil Database, permitting "accurate and timely data sharing between schools, central authorities and local government."[71] The Times Crime and Justice Commission similarly advocates for a single unique identifier for each child from birth to match up datasets across public services.[72]

A mandatory, universal digital ID system would draw in more personal information from students that is likely to stay with them on their permanent record and facilitate greater sharing of this data across government departments.

Problems with digital ID in education

A learner ID would form a detailed record of each pupil's progress and attainment across their compulsory education. TBI suggests that analysis of this data could support teachers to offer targeted interventions and personalised content. In

67 Tony Blair Institute for Global Change, 'The Future of Learning: Delivering Tech-Enabled Quality Education for Britain,' 7 July 2023, https://institute.global/insights/public-services/future-of-learning-delivering-tech-enabled-quality-education-for-britain.
68 Ibid.
69 Open Letter signed by 40 Labour MPs, Labour Growth Group, X, 3 April 2025, https://x.com/LabourGrowth/status/1909499797112844511/photo/1.
70 Labour Together, 'BritCard: A Progressive Digital Identity for Britain,' June 2025, https://www.labourtogether.uk/all-reports/britcard, p20.
71 Department for Education, Unique Pupil Numbers (UPNs), June 2019, https://assets.publishing.service.gov.uk/media/5cfa739a40f0b663fd865a6a/UPN_Guide_1.2.pdf, p4.
72 Times Crime and Justice Commission, 'A report into the state of the criminal justice system,' https://embed.documentcloud.org/documents/25881132-tcjc-full-report/?embed=1, p67.

practice, students could receive tailored suggestions about educational support, career prospects, extracurricular activities and work experience opportunities on the basis of their digital-ID linked data.[73] However, mining student data for insights could also lead to adverse interventions.

Two predictive analytics models which lend themselves to the education context are early alert systems that identify at-risk students and recommender systems that forecast performance and future activity.[74] These algorithms can draw from a wide range of data, including demographic data, test scores, attendance, academic performance and behaviour.[75]

Recommender systems are AI-powered predictive models that forecast performance and future activity.[76] These types of algorithmic profiling are likely to entrench existing biases. For example, certain students could be directed towards inappropriate academic and professional paths, and algorithmic models could predict worse outcomes for racial minorities due to historic discrimination reflected in datasets and replicated in predictions.[77] This was exemplified by the A-level grading scandal during the COVID-19 pandemic. The exams regulator Ofqual relied on an algorithm to centrally moderate internal teacher assessments. Almost 40 percent of students received grades below what they were anticipating, however, the algorithm did not downgrade results uniformly. Higher achievers in historically lower-performing schools were more likely to be given lower grades than predicted. By contrast, the number of A* and A grades achieved at private schools rose by 4.7 percent – more than double the rate at comprehensive schools.[78]

Labelling students in this data-driven way could also stymie future opportunities by leaving them with a 'permanent record'[79] or by creating a self-fulfilling cycle in which students underperform due to lowered expectations from educators and administrators.[80]

---

73 Tony Blair Institute for Global Change, 'The Great Enabler: Transforming the future of Britain's Public,' 15 June 2023, https://institute.global/insights/tech-and-digitalisation/great-enabler-transforming-future-of-britains-public-services-digital-identity.

74 New America, 'The Promise and Peril of Predictive Analytics in Higher Education,' October 2016, https://www.luminafoundation.org/wp-content/uploads/2017/08/promise-and-peril.pdf.

75 Ibid.

76 Ibid.

77 Inside Higher Ed, 'Report: Predictive Models may have bias against black and Hispanic learners,' 19 July 2024, https://www.insidehighered.com/news/student-success/academic-life/2024/07/19/predictive-models-higher-ed-disadvantage-some#:~:text=Predictive%20analysis%20models%20commonly%20used,sets%20and%20other%20systemic%20inequitiessets and other systemic inequities".

78 BBC, 'A-levels: Anger over 'unfair' results this year,' 13 August 2020, https://www.bbc.co.uk/news/education53759832.

79 Zeide E. Education Technology and Student Privacy. In: Selinger E, Polonetsky J, Tene O, eds. The Cambridge Handbook of Consumer Privacy. Cambridge Law Handbooks. Cambridge University Press; 2018:70-84, 70.

80 New America, 'The Promise and Peril of Predictive Analytics in Higher Education,' October 2016, https://www.luminafoundation.org/wp-content/uploads/2017/08/promise-and-peril.pdf.

By proposing that a digital ID could be used to "apply directly to further study or jobs,"[81] the proposal provides incentives for excessive data sharing. Even if this were optional, employers may come to expect high levels of educational data disclosure from applicants to the extent that it becomes de facto mandatory in order to remain competitive.

TBI argues that data collected could be anonymised and aggregated to analyse trends and real-time patterns.[82] One example is to allow local governments to provide targeted interventions. It is not difficult to imagine a scenario in which the National Pupil Database is linked with policing data for pre-crime interventions, welfare and family data for safeguarding interventions or health data for pre-emptive medical interventions.[83] For example, in several US states, Google Chromebooks were automatically installed with suicide prevention software that scanned the work and behaviour of students in order to detect signs of depression.[84]

Algorithmic profiling has already been used by Bristol City Council and Avon and Somerset Police to identify children at risk of sexual or criminal exploitation and those at risk of becoming 'Not in Employment, Education or Training' (NEET) by drawing on the Think Family database, comprising of the data of 50,000 families derived from the police, the Department for Work and Pensions (DWP), and the social care department.[85] Schools who use the app receive notifications when children and their family members have contact with the police or have involvement with anti-social behaviour, missing persons incidents or domestic abuse.[86] However, criminal and racial justice campaigners argue that the app risks those from poorer or minority backgrounds being profiled for gang involvement and subjected to increased surveillance.[87]

Finally, the TBI suggests that "granular real-time data could be used to monitor how schools perform, replacing infrequent, high-stakes Ofsted inspections."[88]

---

81 Ibid

82 Tony Blair Institute for Global Change, 'The Future of Learning: Delivering Tech-Enabled Quality Education for Britain,' 7 July 2023, https://institute.global/insights/public-services/future-of-learning-delivering-tech-enabled-quality-education-for-britain.

83 New America, 'The Promise and Peril of Predictive Analytics in Higher Education,' October 2016, https://www.luminafoundation.org/wp-content/uploads/2017/08/promise-and-peril.pdf.

84 LSE Media Blog, EdTech in Schools: A Threat to Data Privacy? 27 May 2021, https://blogs.lse.ac.uk/medialse/2021/05/27/edtech-in-schools-a-threat-to-data-privacy/

85 The Guardian, 'Calls to shut down Bristol schools' use of app, to monitor pupils and families,' 21 September 2023, https://www.theguardian.com/education/2023/sep/21/calls-to-shut-down-bristol-schools-use-of-think-family-education-app-pupils-and-families.

