Response to DCMS call for evidence on digital identity
September 2019

Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect fundamental rights to privacy and free speech online. With over 3,000 active supporters, we are a grassroots organisation with local groups across the UK.

Our response to this consultation builds particularly on our past work on proposals for a Scottish National ID Database, Verify and the Digital Economy Act 2017.

Needs and problems

The value of digital identity checking for individuals and organisations depends on:

(a) the service for which ID is being required;
(b) the need for an identity check to access that service;
(c) the level of assurance the identity check needs to achieve.

Whilst digital ID solutions can improve consumer experience and increase efficiency, their benefit in particular circumstances is always contextual. Requiring digitally verified authorisation to access simple benefits or implementing digitisation in a situation where service users are unlikely to possess the required documents or be able to access an online checking system will not meet the needs of individuals or organisations. In these circumstances, both parties will be frustrated by impassable hurdles and either find ways of bypassing them (presuming the digital route is not mandatory) or opt not to engage with them at all and default to a basic face-to-face confirmation.

The National Audit Office report on Verify points to some of those needs and problems, noting that these ultimately led to a significantly lower take-up of the system than expected and poor verification success rate. The 2015 business case states the verification should be 90%; in reality

the success rate was 48%.[1] Particularly concerning are the applications for universal credit which had a success rate of 38%.[2]

- **Before embarking on setting new standards and deciding on authorisation levels, the Government should explore further what factors contributed to the low level of successful verifications in Verify.**

This is the stand-out need for this stream of work: understand the problems of what came before. If the Government cannot sufficiently explain why current verification practices are so low, exploring suitable solutions will be impossible. The issues could be myriad, including but not limited to; bad user journeys, failure to have required documentation and user error, perhaps a result of poor systems or explanations. Each of these problems, and there could be more, would have a different solution to explore.

Criteria for trust

Strong privacy protections are essential to build trust. User testing undertaken on behalf of the Scottish Government showed a recurring theme of "cautious", which focused on concerns about data privacy and security.[3]

There were also findings that showed that different actors were trusted differently by citizens. Some people were comfortable with private sector organisation such as banks and Google holding data and distrustful of government. Others were more trustful of government and more wary of private actors.

- **Consumer choice can assist to build trust: there should never be only one route by which people can verify their identity.**

Other Scottish user concerns included how secure the system would be, with test subjects raising questions about data held centrally and giving access to multiple services. If personal identity data were compromised it would be a very concerning outcome with potentially long-term damaging effects.

Demonstrating security while also not creating an overly burdensome system is a difficult task. But there are ways that this can be worked on, including by organisations and government working harder across the board to demonstrate their trustworthiness to individuals. Public Key Infrastructure could be used to provide assurance by helping a user verify an identity provider or

[1] Verification success rate, https://www.gov.uk/performance/govuk-verify/verification-success-rate.
[2] National Audit Office, Investigation into Verify, https://www.nao.org.uk/wp-content/uploads/2019/03/Investigation-into-verify.pdf.
[3] Online Identity Assurance - Listening to your views, Scottish Government, 1 June 2018, https://blogs.gov.scot/digital/2018/06/01/online-identity-assurance-listening-to-your-views/.

a third party. There are fraudulent acts conducted on individuals by individuals pretending to be institutions,[4] yet the Verify programme's use of PKI only operates between the service, the Identity Provider, and the Verify Hub;[5] the user is left out of the trust process. If the trust only flows one way - the individual proving they are who they say are to the institution - there is a trust deficit. PKI could and arguably should move both ways.

