

BIG BROTHER WATCH

**Submission to the Cabinet
Office's consultation on
draft legislation to support
identity verification**

February 2023

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 technological 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

Silkie Carlo

Director

Direct line: 020 8075 8478

Email: silkie.carlo@bigbrotherwatch.org.uk

Susannah Copson

Legal and Policy Officer

Direct line: 020 8075 8480

Email: susannah.copson@bigbrotherwatch.org.uk

INTRODUCTION

1. We welcome the opportunity to respond to the consultation on draft legislation to support digital identity verification services.

2. Digital identity verification is the process of remotely confirming someone's personal data against a trusted dataset (e.g. government records). This is important in the digital age, where many activities that require identification increasingly take place online – such as filing tax returns, online banking, and dealing with legal documents – and people expect a quick and efficient service.

3. The proposed data-sharing legislation specifically enables a new government identity verification system known as GOV.UK One Login, for citizens to prove who they are online when accessing government services. This is aimed at “inclusive digital transformation”¹ – i.e. to encourage more people to access government services online. It also aims to prevent fraud and promote service efficiency by streamlining the government identity verification process. According to the Cabinet Office's press release, the system would replace more than 190 existing sign-in routes and 44 separate accounts.²

4. Separately, the Government is legislating to create a system of regulated digital identity verification in the private sector, via Part 2 of the Data Protection and Digital Information Bill. This would establish a regulatory framework for digital identity verification services in the UK and allow public authorities to disclose personal information to “trusted” digital verification services for the purpose of identity verification.³

5. It is important that digital identity systems are always optional for inclusion, accessibility, user empowerment and privacy. The growth in digital identity systems and services should not mean that offline government services that require identity verification are made any more difficult to access and use.

6. That said, millions of people use online services that require digital identification. It is important that when people opt to use digital identity and verification services,

1 Consultation on draft legislation to support identity verification – Cabinet Office, 4th January 2023: <https://www.gov.uk/government/consultations/draft-legislation-to-help-more-people-prove-their-identity-online/consultation-on-draft-legislation-to-support-identity-verification>

2 Cabinet Office launches consultation on departmental data sharing – Cabinet Office, 4th January 2023: <https://www.gov.uk/government/news/cabinet-office-launches-consultation-on-departmental-data-sharing>

3 Data Protection and Digital Information Bill 2022: <https://publications.parliament.uk/pa/bills/cbill/58-03/0143/220143.pdf>

those services are built to prioritise privacy, security and user trust. There is a vast amount of data that risks misuse if not properly protected.

7. As such, Big Brother Watch would welcome legislation that protects the public's privacy, security and ability to choose when it comes to digital identity and verification. However, the Government's proposal and four-paragraph long draft regulations do not currently provide the appropriate safeguards for a government identity verification system at all. Rather, it appears that under the broad mandate of identity verification, a giant, centralised database and data-sharing system of population-level identity information is being constructed with next to no limitations on its use. This has strong echoes of the identity scheme that was resolutely rejected in the 2000s, that the Conservative government stood on a mandate to dismantle. The SI is a totally inappropriate enabling instrument in one of the most sensitive areas of public administration and individual privacy.

8. Big Brother Watch strongly believes that the draft regulations should be withdrawn and the government should resume the consultation process.

PRIVACY AND DATA PROTECTION

9. The proposed legislation provides the legal basis to share identity documents or verifiers. Recording a person's identity information, email and two-factor authentication method creates a record of identifying information for the population; essentially facilitating an identity database.

10. Any such system should have strict rules defining the purpose of data sharing. In its current state, the legislation is too brief to provide anywhere near the appropriate level of detail required for this, and permits apparently open-ended data sharing for the purpose of creating "a reusable digital identity in a convenient, secure and efficient way" and "improving [...] mental health, emotional or economic well-being".⁴ **We are concerned and confused, as are other expert groups, on the inclusion of emotional and mental health and believe this should be removed.** The broad scope of data sharing permissions leaves the sharing of people's personal data effectively unregulated.

11. It is crucial that any digital identity legislation provides specific limitations on the purposes and substance of data sharing. Guarding against function creep is vital, particularly in the context of sensitive personal data. This is key towards protecting privacy rights and preserving public trust in digital identity verification systems.

⁴ (Draft) The Digital Government (Disclosure of Information) (Identity Verification Services) Regulations 2023: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1127290/Draft_Digital_Government_Disclosure_of_Information_Identity_Verification_Services_Regulations_2023_.pdf

Providing safeguards and justifications for the public authorities set to be providers and recipients is a key step towards achieving this. **Limitations should reflect data protection principles, agreed-on identity principles (e.g. the 9 Identity Assurance Principles⁵ developed by the Privacy and Consumer Advisory Group), and should protect and promote the right to privacy protected by the Human Rights Act 1998.**

12. The consultation document states that a user's name, date of birth, home address, email address, photographs (which are increasingly converted into biometric data), "various identifiers" such as passport number or driving license number, transactional data such as income, and other fields of data may be shared. This is an extensive list that indicates governmental data sharing on a scale not seen before. It could fundamentally alter the relationship between the individual and the state. Further, the document states that "other data items may be processed as identity verification services develop". The proposed system is vast and entirely open-ended. Without further safeguards, and with its emphasis on "convenience" over privacy, it is likely that this would become a gateway for individuals to access government services via a facial biometric, for example – a more advanced, vastly more intrusive version of the mass ID card proposal.