86 Bristol.gov.uk, Insight Bristol and The Think Family Database, https://www.bristol.gov.uk/residents/social-care-and-health/children-and-families/insight-bristol.

87 The Guardian, 'Calls to shut down Bristol schools' use of app, to monitor pupils and families,' p21. September 2023, https://www.theguardian.com/education/2023/sep/21/calls-to-shut-down-bristol-schools-use-of-think-family-education-app-pupils-and-families.

88 Tony Blair Institute for Global Change, 'The Great Enabler: Transforming the future of Britain's Public,' 15 June 2023, https://institute.global/insights/tech-and-digitalisation/great-enabler-transforming-future-of-britains-public-services-digital-identity.

While Ofsted inspections have been criticised as being "unfair" and "inaccurate," it is unclear whether subjecting teachers to constant data-driven surveillance and analysis, even in aggregate, is likely to reduce stress or improve outcomes.[89]

The type of data analytics, data-mining, and profiling imagined in the aforementioned proposals requires the expertise and software of the private sector, which is known as 'EdTech.' As a result, data extends far beyond the school's systems and may be processed by programmers, administrators, business strategists, data analysts and others who develop, sell and manage these technologies.[90] It also removes what Velislava Hillman calls "pedagogic agency," as EdTech models become the key driver for educational philosophy, "overrid[ing] existing pedagogies and the very expertise of educators." In doing so, it completely reverses the relationship between students and teachers and redefines the education landscape with unintended consequences to rights and freedoms.[91]

Welfare

Labour Together suggests that BritCard could be expanded to control access to welfare benefits.[92] The 40 Labour MPs who called for a digital ID programme in an open letter propose that it could be instrumental in "tackling benefit fraud and to offering more targeted financial support."[93] The TBI argues that digital ID could be used to administer welfare benefits automatically by sharing data across governmental departments. For example, digital ID could permit disclosures between the HMRC, the DWP and energy providers to identify households entitled to electricity cost subsidies.[94] The Institute also suggests that digital ID could facilitate the linkage of benefits and health data to reduce workforce inactivity by offering tailored and personalised support to specific groups.[95]

89 UCL, Teachers call Ofsted Inspections Unfair and Inaccurate Even in Outstanding or Good Schools, 2 November 2023, https://www.ucl.ac.uk/news/2023/nov/teachers-call-ofsted-inspections-unfair-and-inaccurate-even-outstanding-or-good-schools.
90 LSE Media Blog, EdTech in Schools: A Threat to Data Privacy? 27 May 2021, https://blogs.lse.ac.uk/medialse/2021/05/27/edtech-in-schools-a-threat-to-data-privacy/.
91 Yoni Har Carmel, 'Regulating "big data education" in Europe: lessons learned from the US,' Internet Policy Review (2016) 5(1), https://doi.org/10.14763/2016.1.402.
92 Labour Together, 'BritCard: A Progressive Digital Identity for Britain,' June 2025, https://www.labourtogether.uk/all-reports/britcard, p9.
93 Open Letter signed by 40 Labour MPs, Labour Growth Group, X, 3 April 2025, https://x.com/LabourGrowth/status/1909499797112844511/photo/1.
94 Tony Blair Institute for Global Change, 'The Great Enabler: Transforming the future of Britain's Public,' 15 June 2023, https://institute.global/insights/tech-and-digitalisation/great-enabler-transforming-future-of-britains-public-services-digital-identity.
95 Tony Blair Institute for Global Change, 'Governing in the Age of AI: Building Britain's National Data Library,' 25 February 2025, https://institute.global/insights/tech-and-digitalisation/governing-in-the-age-of-ai-building-britains-national-data-library.

Problems with digital ID in welfare

However, there are dangers associated with algorithmically administering benefits and detecting fraud based on vast quantities of personal information received about an individual for different purposes. For example, in Denmark, where databases are linked by a single citizen ID, the welfare authorities administered almost 60 separate algorithms with the help of a private company in order to detect fraud and flag individuals for further investigation. Amnesty International found that algorithms designed to detect a person's relationship status or living arrangement discriminated against people on the basis of national origin or migration status, as well as those living in non-traditional arrangements including disabled people, the elderly and multi-generational immigrant households.[96]

Further, given the current controversies over disabled people being pressured back into work and the low level of public trust towards the DWP, proposals to counter economic inactivity by analysing the health and welfare data of benefits recipients are likely to be controversial.

Healthcare

In its BritCard proposal, Labour Together argues that the NHS could use a digital ID system to check health records and verify whether someone is entitled to free healthcare, thereby "making healthcare more effective and efficient."[97] Other proponents of digital ID systems have argued that digital IDs could facilitate NHS "patient passports"[98] and a centralised digital health record "containing an individual's full medical history."[99]

The NHS has already gone some way in developing these systems. The NHS app, which is accessed through the NHS login system, gives patients access to their GP medical records, test results and prescriptions. In order to access their healthcare record, patients must provide a high level of proof of who they are.[100] This could be

96 Amnesty International, 'Denmark: AI powered welfare system fuels mass surveillance and risks discriminating against marginalized groups – Report,' 12 November 2024, https://www.amnesty.org/en/latest/news/2024/11/denmark-ai-powered-welfare-system-fuels-mass-surveillance-and-risks-discriminating-against-marginalized-groups-report/.

97 Labour Together, 'BritCard: A Progressive Digital Identity for Britain,' June 2025, https://www.labourtogether.uk/all-reports/britcard, p19.

98 Open Letter signed by 40 Labour MPs, Labour Growth Group, X, 3 April 2025, https://x.com/LabourGrowth/status/1909499797112844511/photo/1.

99 Tony Blair Institute for Global Change, 'The Great Enabler: Transforming the future of Britain's Public,' 15 June 2023, https://institute.global/insights/tech-and-digitalisation/great-enabler-transforming-future-of-britains-public-services-digital-identity.

100 NHS, 'NHS Login,' 22 December 2021, https://www.nhs.uk/nhs-services/online-services/nhs-login/#:~:text=By%20submitting%20photo%20identification%20and,UK%20entry%20clearance%20visa%20sticker.

through a biometric face scan or using registration details from their GP surgery.

During the pandemic, the government also introduced the NHS COVID pass, which was incorporated into the NHS app to allow users to prove their vaccination status. COVID passes were required as a condition of entry to various venues, including pubs, restaurants and cinemas. Big Brother Watch opposed this population-wide digital ID health system on the basis that it amounted to an unprecedented privacy intrusion that undermined fundamental rights and threatened to discriminate against some of the most marginalised groups in society. There was no evidence that COVID passes stopped the spread of coronavirus.[101] The scheme was scrapped in May 2021.[102]

Problems with digital ID in healthcare

Medical data is among the most sensitive personal information about an individual. The Ada Lovelace Institute explains that the "datafication" of health gives those with control over data the wide-reaching potential to influence individuals by inferring their health status from their data and repurposing it for other uses.[103] In India, where a digital ID is required for the sharing of healthcare records, individuals living with HIV and AIDS reportedly refused medical treatment and medicines because they feared that their identities would be disclosed.[104] In a joined-up system with liberal cross-departmental sharing across databases, it is not a stretch to imagine welfare applications being decided without the claimant's input, but merely by reference to their health and tax records.

