House Financial Services AI Task Force

I Am Who I Say I Am: Verifying Identity while Preserving Privacy in the Digital Age

July 16th 2021

Dr Louise Maynard-Atem, Women in Identity

Good afternoon and thank you Chairman Foster, Ranking Member Gonzales and the other members of the task force for the opportunity to testify today.

My name is Louise Maynard-Atem and I'm the research lead for the non-profit organisation Women in Identity; an organisation whose mission is to ensure that digital identity solutions are designed with the diverse communities that they serve in mind. We are a volunteer-led and member-focused organisation, and all work full-time in the digital identity sector. Women in Identity is entirely independent and not acting in the interests of any one organisation or individual. Instead, our volunteers and members are united by the belief that we need to make identity systems that work for everyone, ensure that they are inclusive for all and free from bias. Today I will be representing the views of Women in Identity, but it is also pertinent to the topic of today's hearing to mention my full-time role. I lead the data insights function at GBG, an identity and fraud organisation whose mission is to drive trust and confidence in digital transactions through the provision of identity proofing services.

The specific topic I would like to focus on today is that of inclusion and bias. The need for improved digital identity systems and infrastructure has been a pressing requirement for many years, as more businesses have moved their operations online. The pandemic has accelerated that shift online, and increased the focus on the need for digital identity infrastructure over the last 18 months. This presents us with a unique opportunity to enable economic and societal value creation as digital identity systems are the gatekeeper to access services like online banking, e-commerce and insurance. However, we also need to recognise that the use of technology in digital identity systems has the potential to further entrench, and potentially exacerbate, the exclusionary and biased practises that persist in society today. Simply digitising what were previously analog processes and utilising flawed data would be a missed opportunity to deliver systems and services that benefit all citizens.

At Women in Identity we believe that inclusion doesn't just happen on its own. In order for identity systems to be inclusive and free from bias, the requirement for it must be mandated. There are many examples where exclusion and bias have not been explicitly mandated against within identity systems, and in many of those instances identity systems have been built which have excluded certain groups, often because of particular characteristics such as skin colour, gender, culture, socio-economic background or disabilities. Examples include:

- Up to a third of adults (women and the elderly were particularly affected) in Kenya were excluded from healthcare and social services due to lack of a national ID card, a prerequisite for gaining access to the country's digital identity card[1]

1 https://www.theguardian.com/global-development/2021/jun/09/ugandas-id-scheme-excludes-nearly-a-third-from-healthcare-says-report

- According to a member of the Iraqi Commission for Human Rights quoted in Kurdistan, 1.5 million Iraqis born between 2001 and 2003 and who should be voting for the first time, will not be able to do so as their names are not on the voter register and they have not received their biometric or temporary cards.[2]

According to recent population statistics for adults in the United States:

- Approx. 11% of American adults don't have government issued ID documents (which is approximately 20m people)[3]
- Approx. 18% of American adults don't use a smartphone[4]
- 5.4% of US households are unbanked (approximately 7.1m households)[5]

The lack of government issued ID, ownership of a smartphone or bank account can often be some of the building blocks used in creating a digital identity for an individual. There are many and varied reasons for the above, but it is essential that any digital identity solution is accessible to all of these groups, and does not cause them to be further excluded from the opportunities that such technology-driven solutions may become the gatekeeper for.

In the physical world, we would never erect buildings that weren't accessible to all (features like wheelchair ramps are mandatory). We need to ensure we are mandating equivalent accessibility in the digital world.

Establishing an inclusive identity system requires an exclusion risk assessment and explicit strategies to ensure access to identification for all, with particular attention to groups that are at higher risk of exclusion, such as remote and rural residents, ethnic and linguistic minorities, people with disabilities, marginalized women and girls, and those with low technical literacy.[6] As part of the planning process, decision makers should also carefully consider the exclusion risks of formalizing or increasing identification/authentication requirements for different transactions.

What we are observing is a move towards identity trust frameworks being developed around the world, where the need for inclusion and testing for bias is being explicitly called out. To share some insight into how inclusion in digital identity is being thought about here in the UK, I wanted to discuss the UK Digital Identity and Attribute Trust Framework[7] that Women in Identity was involved in consulting on. The UK trust framework, published in alpha form in February 2021, sets out requirements to help organisations understand what 'good' identity verification looks like. There are explicit call-outs around making sure that products and services are inclusive and accessible, and organisations are required to complete an annual exclusion report to transparently explain if certain users are excluded and why.