- **To mitigate against trust deficits, the Government could consider a certificate authority that works to demonstrate and foster two-way trust to users.**

Protecting user privacy whilst responding to innovation

We encourage DCMS and others to take lessons from the fractious situation in Ireland created by the Public Services Card (PSC).[6] The PSC scheme (a Government-issued smart card that became mandatory by practice) was conceived as one that would make it easier access to public services with chip-and-pin type cards being used for actual card-based transactions. However, the Irish Data Protection Commissioner found that the scheme quickly lost its original purpose and was subject to piece-mail changes that lacked coherence and did not sufficiently balance the interests of the State, acting through the public bodies which participated in the scheme, and the interests of the members of the public who were required to obtain and produce the card.[7]

The PSC initiative provides an important lesson: make sure that appropriate governance is in place before data processing begins, and ensure it responds specifically to the framework proposed with all the relevant actors and transactions laid out ahead of time.

- **Before any system is implemented, the Information Commissioner's Office needs to have sight of the proposed processing framework in the form of a service-wide data protection impact assessment.**

Choice is also vital to ensure privacy. If there is only one identity provider available for a particularly sensitive group or particularly sensitive process then the system in effect identifies those individuals through their relationship with that one identity provider.

---

[4] Fraudsters targeting people with offers of free or low cost government loans, Action Fraud, 30 July 2019, https://www.actionfraud.police.uk/alert/fraudsters-targeting-people-with-offers-of-free-or-low-cost-government-grants-and-loans.

[5] Gov.uk Verify, Message Flow, https://www.docs.verify.service.gov.uk/technology-overview/message-flow/#message-flow.

[6] Public Services Card, Citizens Information Ireland, https://www.citizensinformation.ie/en/social_welfare/irish_social_welfare_system/public_services_card.html

[7] DPC Statement on Matters Pertaining to the Public Services Card, 16 August 2019, https://www.dataprotection.ie/en/dpc-statement-matters-pertaining-public-services-card-0

To prevent this outcome, there needs to be some form of service agreement with identity providers entering the UK market whereby they commit to providing ID checks for all necessary processes, or all processes under a certain level of authorisation: this will prevent any one specific service being tied to just one provider.

There is a significant fundamental rights deficit to be made up when it comes to technology and identity. It is only by doing the hard work of showing transparent governance that the deficit can be paid off.

- **Identity providers and relying parties need to be pushed to demonstrate their compatibility and privacy credentials to users and regulatory authorities.**

Providers need to be governed transparently and provide relying individuals with clear lines of accountability. Data Protection Impact Assessments need to be completed and published. Compliance with the General Data Protection Regulation (GDPR) must be shown and checked, including that providers are obtaining valid consent for personal data processing, making secure and limiting data retention, and restricting data processing to the specific identifying task required.

Institutions engaged in the process

- **The Information Commissioner's Office should be involved in terms of ensuring data privacy, including trust services established in the eIDAS regulations.**
- **The National Cyber Security Centre should be consulted on matters of security.**
- **The Centre for Data and Ethics and, by extension, a much wider cohort of academics, civil society organisations and members of the public, should be engaged to ensure ethics and human rights are embedded into systems and processes.**

From a public engagement perspective, it is advisable to take the path set out in Scotland: setting up regular stakeholder working group meetings and an independent expert group, to which the team responsible can bring ideas and updates on progress. This will help continue to demonstrate to all stakeholders how the approach is developing and protecting the privacy of users.

There should also be regular audits, and spot checks of the framework by independent groups after one year with a decision taken after this whether to keep the rate of review at the same point or extend.

Role of the government

The most important role for the Government is setting out a legal framework that creates a robust, trustworthy and reliable system for citizens to use. This could be done in the form of

setting out laws, facilitating the creation of a technical framework and importantly providing opportunities for consultation and feedback.

The Government has made a strong start in providing this consultation opportunity and holding roundtable events across the United Kingdom. Open Rights Group is encouraged by this effort and hopes it will continue throughout this process. The Scottish Government set up regular stakeholder engagement activities throughout their process of developing a digital identity system,[8] which provided many valuable opportunities for feedback and mutual learning either in person or via email; Open Rights Group encourages the United Kingdom Government to adopt a similar Open Government approach to this work.

Digitising attributes

The Government does not need to make the ID attribute in digital form shareable. Instead there could be a system that provides an attestation attributes online for relying parties to query, e.g.:

- Over 18?
- Goes to this school?