Health Secretary Wes Streeting expressed his mission to "transform the NHS over the coming decade, from a service which diagnoses and treats ill-health to one that predicts and prevents it."[105] In June 2025, Streeting announced that all babies will have their DNA mapped and undergo whole genome sequencing in order to predict diseases and personalise health care.[106] This plan to process, record and monitor highly sensitive personal information has serious privacy implications. In this context, proposals for a joined-up digital ID system, where health and biometric data can be linked to all other data available to public authorities, are particularly chilling.

---

101 BBC, 'COVID passes: Where do I still need to use one?' 28 February 2022, https://www.bbc.co.uk/news/explainers-55718553.

102 UK Health Security Agency, NHS COVID Pass, 7 May 2021, https://www.gov.uk/guidance/nhs-covid-pass.

103 Ada Lovelace Institute, 'The Data Will See You Now: The Datafication and the boundaries of health,' 29 October 2020, https://www.adalovelaceinstitute.org/report/the-data-will-see-you-now/.

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

105 The Telegraph, 'DNA Screening for Every Baby on the NHS,' 20 June 2025, https://www.telegraph.co.uk/news/2025/06/20/dna-screening-for-every-baby-under-nhs-plan/.

106 Ibid.

The integration of genetic data into digital ID systems raises serious ethical and privacy concerns, especially regarding consent and control of personal data. Babies and children cannot meaningfully consent to having their genetic information linked to a digital identity that is permanently on their record. Moreover, genetic data is inherently relational; due to patterns within families, it is possible to derive information about relatives without obtaining their express consent.[107] There are additional concerns that attaching genetic data to digital ID systems could lead to discriminatory outcomes. For example, individuals can carry genetic patterns that they would prefer to keep private. If such information is accessible through a digital ID system, either intentionally or through data breaches, those individuals could be discriminated against by the government, employers and insurance companies.[108]

Worryingly, these proposals are also being couched in terms of third-party data sharing. TBI suggests that patients could supplement their digital health record with "information generated by wearables, genomic-risk profiles, routine at-home diagnostic tests and care provided outside the NHS."[109] This raises further concerns about how data would be shared with private companies and the level of control the user would have over their data once it had been surrendered. The digital record could be "expanded to provide targeted guidance on new treatment options or clinical-trial opportunities to match patient needs."[110]

National Data Library

In its manifesto, the Labour Party committed to creating a National Data Library (NDL) in order to consolidate "existing research programmes and help deliver data-driven public services."[111] There is no articulated blueprint for what this Data Library would look like; however, several organisations have put forward proposals.

The centre-right think tank Onward recommends that the NDL should take the format of a "centralised, platform focused on linked-up high-quality data to allow companies and researchers to harness AI."[112] A digital ID system would facilitate the linking of public data for this purpose. Similarly, the TBI envisions a NDL which links de-identified data sets across governmental departments to unlock insights and argues that the "UK should introduce a unique personal identifier to

107 Simon Garfinkel, Database Nation: The Death of Privacy in the 21st Century (2000), O'Reilly & Associates.
108 Ibid.
109 Ibid.
110 Tony Blair Institute for Global Change, 'The Great Enabler: Transforming the Future of Britain's Public Services Through Digital Identity,' 15 June 2023, https://institute.global/insights/tech-and-digitalisation/great-enabler-transforming-future-of-britains-public-services-digital-identity.
111 Labour Party Manifesto, 2024, https://labour.org.uk/wp-content/uploads/2024/06/Change-Labour-Party-Manifesto-2024-large-print.pdf, p33.
112 Onward, 'Let's get real about Britain's AI status,' 2 May 2024, https://sciencesuperpower.substack.com/p/lets-get-real-about-britains-ai-status

support accurate and efficient data linkage across public services."[113] In practice, the TBI imagines this could look like digital ID systems drawing together data on student-progression, employment and earning records and linking it to anonymised exams and teaching materials in order to train ed-tech AI models.[114]

Problems with this model

The Ada Lovelace Institute has identified several common issues with datasets, including historical biases, inaccuracies, inconsistencies in data recording, a lack of clarity around what the data actually measures, and the underrepresentation of historically marginalised groups.[115] A digital ID system can give a false sense of accuracy when it comes to tracking and observing someone. In such multi-purpose systems, data can be taken out of its original context and amplified when fed into AI models, meaning that it does not reflect an individual's experience. As a result, individuals can be wrongly flagged, miscategorised, or disregarded, which has significant implications when their data is mined for insights.

The limitations of de-identification

Data is considered anonymised when it is removed of personal identifiers such as names, telephone numbers, and postcodes. However, even de-identified data can be re-identified in three specific ways: firstly, where it is has been insufficiently de-identified; secondly, where datasets have been pseudonymised, but the method for pseudonymisation is decoded and reversed; and finally, and most effectively, where datasets are combined.[116] This is because "quasi-identifiers" such as date of birth and gender can be linked with quasi-identifiers in another dataset which still contains personal identifiers, making it possible to reidentify an individual.[117]

Given the aim of combining datasets in a digital ID system, the safeguard of anonymisation is particularly weakened. Additionally, the more the data is anonymised, the less useful it is for analysis; therefore, there is an incentive for re-identification of anonymised datasets.[118] The TBI acknowledges this incentive

113 Tony Blair Institute for Global Change, 'Governing in the Age of AI: Building Britain's National Data Library,' 25 February 2025, https://institute.global/insights/tech-and-digitalisation/governing-in-the-age-of-ai-building-britains-national-data-library.
114 Ibid.
115 Ada Lovelace Institute, 'Learn Fast and Build Things,'14 March 2025, https://www.adalovelaceinstitute.org/policy-briefing/public-sector-ai/.
116 Boris Lubarsky, 'Re-Identification of "Anonymized" Data' (2017) Georgetown Law Technology Review, 1 GEO. L. TECH. REV. 202, https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/.
117 Michael. D Smith, Jim Waldo, Anonymity, De-Identification, and the Accuracy of Data, 28 August 2023, https://www.harvardonline.harvard.edu/blog/anonymity-de-identification-accuracy-data.
118 Boris Lubarsky, 'Re-Identification of "Anonymized" Data' (2017) Georgetown Law

by proposing that the National Data Library should eventually use identifiable data, since policy formation, research projects and service delivery sometimes require a "more granular level of detail to be effective."[119]

Technology Review, 1 GEO. L. TECH. REV. 202, https://georgetownlawtechreview.org/re-identification-of-anonymized-data/GLTR-04-2017/.

