13 SEPTEMBER 2019 TECHNOLOGY AND PUBLIC POLICY

Response to DCMS-GDS Call for Evidence on Digital Identity

TONY BLAIR INSTITUTE FOR GLOBAL CHANGE

Contents

About the Tony Blair Institute for Global Change

1. The Tony Blair Institute for Global Change works to equip political leaders and governments to build open, inclusive and prosperous societies in an interconnected world. We do this by shaping the policy debate with bold ideas and practical reforms as well as advising reforming global leaders on strategy and delivery.

Summary

2. We are encouraged by the government's efforts to simplify identity verification for businesses, citizens and the public sector alike. As this call for evidence notes, digital identity in the UK has not kept pace with the speed and standards of the internet era. In many cases, this was due to legitimate concerns from citizens about security or from government departments about usability. However, the crucial lesson must be that new technologies which enhance privacy and security can mitigate many worries of old. With both digital public services and trends in regulation highlighting the growing need for electronic identity verification, it is right to move the debate forward.

3. In every country that is serious about modernising government, electronic identity is often the foundational component in a suite of digital infrastructure that enables innovation both

inside government and across society. Indeed, the UK's failure to implement a fit-for-purpose identity system has been a major constraint on the much-needed, radical transformation of government and public services – both in terms of improving front-end user experiences and simplifying back-end processes. Though GDS's work on 'Government as a Platform' has lost some momentum of late, we nevertheless link the identity opportunity to this work to highlight the enabling potential for organisations across both government and society.[1]

4. Finally, we acknowledge that a new identity system will require some public investment. It is not feasible to provide a robust cost estimate as part of this response. However, it is worth considering the context in which this spending would be made. According to a March 2019 report by the National Audit Office, GOV.UK Verify – which uses external providers who already hold identifying information about individuals to verify identities – and its predecessor have already cost at least £154 million, not including costs incurred by departments to reconfigure their processes to use it.[2] This investment was set against a backdrop of expected benefits originally totalling £873 million, but which have since been revised down by 75% to only £217 million due to the system's difficulties. Similarly, other programmes aimed at simplifying data collection and interactions between the citizen and state illustrate the potential opportunity. For example, the Tell Us Once (TUO) initiative, which allows people to inform the state about a birth or death only once, received a 98% satisfaction rating in a 2013 survey, and is also far more efficient for government, with TUO delivering estimated savings of £22 million ($28.5 million) annually.[3]

5. As such, if we are ever to secure these larger financial benefits, not to mention the significant economic gains of opening up this identity system for use *across* society and not *only* by government, a new approach combined with new investment is likely the only route forward. As a platform for society, and not just government, we note there is also an opportunity for a public-private funding model involving members of the ecosystem who would benefit from simple and affordable credential-checking.

Context

6. Several trends highlight the need for government to confront the identity debate head-on. Perhaps most notably, the UK continues to explore increasingly widespread applications for digital identity verification beyond accessing public services. These include age verification for accessing online pornography, tracking migrants, age-appropriate design codes for social media use, and potentially online purchases of age-restricted items such as knives,

[1] Andrew Bennett, "Transforming Government for the 21st Century: Enabling Infrastructure", Tony Blair Institute for Global Change, June 2019, https://institute.global/insight/renewing-centre/transforming-government-21st-century

[2] "Investigation into Verify", National Audit Office (NAO), March 2019, https://www.nao.org.uk/report/investigation-into-verify/

[3] "Transforming local public services: using technology and digital tools and approaches", Local Government Association, June 2014, https://www.local.gov.uk/sites/default/files/documents/transforming-public-servi-80e.pdf

alcohol or (e-)cigarettes.[4] The risk is that the government rushes to address specific use cases without setting clear standards or parameters on what digital identity should look like or how it should be implemented, and without securing public consent.

7. Globally, too, the prospect of emerging technologies – such as cryptocurrencies and digital wallets, on the one hand, or facial recognition technologies, on the other – in some way drawing on or interacting with state-backed (digital) identities, should encourage the government to consider its approach carefully.

