PRIVACY INTERNATIONAL

Digital Identity: Call for evidence by the Department of Digital, Culture, Media, and Sport, and Cabinet Office

September 2019

About Privacy International

Privacy International (PI) is a leading charity advocating for strong national, regional, and international laws that protect the right to privacy around the world. Founded in 1990 and based in London, PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy.

Within its range of activities, PI investigates how peoples' personal data is generated and exploited, and how it can be protected through legal and technological frameworks. PI employs technologists, investigators, policy experts, and lawyers, who work together to understand the technical underpinnings of emerging technology and to consider how existing legal definitions and frameworks map onto such technology. A representative from PI sits on the Privacy and Consumer Advisory Group (PCAG).

Introduction

The opportunity to contribute to this Call for Evidence on the future of Digital Identity in the UK is a welcome one. It would be positive for both the UK, and the development of identity systems around the globe, if the UK builds a digital identity ecosystem that becomes a world-leader in respecting the rights of individuals and communities. Yet the risks of digital identity are large, from dangers surrounding the curtailing of people's rights and state surveillance, to the exploitation of their data by private companies. As a result, the highest standards must be in place to meet the promise of a world-leading system.

Needs and Problems

The initial question surrounding the development of *any* identity system has to be one of its purpose and need, and it's essential that the design of the system meets that need[1]. At the same time, given the potential of an identity system to interfere with the fundamental right to privacy, the purpose should be clearly defined, legitimate, and such systems should be deployed only if there is not another less intrusive way to achieve the same goals.

[1] See Privacy International's material on guidance on the design of an identity system: https://privacyinternational.org/explainer/2669/understanding-identity-systems-part-1-why-id

As a result, it is important to recognise that there are design choices that would be inappropriate in meeting the stated need of allowing individuals to "use different verified attributes to access a range of services as and when needed"[2].

The Call for Evidence calls for a digital identity system "without the need for identity cards". This is to be welcomed, yet it is important to emphasise that this must also extend to not having a centralised identity database. The research done on the proposed UK ID system in the mid-2000s is still salient[3]. The abuses of systems like India's Aadhaar since this has shown that these arguments remain relevant[4].

It is also essential that there are no 'unique identifiers' (for example, a single ID number used across multiple services, whether such an identifier is known to the user or not). Such an identifier enables the creation of dossiers of information about individuals - "the hallmark of the totalitarian state"[5] - as well as the private sector (as illustrated in the Supreme Court ruling on Aadhaar that found the private sector use of Aadhaar unconstitutional because of the risk of profiling it brought[6]).

Further, a system must not necessitate the creation of one, single unique identity for individuals. An individual's identity is a set of complex, multifaceted and interrelated issues[7]; and the creation or imposition of a single unique digital identity can limit or condition the development and expression of this complexity. A single and unique 'digital identity' removes much of the individual's agency in managing their identities, and so is central to allowing individuals to have control over their identities.

A well-designed federated identity ecosystem has the *potential* to avoid many of these issues, for example by not having a centralised database or ID card, and enabling the opportunity for creating multiple accounts with various Identity Providers. However, it remains the case that even such a system can be open to human rights abuses or open to exploitation of people's data. The design of such a system must be such that the risks are minimalised.

---

[2] As stated in the Call for Evidence: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/818801/Digital_Identity_-_Call_for_Evidence.pdf

[3] http://eprints.lse.ac.uk/29117/

[4] See, for example, these examples of failings: https://privacyinternational.org/aadhaarsecurityfails

[5] Marcel v Commissioner of Police of the Metropolis [1992] Ch 225, 240 (Browne- Wilkinson VC).]

[6] See Privacy International's analysis of the Aadhaar ruling: https://privacyinternational.org/long-read/2299/initial-analysis-indian-supreme-court-decision-aadhaar

[7] See https://privacyinternational.org/long-read/2274/identity-discrimination-and-challenge-id

Rather than starting from a blank page, the starting point for this has to be the existing work done on this subject, including the Identity Assurance Principles[8].