119 Tony Blair Institute for Global Change, 'Governing in the Age of AI: Building Britain's National Data Library,' 25 February 2025, https://institute.global/insights/tech-and-digitalisation/governing-in-the-age-of-ai-building-britains-national-data-library.

WHAT ARE THE RISKS OF DIGITAL ID?

WHAT ARE THE RISKS OF DIGITAL ID?

Privacy

What data is collected?

If a multi-purpose system which 'joins up' government records is introduced, a digital ID system with a permanent unique identifier linking an individual's immigration, employment status, and healthcare and education data would be possible. The 'BritCard' proposal recommends creating a log every time the digital ID is used, which means that every interaction requiring its use would create a permanent record in the government's databases.[120]

When individuals currently prove their identity, they typically do so in a context-specific manner appropriate for the interaction, rather than through a single unique identifier linked to all of their activities. This approach preserves privacy by limiting data disclosure to what is necessary for each interaction, reducing the risk of excessive data sharing. As the LSE Identity Project Report explained in June 2005, "existing systems are purpose built and necessarily proportionate in their demands for personal information."[121] In this context, data silos are safeguards. While they may limit the efficiency of data sharing between governmental departments, they preserve something far more valuable: autonomy; security; dignity; and privacy.

Currently, data sharing across governmental departments typically occurs within explicit legal frameworks, statutory powers and formal data sharing agreements. Although these sharing frameworks vary and cross-departmental sharing can be improved from a privacy and security perspective, data sharing remains largely context-specific and, in some cases, subject to public debate and consultation. Similarly, in order to access the National Pupil Database, external third party requesters must apply to the Department for Education's Data Sharing Approval Panel, which scrutinises every application.[122] While these data-sharing processes are far from perfect, and have received far-ranging criticism from rights groups[123] and

120 Labour Together, 'BritCard: A Progressive Digital Identity for Britain,' June 2025, https://www.labourtogether.uk/all-reports/britcard, p15, p23.
121 Simon Davies, Simon, Ian Hosein and Edgar Whitley, The identity project : an assessment of the UK Identity Cards Bill and it's implications (2005) London: LSE Research Online, http://eprints.lse.ac.uk/archive/00000684, p258.
122 Department for Education, Data Sharing and Approval Panel (DSAP) – Terms of Reference, https://assets.publishing.service.gov.uk/media/66e076fe865c0eef0bc42dea/DSAP_ToR_Jul24.pdf
123 Defend Digital Me, 'National Pupil Database,' https://defenddigitalme.org/my-school-records/national-pupil-data/; The Register, UK.gov STILL wants to tout pupil data – don't use the word 'product', 20 May 2013, https://www.theregister.com/2013/05/20/national_pupil_database_government_response_on_gove_proposed_amendments/

even the Information Commissioner,[124] each case has to be justified and assessed, and the sharing occurs in a targeted way for a specific purpose. The introduction of a digital ID system could remove many of the friction points that currently serve as essential safeguards in these processes.

Even with transparency about when and how individuals' data has been shared between governmental departments and with third parties, this is not a remedy for normalising data sharing in situations where it is neither necessary, proportionate, nor clearly limited in purpose. The existence of shortcomings in the current system should not justify a wholesale expansion of cross-departmental data sharing through a digital ID system linked by a single unique identifier.

The use of digital IDs is also set to expand within the private sector with the government announcing the upcoming launch of a 'digital wallet' scheduled for this summer. Depending on how these systems are designed, they could enable the collection of detailed data by the state on individuals' purchases such as where and when they buy alcohol or cigarettes, use gambling apps and dating sites, or access age-restricted websites. If linked to a wider digital ID system with a database, all of this information could be associated with an individual's record. This process has been described as "phone home," meaning that the digital identification system communicates with the original issuer or a proxy to verify the validity of the credential.[125] This configuration would provide the government with a record of every time you use digital ID to prove your identity, even for non-governmental services. Without protection against such measures, an individual's record in a national database could be supplemented not only with every interaction they have with public bodies, but also their credit history, transaction data, and browsing history.

The 'BritCard' proposal includes a recommendation to link the digital ID system to biometric data, which is considered to be among the most sensitive types of personal data under the UK GDPR.[126] If biometric data is linked to facial recognition systems, it could be used as a population-wide policing database, as has already been happening with the passport and DVLA databases.[127]

---

124 The Guardian, "'Woeful' DfE blamed as betting firms gain access to children's data,' 6 November 2022, https://www.theguardian.com/education/2022/nov/06/woeful-dfe-blamed-as-betting-firms-gain-access-to-childrens-data.

125 Timothy Ruff, 'Phone Home is Bad. Really Bad,' 2 June 2025, https://rufftimo.medium.com/phone-home-is-bad-really-bad-eccbbf89fc6e.

126 Labour Together, 'BritCard: A Progressive Digital Identity for Britain,' June 2025, https://www.labourtogether.uk/all-reports/britcard, p23.

127 Liberty Investigates, 'Hundreds of Thousands of Innocent People on Police Databases as Forces Expand Use of Facial Recognition Tech,' 25 September 2023, https://libertyinvestigates.org.uk/articles/hundreds-of-thousands-of-innocent-people-on-police-databases-as-forces-expand-use-of-facial-recognition-tech/.

A detailed dossier

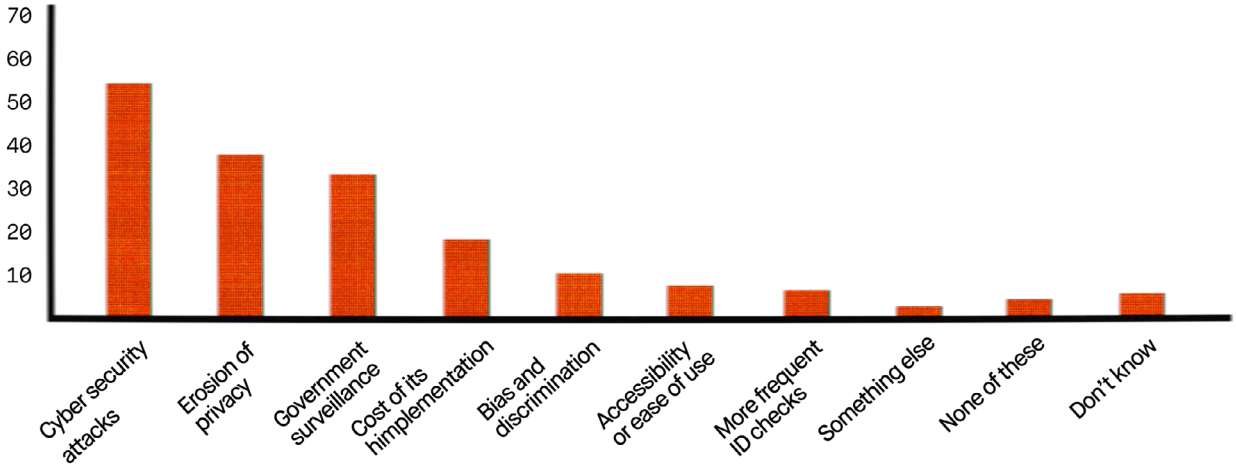
Especially worrying is that this collection of deeply sensitive, private and wide-ranging personal data could become part of "an enduring and unalterable documentary record," which the Government can search.[128] Collecting, recording, and sharing personal information engages privacy rights under Article 8 of the European Convention on Human Rights (ECHR). Public authorities may only interfere with these rights when it is in accordance with the law, there is a legal basis, and it is necessary and proportionate. The presumption must rest in favour of protecting these rights.