8. GOV.UK Verify (Verify), the government's most recent iteration, was rightly designed to avoid a large central database that might confer undue power to the state and become a honeypot for cyberattacks. However, its federated approach means only a limited number of providers are involved, undermining uptake; it has been difficult for government departments to use; and the Public Accounts Committee has also highlighted how Verify has failed to meet its original performance targets or achieve value for money.[5] Though Verify should not be closed immediately, given that Universal Credit is dependent on the system (even though only 38% of claimants can successfully sign up through it), it's clear that a new approach is needed.[6] That the government has already announced an end to public funding post-2020 is further evidence of this.[7]

9. The lesson must not be to reject the trend towards decentralisation but to empower it further. As evidenced by a 2018 hack on India's Aadhaar ID system, a single centralised system is especially vulnerable to hacking.[8] GOV.UK Verify mitigates this 'honeypot' vulnerability through its federated structure but is not a perfect solution. The Science and Technology Select Committee, which has also been critical of Verify, has called for single unique identifiers, yet we must be wary of any approach that might also bring greater centralisation with it.[9] Instead, a better way forward can be found by adopting a fully secure, private and decentralised model of digital identity.

10. To that end, we are encouraged by the consultation's vision for reusable digital identities that are under the control of individuals. Given the fraught history of the identity debate in

---

[4] Rowland Manthorpe, "Sky Views: The government is quietly creating a digital ID card without us noticing" https://news.sky.com/story/sky-views-the-government-is-quietly-creating-a-digital-id-card-without-us-noticing-11726548

[5] Lesley Cowley (16:36), "How digital innovation can improve public services", Institute for Government, March 2018, https://www.instituteforgovernment.org.uk/events/how-digital-innovation-can-improve-public-services; "Government flagship digital identification system failing its users", Public Accounts Committee, May 2019, https://www.parliament.uk/business/committees/committees-a-z/commons-select/public-accounts-committee/news-parliament-2017/accessing-public-services-through-verify-report-published-17-19/

[6] "Investigation into Verify", NAO, p9.

[7] Oliver Dowden, "GOV.UK Verify programme: Written Statement – HCWS978", Cabinet Office, 9 October 2018, https://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2018-10-09/HCWS978/

[8] Rachna Khaira, Aman Sethi and Gopal Sathe, "UIDAI's Aadhaar Software Hacked, ID Database Compromised, Experts Confirm", HuffPost India, 11 September 2018, https://www.huffingtonpost.in/2018/09/11/uidai-s-aadhaar-software-hacked-id-database-compromised-experts-confirm_a_23522472/

[9] "Government's digital approach has lost momentum", Science and Technology Committee, July 2019, https://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/news-parliament-2017/digital-government-report-publication-17-19/

the UK, this is a promising starting point which lends itself towards a decentralised and user-centric model of digital identity, which we believe would both deliver the benefits of electronic identities and restore public trust. The prize – hassle-free and trusted interactions between citizens and the state – is huge, and a model based on these principles would enable precisely this while keeping personally identifiable information private, secure and under individuals' control.

A proposed model for digital identity

11. A simple, robust and comprehensive identity is vital for simplifying thousands of public-facing services and is used across Europe and beyond.[10] This new debate must also recognise that governments already hold a lot of personal data about citizens in the form of passports, driving licences or other records and registrations, but this information is fragmented across different government departments and agencies. Moreover, at present citizens have no way of knowing how or when this data is being accessed, shared or used across government. Unlocking the potential opportunity by correcting this fragmentation and promoting transparency – bringing data points together but under the control of individuals, not the state – must be the starting point for a new approach.

12. However, governments should also distinguish between the direct benefits of specific models and the indirect benefits of digital identities in general. We advocate for a decentralised, user-centric and privacy-protecting model that would directly enable data minimisation by giving individuals granular control over what is shared and for how long. In practice this means splitting information up into distinct attributes, allowing, for example, users to share a verified 'over 18' attribute rather than everything on a physical identity document.