Data and Identity Assurance Systems
Particular attention is drawn by PI to the abuses of data. The Identity Assurance Principles[9] state that: "Identity Assurance data processed by an Identity Provider or a Service Provider to facilitate a request of a Service User must be the minimum necessary in order to fulfil that request in a secure and auditable manner." PI would like to emphasise that 'data' includes personal data as well as 'metadata', for example data about identity transactions. It should also include pseudonymised, anonymised and aggregate data.

An identity assurance system is a 'gatekeeper' to accessing services to which the individual is entitled, and thus has to protect that individual. It is thus inappropriate, and must be prevented, for the use of these various forms of data for purposes other than providing the identity assurance system[10]. For example, it is not appropriate to use this data for the purposes of direct marketing; to train algorithms (for example, developing age verification algorithms); or to use aggregate data for marketing purposes.

The identity ecosystem that is developed, and the economics of the system, must reflect this: for example, the source of income for identity providers must be from providing identity assurance services, rather than any other use of the data (with the appropriate Chinese walls and other measures in place within companies, if necessary).

There are technical solutions that can aid in the design of the system. For example, a federated system can make use of Zero Knowledge Proofs, which can be used to prove that a party has evidence or proof of an attribute without revealing that evidence or the underlying data. One of the great opportunities will be for the development of new innovations in these types of technologies, deployed in a real-world environment.

---

[8] https://www.gov.uk/government/publications/govuk-verify-identity-assurance-principles/identity-assurance-principles

[9] https://www.gov.uk/government/publications/govuk-verify-identity-assurance-principles/identity-assurance-principles#data-minimisation

[10] The current data protection framework further reinforces this point. The principles of data minimisation, purpose limitation and storage limitation, present in both the GDPR and the Data Protection Act 2018, establish that only necessary data must be processed, according to clearly (pre)defined purposes, and only for the necessary amount of time.

Technology, however, is never a panacea. It is also essential that the identity providers, the hub, and the relying parties are subject to appropriate regulation, certification, and standards.

Inclusion and Exclusion

Particularly as the ID system's role is to enable people to authenticate their identity to access government services, it is imperative that the ID system is as inclusive as possible, and mitigate exclusionary consequences, which might be caused by economic, cultural, geographical, physical ability, or other factors. This is why some identity startup solutions (that require users to have an existing document like a passport) or bank-based systems (that require users to have passed KYC checks) are not suitable solutions.

As highlighted in Privacy International's research on identity and exclusion, mandating the need for identification - or one particular form of ID - to access services leads to social exclusion[11]. Similarly, it has to be recognised that those who have difficulty getting the proof of identity are also those open to exploitation, as shown by Privacy International's research into the fintech sector[12], emphasising the importance of protections to be placed in a system.

To broaden inclusion in the system, we need to make sure that a broad range of diverse ways for people to prove their identity are permitted, as well as measures to improve accessibility (like, for example, real-world help points). To lessen the risks of exclusion as a result of identity systems, the situations that need a form of identification must be minimised – in particular, the introduction of a digital ID system must be stopped from leading to new uses of ID where currently there is no such requirement. If it is the case that identity is required, there needs to be a breadth of options available, not limited to one particular system.

These are reasons to emphasise that it needs to be that service providers (Relying Parties) are governed standards and certification about the use of any identity system.

Trust

Any standards, assurance or certification must arise from the Principles upon which a system is built. These Principles must be built into any standards, as well as any contracts between the government and private entities.

[11] See https://privacyinternational.org/long-read/2544/exclusion-and-identity-life-without-id

[12] See https://privacyinternational.org/report/998/fintech-privacy-and-identity-new-data-intensive-financial-sector

However, while strong standards are important, so is strong enforcement of these standards. A vital element of this is the role of data protection laws, namely the EU General Data Protection Regulation and the UK Data Protection Act 2018, that set out various principles (lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, as well as accountability). The design of a digital identity system must allow the user to exercise their rights effectively, and also allow regulators to oversee the implementation of the scheme and make sure that users' rights are upheld and providers are subject to strict scrutiny. Ways of effectively exercising users' data protection rights (for example, to access, erasure, restriction of processing, rectification and portability) in a user-friendly way should be developed, for example through an online platform. It is also the case that the ICO must play a key role in the development, regulation and enforcement of any system; they must have the resources to be sure to be able to do so.