The 'BritCard' proposal recommends that the Government "avoid creating a new centralised database created bringing together all of the information relating to each citizen," [sic] however the collection, monitoring and profiling of citizens can still occur without one centralised database.[129] Data privacy expert Roger Clarke explains that provided there are several purpose-specific databases that are connected and the data is identified consistently (i.e., through a digital ID), a single centralised database "is no longer a precondition of the dossier society."[130] In other words, as long as the digital ID has a unique identifier that allows the linkage of separate databases, it is largely irrelevant whether there is a centralised or decentralised database. If a national ID system allows for separate databases linked by a unique identifier, it is centralised in all but name.

Although some proposals pay lip service to the importance of 'user control over data' the calls for a mandatory, universal system with record logs and unique identifiers are antithetical to these commitments. Additionally, if most of the population consents to the data being shared, others cannot avoid it. Even if you do not consent to your data being used, you will 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 their 'student identification numbers,' your child may also be subject to intervention measures despite not consenting to data sharing themself.

128 David Lyon, Identifying Citizens: ID Cards as Surveillance (Themes for the 21st Century) (2009) Polity Press, p10.
129 Labour Together, 'BritCard: A Progressive Digital Identity for Britain,' June 2025, https://www.labourtogether.uk/all-reports/britcard, p27.
130 Roger Clarke, 'Information Technology and Dataveillance,' Commun. ACM 31,5 (1988) 498-512, https://www.rogerclarke.com/DV/CACM88.html.

Which of the following, if any, would you be most concerned about if the government introduced a mandatory digital ID? Please select up to two



All figures, unless otherwise stated, are from YouGov Plc. The total sample size was 2,153 adults. Fieldwork was undertaken between 20-21 August 2025. The survey was carried out online. The figures have been weighted and are representative of all GB adults (aged 18+).

Surveillance, monitoring, and profiling

Mass surveillance involves indiscriminate, population-wide surveillance to identify targets for even more intrusive interventions. Data-driven mass surveillance relies on amassing vast quantities of data, which is mined using algorithms to sort, predict and profile populations. In constructing population-wide databases, digital ID systems are particularly well-suited to mass surveillance. Our commissioned polling shows that concerns about privacy and mass surveillance are among the most prominent concerns associated with digital ID.

Predictive analytics and profiling

The use of predictive algorithms is already expanding across government agencies, often without clear transparency or oversight. With the introduction of digital ID systems, even more personal data would be pulled into these systems, potentially enabling what amounts to digital fishing expeditions, where the private lives of individuals are laid bare for data mining by the state.

However, more data does not automatically lead to better decisions. Much of this data is used out of context, and the systems that process it often operate as "black boxes," meaning their internal logic is opaque, even to those deploying them. The use of decontextualised data can also reinforce existing biases and stereotypes.

In Britain, we have a principle that individuals should not be subject to surveillance without suspicion. The application of AI to digital ID-linked population-wide databases would turn this principle on its head, undermining the presumption of innocence, by treating everyone as a suspect by default. Individuals may be flagged where they have qualities which match the profiles of known offenders even if they do not arouse suspicion themselves. Certain groups might meet risk profiles on the basis of generalised suspicion. This is a significant shift, subjecting vast swathes of the population to surveillance in an effort to pre-empt and risk manage threat, rather than monitoring suspicious individuals based on specific behaviour.

These types of expansive, all-encompassing datasets operate on the assumption that having access to all of this information will improve services, cut costs, pre-empt harm and reduce risk, but the by-product is that the state "becomes increasingly aware of the profile of the citizen."[131] In this context, this profile is not considered on an individual basis but amalgamated to draw out broad trends or make consequential decisions without individual input. [132]

Function creep

Although they might be intended for narrow and specific purposes, digital identification systems are prone to expansion. This is particularly true of systems designed to pre-empt harm, disorder, or crime, which often operate under the assumption that it is necessary to acquire as much data as possible. The ID card introduced by the government during the Second World War was initially designed for a limited set of purposes, namely rationing, conscription and national security. However, by 1950 a parliamentary committee found that it had expanded to 38 different functions.[133] Equally, National Insurance Numbers were initially only designed to facilitate sickness and unemployment benefits, but are now used in tax and 'Right to Work' checks.[134] Although the BritCard proposal is aimed at tackling unauthorised immigration, it is not difficult to see how it could be expanded for other purposes -- indeed, this seems to be the point.

131 John Taylor , Miriam Lips & Joe Organ (2007) Information-Intensive Government and the Layering and Sorting of Citizenship, Public Money & Management, 27:2, p164, http://dx.doi.org/10.1111/j.1467-9302.2007.00573.x.

132 The German Marshall Fund of the United States, 'Addressing the Harmful Effects of Predictive Analytics Technologies,' 19 November 2020, https://www.gmfus.org/news/addressing-harmful-effects-predictive-analytics-technologies.

133 RUSI, 'UK grapples with the complex issue of national ID cards,' 16 November 2007, https://www.rusi.org/publication/uk-grapples-complex-issue-national-id-cards-1.