DIRECT BENEFITS

13. The decentralised approach would also directly reduce the risk of forgery or insecure storage by leveraging modern cryptography, replacing the status quo where physical documents are routinely shared, stored, copied or transcribed in ways that take data outside users' control. A truly decentralised system – in which data is not stored in a centralised database, managed either by government or a private company, but on an individual's trusted, personal device[11] – would also reduce worries about an all-powerful state or the risk of 'honeypot' cyberattacks by obviating the need for either centralised or even federated servers that store users' data or record all requests to verify identities.

14. A decentralised, user-centric model would also enable service providers to generate unique identifiers, so that there is an option for users to be remembered by individual

[10] Ben Terrett, "Digital service delivery in the Peruvian government", 3 May 2018, https://public.digital/2018/05/03/digital-service-delivery-in-the-peruvian-government/
[11] Chris Yiu and Harvey Redgrave, "A New Approach to Digital Identity", Tony Blair Institute for Global Change, 29 March 2018, https://institute.global/insight/renewing-centre/new-approach-digital-identity

organisations but not matched across them. This does not preclude data-sharing across services, such as medical data across medical clinics and hospitals, but ensures that users would have to consent beforehand.

15. Our focus is on delivering on these principles, rather than prescribing any one specific architecture. However, whichever system is adopted should reflect the distributed nature of identity. For example, in a decentralised and user-centric model where no single server stores every data point, characteristics of an individual or organisation's identity would be disaggregated from one another. As patient records, degree certificates, passports, driving licences or criminal record certifications are all issued by different agencies and organisations, the technical architecture of an optimal digital identity model should reflect this distributed nature and prioritise setting open standards rather than seeking to unify attributes in one system.

16. For the user, a new model could work as follows:

    a. Users install an app-based digital wallet, with personal data stored on the phone (a trusted personal device which acts as the digital-equivalent of a 'safe place').

    b. Data is protected using modern cryptographic methods, with the digital wallet generating a 'keypair' of public and private keys. As with messaging services, the public key can be shared with anyone, and because the user's keys are linked only their private key can decrypt a public key-encrypted message.

    c. Users send claims to be verified by identity authorities, such as being a citizen of a country or having the right to work, along with their public key and scans of 'proof documents' (e.g. birth certificates, driving licences or passports). Identity authorities then provide digitally-signed attestations and associate them with a user's public key, verifying that the claim is indeed proven by the attached document.

    d. Users then share these digitally-signed attestations with third parties when required, such as to prove eligibility to work, verify qualifications or buy restricted items. They can also create authoritative, digital signatures for official documents using their private key, with the encrypted, decentralised system ensuring trust between counterparties without the need for any central intermediary.

We also advocate that government retains a role as the ultimate identity authority. In many cases, organisations will not need to verify identities authoritatively (e.g. retail loyalty schemes, where loyalty cards could sit independently of other attestations in a digital wallet). Yet for others, such as employers verifying applicants' qualifications, organisations will need to know that certifiers are authoritative. In this example, universities would themselves need to be certified as such by government in order to provide authoritative attestations to graduates of their degree status.

INDIRECT BENEFITS

17. The decentralised model would enable organisations as varied as dentists, doctors, and councils to request API access to data stored on each other's servers – when necessary and with users' consent – while avoiding either a central database or multiple duplicated ones.

18. In turn, this approach could also facilitate a new model of transparency where users can see who has accessed their data and why, as the Science and Technology Committee has recommended based on the Estonian model. Similarly, as part of the TUO initiative, data is collected once only and recorded in a standardised, machine-readable format so that each of the partner organisations can receive updated information via an automated API. A similar model used across society could be hugely impactful, enabling citizens to push new credentials from their wallet (e.g. when their name or address changes) to a range of organisations via an API. This would also obviate the need to duplicate information across organisations and ensure that data need only be collected once. Embedding these user-centric and economically productive benefits in a new model should be a priority.