13. While the consultation document claims that all public authorities party to the data-sharing will ensure appropriate data storage and protection protocols, this is not reflected in the draft regulations - there is currently no detail of the measures that will be put in place to achieve this.

14. More information is needed on whether data uploaded under the proposed legislation can be shared with third parties as part of private-public sector partnerships, whether now or in the future.

DIGITAL IDENTITIES

15. While cognisant that the digital identity verification service outlined in this draft legislation is not a digital ID in and of itself, it is the necessary precursor towards widespread digital ID implementation. Introducing digital verification services therefore raises key concerns around the increasing trend towards online identities and casual use of biometric checks.

16. Digital identities create a unique identifier for each user, designed to help governments join up personal information currently held in databases across different departments. Such identifiers can have administrative benefits, but can also be used in

⁵ Identity Assurance Principles, 2015: <https://www.gov.uk/government/publications/govuk-verify-identity-assurance-principles/identity-assurance-principles>

ways that are uniquely harmful to privacy, equality and civil liberties. At their worst, digital IDs can be misused to perform widespread population surveillance⁶, implement curbs on individuals' liberties, predict and shape individuals' decisions⁷, and aid in the tracking, persecution or other differential treatment of ethnic, religious and other marginalised groups.⁸

17. Clause 3(2)(a) outlines the draft legislation's purpose to "create a reusable digital identity", as data will be shareable between a large number of government departments.⁹ It seems impossible to separate the purpose of this instrument from its potential impact and use; supporting the increased use of digital identities and normalising the sharing of personal - often biometric - data across government. Given this potential, it is crucial that a full impact assessment, as well as a data protection impact assessment, is produced and published.

INCLUSION AND EXCLUSION

18. Identity checks have become a prerequisite for many key life tasks, such as starting employment or renting property. It is vital that services are never contingent on a digital identity check, as this could prevent people from participating in key activities. There should always be an offline alternative for those who do not wish to share their information digitally, so that participation is not coercive and to uphold equal access opportunities. **In creating a digital identity regulatory system, the government should also legislatively safeguard individuals' rights to offline alternatives to digital verification processes.**

19. Some people in marginalised, vulnerable and minority groups are more likely to have reduced access to online services (e.g. people with disabilities, low income, low digital literacy levels or limited internet access), particularly where digital identity is a requirement (e.g. migrants, and people in Gypsy, Roma and Traveller communities). Charities have explained how they currently dedicate a large portion of their time helping vulnerable users access government online services.¹⁰ Having an online

6 China's Surveillance State Should Scare Everyone, The Atlantic, January 2018. Last accessed 14th February 2023: <https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/>

7 The Facebook and Cambridge Analytica scandal, explained with a simple diagram, Vox, May 2018. Last accessed 14th February 2023: <https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram>

8 How some countries are using digital ID to exclude vulnerable people around the world, The Conversation, August 2021. Last Accessed 14th February 2023: <https://theconversation.com/how-some-countries-are-using-digital-id-to-exclude-vulnerable-people-around-the-world-164879>

9 (Draft) The Digital Government (Disclosure of Information) (Identity Verification Services) Regulations 2023, Regulation 4(2)(a): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1127290/Draft_Digital_Government_Disclosure_of_Information_Identity_Verification_Services_Regulations_2023.pdf

10 Digital Identity: Call for Evidence Response. September 2020: <https://www.gov.uk/government/consultations/digital-identity/outcome/digital-identity-call-for-evidence-response>

verification process as the promoted method of identity checking will exacerbate this burden.

20. The Public Sector Equality Duty assessment considers the impact of digital identity verification on individuals with protected characteristics.¹¹ While the consideration of human rights through the lens of inclusivity is welcome, the assessment adopts a strictly positivist approach and does not acknowledge the exclusion that digital verification systems give rise to. It is crucial for the government to consider and address the potential negative impacts of GOV.UK One Login before its implementation.

RECOMMENDATION

Big Brother Watch strongly believes that the draft regulations should be withdrawn and the government should resume the consultation process.

¹¹ Impact assessment of the draft data sharing legislation on people with protected characteristics. 4 January 2023. Last accessed 17 February 2023: <https://www.gov.uk/government/consultations/draft-legislation-to-help-more-people-prove-their-identity-online/impact-assessment-of-the-draft-data-sharing-legislation-on-people-with-protected-characteristics>