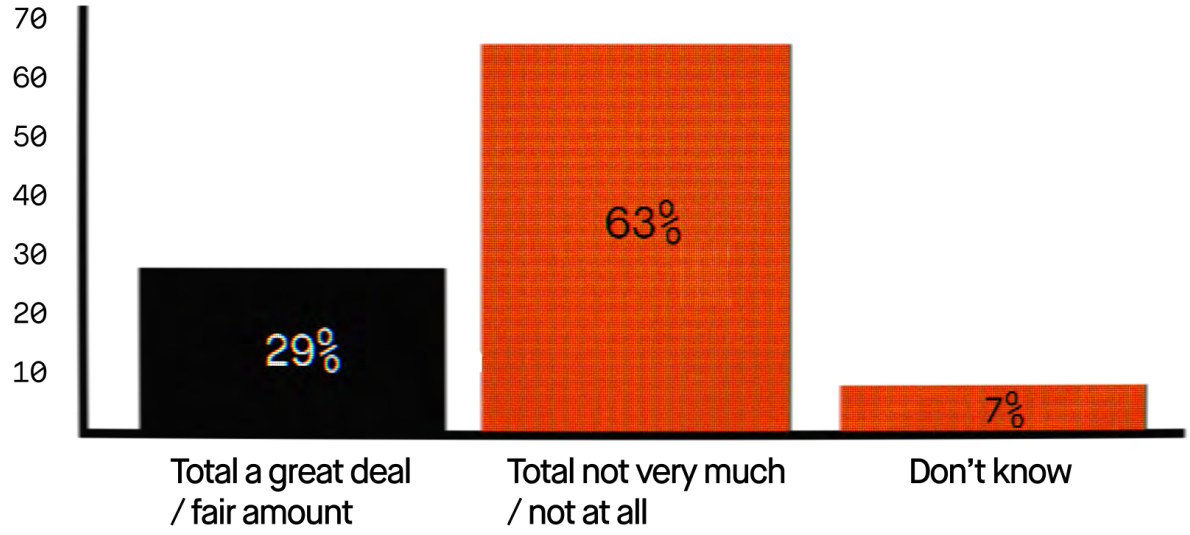
134 The New Arab, 'Introducing Mandatory ID cards will threaten the civil liberties of minorities in the UK,' 24 November 2022, https://www.newarab.com/opinion/id-cards-will-threaten-minorities-civil-liberties-uk.

Security

There are serious concerns about the security of digital ID systems. Centralised identity systems that are capable of uniquely identifying an individual and troves of deeply personal data are particularly valuable to hackers. The UK's existing digital identification system, One Login – which underpins the credential issuing process in the 'BritCard' proposal' – reportedly suffers from substantial cybersecurity and data protection weaknesses.[135]

The UK government does not have an enviable track record when it comes to data breaches. The original ID scheme introduced by the last Labour government suffered a major loss of public trust after a data breach in October 2007. In that instance, a HMRC civil servant sent a copy of the child benefit database to the National Audit Office with a weak password; however, it never reached its intended destination.[136] As polling data below show, the public have noticed the government's history of breaches and does not trust the government to keep digital ID data secure.

Generally speaking, to what extent, if at all, would you trust that your digital security related to digital ID would be protected?



All figures, unless otherwise stated, are from YouGov Plc. The total sample size was 2,153 adults. Fieldwork was undertaken between 20-21 August 2025. The survey was carried out online. The figures have been weighted and are representative of all GB adults (aged 18+).

135 Computer Weekly, 'Security test reveal serious vulnerability in Government's One Login digital ID system,' 16 May 2025, https://www.computerweekly.com/news/366623991/Security-tests-reveal-serious-vulnerability-in-governments-One-Login-digital-ID-system.

136 Edgar A. Whitley, Aaron K. Martin and Gus Hosein, 'From surveillance-by-design to privacy-by-design: Evolving identity policy in the United Kingdom,' p211.

In April 2025, the Legal Aid Agency was the target of a cyberattack that resulted in hundreds of thousands of legal aid applicants stretching back to 2010 having their personal data – including contact details, dates of birth, criminal history, employment status and financial information – accessed and downloaded.[137] The hack was believed to have originated from a criminal gang, which a legal expert noted "could make any individual subject to blackmail threats."[138]

The British government also has a track record of concealing data breaches, further undermining public trust in the security of official databases. In February 2022, the personal data of approximately 19,000 Afghan nationals applying for relocation to the UK was leaked. This included the names and contact details of individuals who had assisted UK forces during the occupation of Afghanistan, as well as information relating to MI6 and SAS personnel.[139] The Ministry of Defence was granted a super injunction, which meant that the breach could not be reported on or scrutinised.[140] Similar data breaches and cover-ups in the context of a digital ID system would destroy public trust.

The large volumes of information recorded by digital ID systems also make them attractive to foreign adversaries and malign actors. In 2022, the digital identification and signature service BankID, which Norwegians use to access online banking, private services and public services, was reportedly hacked by a Russian group.[141]

Where states are inevitably targeted by these attacks, individuals can lose access to vital services. In 2017, 760,000 Estonians lost access to their identity cards when security researchers detected a security flaw that could allow hackers to decode personal data and impersonate cardholders.[142] In April 2025, a cyberattack on Poland's centralised state registry disrupted access to government online tax services and the mObywatel digital identity app.[143]

Data breaches and the associated loss of sensitive personal information also

137 The Guardian, Legal aid hack: data from hundreds of thousands of people accessed, says MoJ, 19 May 2025, https://www.theguardian.com/law/2025/may/19/significant-amount-of-personal-data-accessed-in-legal-aid-agency-data-breach-says-moj.
138 The Guardian, Legal aid hack: data from hundreds of thousands of people accessed, says MoJ, 19 May 2025, https://www.theguardian.com/law/2025/may/19/significant-amount-of-personal-data-accessed-in-legal-aid-agency-data-breach-says-moj.
139 The Standard, 'What is the Afghan Data Breach: Everything You Need to Know,' 16 July 2025, https://www.standard.co.uk/news/world/afghan-data-breach-resettlement-scheme-b1238396.html
140 BBC, 'Security Committee launches inquiry into Afghan data leak,' 21 July 2025, https://www.bbc.co.uk/news/articles/c0k70de6jpgo
141 Freja, 'Norwegian Bank ID under attack by Russian Hackers,' 7 July 2022, https://frejaeid.com/en/norwegian-bankid-under-attack-by-russian-hackers/.
142 BBC, 'Security flaw forces Estonia ID 'lockdown',' 3 November 2017, https://www.bbc.co.uk/news/technology-41858583.
143 The Record, 'Poland's State Registry temporarily blocked by cyber incident,' 1 May 2025, https://therecord.media/poland-pesel-system-state-registry-cyber-incident.

heighten the risk of identity theft. A breach of the Indian digital ID system reportedly resulted in personal information, including names, home addresses, email addresses, phone numbers and photographs, being made available for purchase online for only £6.[144]

Lack of choice in mandatory systems

The proposals put forward by several Labour-aligned think tanks propose a mandatory, universal form of digital ID. However, digital ID checks should never become a prerequisite for accessing public services. There should always be an offline alternative for those who are not able or do not wish to share their information digitally, 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 explains 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."[145] Therefore any implementation of digital IDs must also come with a legal right to use non-digital methods of identification.

Inaccuracies and exclusion

Where digital IDs are mandatory and they become the essential barrier through which services can be accessed, their failure becomes all the more catastrophic. Individuals who either have to prove they are not who the system says they are, or are who they claim to be, will face considerable difficulty in establishing their identity.[146] Charities have reported on the widespread inaccuracies of migrants' nationalities under the UK's eVisa digital ID scheme, which led to authorised migrants being stranded at an international airport when their eVisas failed.[147]

Digital identification systems are inherently exclusionary: they are designed to

144 The Guardian, 'Personal data of a billion Indians for £6 a report claims,' 4 January 2018, https://www.theguardian.com/world/2018/jan/04/india-national-id-database-data-leak-bought-online-aadhaar.