Existing models for government to explore include the Alberta Credentials Ecosystem[9] which utilises a decentralised model allowing an individual to hold the credential or attestation themselves. This would allow the querying of the credential on request, or alternatively allow passively but with a log of who accessed the attribute, and when.[10] The Government's role in this could involve setting out the types of attributes that would be considered suitable for access to public services, encouraging public authorities to issue attributes through providing a de-centralised technological solution, and technical support for the use of that system.

As a side-note, it is also important that any digital identity system operates where people actually want to use it. Verify suffered in part because even government services did not use it as their identity provider: perhaps the biggest loss was HMRC using a separate identity framework. By 2018, only nineteen government services were using Verify, whereas GDS had expected over twice that number.[11]

Legislation to revisit

[8] See the Scottish Government's Digital Team blog for reports on events throughout 2018 and 2019, https://blogs.gov.scot/digital/2019/02/22/digital-identity-scotland-understanding-the-services-perspective/.
[9] https://www.evernym.com/blog/alberta-credentials-ecosystem/
[10] For more information see evernym's work in this area https://www.evernym.com/solution/.
[11] National Audit Office, investigation into Verify, pg. 5 https://www.nao.org.uk/wp-content/uploads/2019/03/Investigation-into-verify.pdf.

Data sharing provisions in the Digital Economy Act 2017 will need to be considered as part of this programme, in particular to combat fraud. The proposed system may need to allow for data sharing to prove entitlement to combat fraud. Chapter 4 of the 2017 Act focuses on fraud against the public sector, and section 56 creates a power for a specified person to disclose information to another specified person for the purposes of taking of action in connection with fraud against a public authority.[12]

The Government should explore what data sharing agreements are necessary for this purpose. We encourage the Government to focus on three criteria. Data sharing agreements should:

(a) Not lead to a widespread intrusion on people's privacy;
(b) Be proportionate, limited in scope and enshrine fundamental rights; and
(c) Carry strong safeguards against wilful abuse and unintended consequences.[13]

It would also be worthwhile for the Government to undertake an assessment of any proposed framework against the eIDAS Regulations (electronic identification and trust services).

Role of the Private Sector

Open Rights Group is strongly opposed to the idea of a mandatory single identifier issued by the Government as an identity. The private sector has a key role in the success of a digital identity framework that allows choice and innovation.

Millions of individuals have identity relationships with private actors, such as financial institutions who hold personal identity as part of a pre-existing financial relationship, credit reference agencies who require access to personal information in order to issue and manage loans, actors that provide identity services as their primary business such as Yoti, or universities that issue students with identity documents.

- **The challenge for a national identity system is in allowing an individual to use these pre-existing identities to assert their identity, rather than requiring them to set up a new identity relationship which will negatively impact uptake, as we saw in the Verify roll-out.**

- **The private sector also needs to be a good faith partner, only allowing identity information to be used for the purposes it is approved for, and not for commercial purposes or exploitation.**

[12] Section 56, Digital Economy Act 2017, http://www.legislation.gov.uk/ukpga/2017/30/section/56/enacted.
[13] Open Rights Group was extensively involved in drafting the data sharing provisions of the 2017 Act. See Response to data sharing consultation, https://www.openrightsgroup.org/about/reports/orgs-response-to-data-sharing-consultation.

The private sector's role in demonstrating the security of their systems is vital for an identity system which relies on these to work. For this, they need to submit to security audits from independent bodies that will then provide clarity and certainty on the security.

The private sector will also have an important transparency role to play - which could be supported and facilitated by innovation. If private actors are to be the main or sole identity providers or holders of attributes they will represent the key gateway relationship between the individual and the relying party. This will mean that the important task of demonstrating to individuals that the relying party is who they say they are will fall on them in some way. Giving the private sector targets to hit such as meeting a principle of two-way trust could make for an innovative path that improves trust between individuals and relying parties, and ultimately to the benefit of the identity system itself.