One particular aspect that requires additional concerns, is the processing of special categories of data, and particularly biometric data: as the UN Commissioner for Human Rights pointed out, the consequences for misuse of such data are grave.[13] Further to that, it is essential to ensure the integrity and confidentiality of biometric data, especially given the fact of its uniqueness and irreplaceability. It is essential that the role of biometrics in any identity system follows strict rules[14].

The use-cases for identity authentication enable some uses of biometrics to be banned in this context, for example the use of one-to-many matches for the purpose of identification[15]. If after carefully assessment, biometric data needs to be used, such data should be processed on device, and should not be transmitted, stored or shared.

Biometric data should, strictly, not be used outside its defined purposes, including its use to train algorithms or models. It must also not be used for other purposes, even if such purposes are technically not 'biometric' under data protection law: for example, the use of facial photographs to train age-verification algorithms.

The rules of the road

In setting the "rules of the road", it is vital that civil society (including human and civil rights organisations, consumer rights organisations, and others) play a key role in these discussions. As Privacy International's work with our partner organisations

[13] See https://undocs.org/A/HRC/39/29

[14] See https://privacyinternational.org/long-read/3067/have-biometric-id-system-coming-your-way-key-questions-ask-and-arguments-make

[15] For more on biometrics, see https://privacyinternational.org/long-read/3067/have-biometric-id-system-coming-your-way-key-questions-ask-and-arguments-make

across the world has taught us, these organisations provide the skills and expertise that enable the scrutiny of a system. Civil society provides invaluable insight into issues including exclusion, human rights, and privacy. While civil society can be portrayed as the blockers of innovation, in our experience they generate new and innovative solutions that improve individual's privacy and drive the industry forward. In the UK, PCAG would be one tool for a role in this.

The Role of the Government

We must not see a future where there is a 'free-for-all' in the accessing of government databases. The use of other data sets should only be accessible to IDPs in the context of:

- Only happens in the context of the scheme, subject to strong safeugards;
- Based of yes/no verification;
- Limited to identity authentication (eg, confirming someone's address) rather than entitlement to services.

In order to have a digital identity ecosystem with strong privacy and security safeguards, it is necessary to have statutory regulation – within the current human rights and data protection framework – to clearly define and limit the purposes of the processing of personal data. It may also be necessary to have enhanced security requirements and sanctions for data breaches and security incidents in general, including special notification requirements to government departments, and enforceable protocols and standards that enable government and oversight authorities to give due oversight on the process.

The Role of the Private Sector

The private sector are clearly among the key stakeholders for the creation of a digital identity ecosystem. However, the basis for this must be a recognition that the goal must also be a clear and transparent financial model for the ecosystem, based on agreed principles. Certain business models would be inappropriate (for example, if an identity provider was seeking to an age verification algorithm trained on the scans of identity documents as part of this system).

Competition in the identity market has to have socially-desirable ends. For example, it is essential that any identity system is straightforward and easy-to-use for the individual. However, as Privacy International's work on the fintech market has shown, ease of use can be used to "mask a hugely complex process occurring behind the scenes"[16]. The concept can be used to hide from the customer essential details; remove consumer choice and the ability to make privacy-conscious

[16] https://privacyinternational.org/report/998/fintech-privacy-and-identity-new-data-intensive-financial-sector

decisions, or to manipulate the user with 'dark patterns'. Ease of use must be used to enable privacy by design and default, which is where the attention in improving user interfaces and other aspects of design must lie.

Conclusion

Given the international nature of the discourse surrounding digital identities[17], the development of a digital identity ecosystem would be a fantastic opportunity for the UK's international reputation. But this potential can only be realised if it meets the highest standards of privacy and human rights.

[17] See the work conducted by the World Bank, Omidyar Network, Bill and Melinda Gates Foundation, and others.

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint
Instagram @privacyinternational

UK Registered Charity No. 1147471