145 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-and-overlooked-report.pdf, p2.

146 Sullivan, Clare Linda, Digital Citizenship and the Right to Identity in Australia (2013) Federal Law Review, Vol. 41, p. 557, 2013, https://ssrn.com/abstract=2379240, p569.

147 The3Million, 'Widespread Identity Document Errors on Digital Status (Evisa) Accounts, 6 March 2025, https://the3million.org.uk/news/2025-03-06/widespread-identity-document-errors-digital-status-evisa-accounts; The Independent, 'Ukrainian grandmother, 78, stranded for two days after being refused flight to the UK over eVisa issues,' 7 July 2025, https://www.independent.co.uk/news/uk/home-news/uk-evisa-digital-ryanair-flight-ukrainian-grandmother-b2783731.html.

identify who is entitled to services and who is not. When this goes wrong people can be disqualified from accessing essential services to which they would otherwise be entitled. 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.[148] 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.[149] These problems would undoubtedly replicate in a population-wide digital ID system.

Abuses of power

Unauthorised access to data held on digital ID systems

When ID cards were mandatory during the 1950s, police officers were reported to abuse their powers by arbitrarily demanding people produce ID cards, and rounding up and questioning girls in East London who were unable to prove their identity.[150] More recently, there is evidence of police overreach through unauthorised access to the Police National Computer.[151] A digital ID system could be subject to the same abuse, but with even graver consequences given the detailed personal information that could be collected. This was the case in Belgium, where the data protection regulator received 100 complaints about civil servants who were accused of accessing the state register without justification. [152]

Although proposals for an 'audit trail' to show users what data has been accessed by government agencies are one possible measure for improving transparency, the enabling legislation or policies governing such databases could themselves be highly permissive and therefore open to abuse.[153] For example, the Identity Cards

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

149 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.

150 Mark Egan, 'Harry Willcock: The Forgotten Champion of Liberalism,' Journal of Liberal Democrat History, 17: Winter, 1997-1998, https://www.liberalhistory.org.uk/wp-content/uploads/2014/10/17_egan_harry_willcock.pdf.

151 Metropolitan Police, Police Staff Illegally Accessing the PNC from 2013 to 2023, Ref: 01.FOI.23.034574, https://www.met.police.uk/foi-ai/metropolitan-police/disclosure-2024/january-2024/police-staff-illegally-accessing-pnc-2013-2023/

152 Vrt News, 'Are Belgian's Civil Servants nosy parkers?' 2 May 2015, https://www.vrt.be/vrtnws/en/2015/05/02/are_belgium_s_civilservantsnosyparkers-1-2324999/.

153 Labour Together, 'BritCard: A Progressive Digital Identity for Britain,' June 2025, https://

Bill 2006 defined a statutory purpose of the scheme as being necessary in the public interest.[154] However, this public interest test was defined broadly to include "efficient and effective provision of public services," which could have been very broadly interpreted to justify wide-ranging access. Moreover, transparency about what has been accessed does not prevent abuse or amount to individuals being in control of their data. In Estonia, a police officer was fined for checking his fiancée's criminal record and a medic was fined for checking why an ambulance had been dispatched to a particular address.[155]

Policing dissent

Having the infrastructure to monitor and surveil the data of millions of individuals in real-time would equip the government with the tools to suppress and censor political dissent with ease. Although the British public may not believe that such concerns currently apply to the UK, modern history has shown that the erosion of human rights and indeed democracy can take hold suddenly. If a universal digital ID system is implemented, it would be nearly impossible to reverse, and any future government would have access to the vast amounts of personal data collected, and the ability to enforce an even more stringent checkpoint society than may have been intended.

It is widely documented that governments can use digital ID as a tool to police dissent. In Egypt, for example, dissidents have been denied identity documents. Privacy activist Srinivas Kodali warned that the Indian ID card system makes dissent difficult as any data linked under the scheme is relayed to the ministry of home affairs, the police and surveillance agencies.[156] The government authority that administers the Indian ID card scheme admitted that the Bharatiya Janata Party illegally accessed the data of 78 million people for the purpose of profiling, and the states of Andhra Pradesh and Telangana deleted 5.5 million voters from electoral rolls after their ID numbers and voter identities were prematurely linked.[157]

Elsewhere, identity cards have been used to deny specific sub-groups of their human rights. For example, the authorities in Myanmar denied the Rohingya recognition as Bangladeshi citizens on their ID cards, and authorities in both

---

www.labourtogether.uk/all-reports/britcard, p27.

154 HL Deb, Identity Cards Bill, 31 October 2005, https://publications.parliament.uk/pa/ld200506/ldhansrd/vo051031/text/51031-04.htm#51031-04_head3, col 13.

155 eEstonia, 'I spy with my little eye...privacy!' 19 August 2020, https://e-estonia.com/i-spy-with-my-little-eyeprivacy/.

156 Context, Surveillance Nation: India spies on the world's largest population, 20 March 2023, https://www.context.news/surveillance/surveillance-nation-india-spies-on-worlds-largest-population.

157 Article 14, 'Govt has cleared linking of Aadhaar & voter data. Past experience reveals how it can be manipulated,' 27 December 2021, https://article-14.com/post/govt-has-cleared-linking-of-aadhaar-voter-data-past-experience-reveals-how-it-can-be-manipulated-61c937a621c09.

Egypt and Indonesia required religious minorities to renounce their faith in order to obtain an ID card.[158][159] In Iraq, individuals were denied identity documents due to perceived family links to ISIS suspects as a form of collective punishment.[160] In Venezuela, some fear that the smart ID card system, which collects personal information about individuals' family, employment, income, property, medical history, welfare benefits, social media presence, political affiliation, and whether a person voted is being misused to identify supporters and opponents of the government.[161]

The ability to collate vast volumes of data and sort through it to identify certain groups of people means that digital ID systems can also be used to target and exclude minorities. In the United States, the Department of Government Efficiency (DOGE) has been attempting to amalgamate disparate datasets into a centralised Department of Homeland Security database that officials can search and use to track and surveil immigrants almost in real time.[162]

Changes the relationship between the population and the state

'Papers, Please' Society

Digital identification systems can create irreversible changes to the relationship between the individual and the state. Digital ID systems normalise people having to produce documents on demand to access everyday services, such as medical appointments, welfare, employment, banking and renting. In 1996, Privacy International conducted interviews with ID cardholders from around the world. An Argentinian ID cardholder noted that the card:

> *"was required for any sort of proceedings that the person wanted to initiate, e.g., enrol at school, buy a car, get his driving license, get married. Nobody could do anything without it."*[163]

158 Al Jazeera, 'Genocide Card: Myanmar Rohingya verification scheme condemned,' 3 September 2019, https://www.aljazeera.com/news/2019/9/3/genocide-card-myanmar-rohingya-verification-scheme-condemned.

159 Human Rights Watch, Egypt: Allow citizens to list actual religion on ID cards, 11 November 2007, https://www.hrw.org/news/2007/11/11/egypt-allow-citizens-list-actual-religion-id-cards; Human Rights Watch, Indonesia's Ahmadiyah push back against discriminatory laws, 23 June 2017, https://www.hrw.org/news/2017/06/23/indonesias-ahmadiyah-push-back-against-discriminatory-laws

160 Human Rights Watch, Iraq: Families of alleged ISIS Members denied IDs, 25 February 2018, https://www.hrw.org/news/2018/02/25/iraq-families-alleged-isis-members-denied-ids.

161 Reuters, 'How ZTE helps Venezuela create Chinese-style social control,' 14 November 2018, https://www.reuters.com/investigates/special-report/venezuela-zte/.

162 Wired, DOGE is building a master database to surveil and track immigrants, 18 April 2025, https://www.wired.com/story/doge-collecting-immigrant-data-surveil-track/

163 Privacy International, 'Some Personal Views from around the World on ID Cards,' 21 July 1996, https://privacyinternational.org/blog/1380/some-personal-views-around-world-id-cards

Under the common law tradition in the UK, we abide by the principle that we are able to conduct ourselves freely, so long as we do not infringe upon the freedoms of another – at which point the law may intervene. Digital ID systems, however, risk replacing these inherent freedoms with a regime of permissions, in which access to entitlements and public services is no longer assumed but must be repeatedly granted.

Digital ID systems can also weaken social cohesion by fostering a culture of suspicion, in which individuals are presumed to be untrustworthy unless verified by state-issued identification. This dynamic discourages mutual trust among citizens while centralising state power. The original 'No2ID campaign' was waged as a "war with a Whitehall culture of mass supervision that demands we be forbidden from trusting one another but must trust official databases absolutely."[164] By inserting itself into our private interactions and amassing vast amounts of information about us in the process, the state would tip the balance of power away from individuals and towards itself.

Surrendering data privacy

Proponents of digital ID argue that we have become so accustomed to giving up our personal information to private companies that surrendering data should no longer be of concern. Movements to regain control of data would indicate otherwise.[165] But perhaps more pertinently, the danger of the state having joined-up continuous information about us brings new and unexpected challenges. When we give up our personal data to companies, we do so voluntarily in exchange for a specific commercial service; however, the government, in contrast, is asking us to give up our personal data to exercise our rights.

In the context of private companies, the offer of more detailed insights and personalisation enhances their ability to sell us products and services. However, this hyper-granular personalisation also gives companies unprecedented access to our private lives and allows them to predict, shape and nudge our decision-making.[166] If the government conducts data profiling and analytics, we may see some benefit in the form of more tailored public services, but such processes would also have consequences for the population at large in terms of resource allocation, and on the individual level in terms of targeted interventions. It could determine where public funding goes, which communities and individuals are targeted for state intervention, and which neighbourhoods are observed, surveilled and investigated.

164 The Guardian, 'Cameron will scale back database state,' 13 May 2010, https://www.theguardian.com/commentisfree/2010/may/13/id-cards-database-cameron-clegg

165 BBC, 'Facebook to stop targeting ads at UK woman after legal fight,' 22 March 2025, https://www.bbc.co.uk/news/articles/c1en1yjv4dpo.

166 See for example, Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019.

CONCLUSION

CONCLUSION

A mandatory, universal digital ID would undermine the fundamental rights of the UK population – it must be rejected.

Such proposals are antithetical to the tradition in liberal democracies that the citizen holds the government to account, rather than the government holding the citizen to account.

This report has interrogated the claims that digital ID would tackle unauthorised immigration, scrutinised the other proposed use cases, and set out the dangers to civil liberties, privacy and other fundamental human rights.

Digital IDs are proposed as a silver bullet solution with a multitude of promised but unevidenced benefits. As we have demonstrated, universal mandatory digital ID is unlikely to tackle unauthorised immigration. It would however, increase the burdens on law-abiding citizens and push unauthorised immigrants towards unsafe housing and exploitative work. Ultimately, it remains grossly disproportionate to infringe on the civil liberties of over 60 million people in the UK in an attempt to tighten restrictions on a few hundred thousand, particularly when there are simpler means of doing so.

A digital ID system designed with a single unique identifier that records every interaction with public services and private companies risks creating an Orwellian database state, in which our sensitive data can be mined for insights. The calls for AI-enhanced digital ID that permits expansive profiling, surveillance and tracking in order to pre-empt behaviour and justify interventions, undermine democratic norms and fundamental rights. Rather than empowering the citizen, at best, these types of digital ID systems help the state to administer itself.

The promise of 'joined up' government, where data flows across Whitehall departments in the name of improving the efficiency of public services, poses a serious threat to data rights. When personal information is liberally repurposed across agencies – as envisioned in the proposals put forward by proponents of digital ID – individuals lose control over how their data is used, often in ways they never anticipated.

A mandatory digital ID system would force individuals to surrender their privacy rights in order to engage with the state. There are thousands of people who are not able or do not want to use digital ID systems to prove their identities. It will never be possible to get everyone online and the effects of digital exclusion are often

more sharply experienced among marginalised groups, including those living in poverty, disabled people and older people.

The capacity to link such vast quantities of highly personal information under a digital ID system makes it a honeypot for hackers, creating a huge vulnerability for catastrophic data breaches. Big Brother Watch's independent polling on digital ID conducted by YouGOV highlights the serious concerns that the public has about the government's ability to securely hold the population's personal data, as well as the erosion of privacy and government surveillance.

The proposals being considered by the government would normalise frequent ID checks each time we interact with public services. We know what it is like to be subject to identity checks when travelling outside of the country. A universal, mandatory digital ID system threatens to replicate these borders inside of the country, turning us into 'Checkpoint Britain,' where we have to continually prove our identities to go about our daily lives.

Mandatory digital ID already exists for over four million legal migrants to the UK, who are required to use an eVisa. The well-documented problems with eVisa's accuracy – which have left people stranded at airports and unable to access GP services – highlight the reality of what happens when these systems go wrong and how they often hinder, not help, bureaucratic interactions.

Before embarking on yet another ill-fated path towards universal, mandatory ID, the government should reflect on the British public's repeated rejection of such schemes over the past century.

If the Labour government is committed to its promise to "tread more lightly on [our] lives,"[167] it should reject plans for an all-encompassing digital ID system that grants itself sweeping access to our private lives with the promise to monitor, manage and predict them.

167 Gov.uk, Speech, Kier Starmer's first speech as Prime Minister, 5 July 2024, https://www.gov.uk/government/speeches/keir-starmers-first-speech-as-prime-minister-5-july-2024.

BIG BROTHER WATCH

Defending Civil Liberties, Protecting Privacy