---

[2] https://www.biometricupdate.com/202106/biometric-card-delays-exclude-millions-from-iraq-elections

[3] https://www.learningforjustice.org/sites/default/files/general/Percentage%20of%20People%20Who%20Lack%20ID_0.pdf

[4] https://newzoo.com/insights/rankings/top-countries-by-smartphone-penetration-and-users/

[5] https://www.fdic.gov/analysis/household-survey/index.html

[6] https://id4d.worldbank.org/guide/creating-good-id-system-presents-risks-and-challenges-there-are-common-success-factors

[7] https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework

Extracts From the UK Trust Framework[8]

2.3 Make sure your products and services are inclusive

Making your products and services inclusive means everyone can use them no matter who they are or where they're from. One of the aims of the trust framework is to make it as easy as possible for users to create and use digital identities (either online or in person).

All identity service providers must follow the Equality Act 2010 by considering how to make sure no one is excluded from doing this because of their 'protected characteristics'. There are notable exceptions to this, such as it being fair to restrict service access on account of someone's age, e.g. you cannot buy certain products until you are 18.

There are many reasons why a user may be excluded from using a product or service. One common reason is because users are asked to provide specific evidence as proof of their identity.

Example

A service that only accepts a UK passport as proof of someone's identity will exclude users who do not have, cannot find or cannot afford a passport.

You can prevent this happening by accepting a wide variety of evidence as proof of users' identities and eligibility. You can also choose to accept a declaration from someone that knows the user (known as a 'vouch') as evidence.

Requiring information to be checked against certain authoritative sources can also exclude some users from creating a digital identity.

Example

A service that only checks users' information against a credit reference agency database will stop users who do not have much of a credit history from creating a digital identity. This could exclude users because of their age or income.

You can prevent this from happening by checking information about users against a wider range of sources.

Another reason why you might exclude users is if a product or service uses any third party software that's only been tested with a specific user group.

Example

A service might check users' identities using an existing facial recognition system that was tested with a small sample of users. As most of these users were white men, the system was not taught how to recognise users of other genders or ethnicities.

By choosing this system, the service will exclude some users from proving their identity because of the way they look.

You can prevent this from happening by choosing software that you know has been tested with a variety of users from different demographics.

8 https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework

The first step to building an inclusive product or service is to find out as much as you can about the types of people who will use it. If you do not know who they are or what they need, you cannot be sure you have built the right product or service.

You must make sure that making your product or service more inclusive will not expose it or your users to any additional risks.

Submit an annual exclusion report

All identity service providers must submit an exclusion report to the governing body every year. The governing body will tell you exactly what information should go in the report. It will at a minimum need to say which demographics have been, or are likely to be, excluded from using your product or service. You must explain why this has happened or could happen.

Sometimes users will be excluded for a good reason. For example, users under 18 should not be able to create a digital identity to access a gambling website so it would be right to stop them from doing this. You must explain if this has happened in the report.

You must write the report based on evidence, for example findings from user research or data and analytics for your product or service. You do not need to collect any additional personal information from your users.

You must also explain what you'll do to improve the inclusion of your product or service in the report.

2.4 Make sure your products and services are accessible

You must follow the accessibility regulations if you're a public sector organisation that's developing apps or websites. This includes any products or services that help users create digital identities or manage their attributes.
If you're a public sector organisation that develops products or services for users in Wales, you must also follow the Welsh Language Act 1993. This means your product or service must be available in Welsh.

You should also aim to develop products and services that everyone can use if you're not a public sector organisation. To help do this, we suggest you follow the:

- *Web Content Accessibility Guidelines (WCAG)*
- *new European Telecommunication Standards Institute (ETSI) standard on accessibility requirements suitable for public procurement of ICT products and services in Europe*

You should always make sure users have more than one way to use your product or service. For example, a user should have another way to create a digital identity if they're unable to use the online service.

It is also worth noting that the Information Commissioner in the UK (responsible for upholding information rights in the public interest) has responded in support of the UK Trust Framework, but raises cautions if digital identity and attribute systems (or service providers consuming digital identity and attributes) rely on automated processing, due to use of algorithms or artificial intelligence within the systems. Automated decision making may have discriminatory effects due to bias present in system design, algorithms or datasets used in the creation and build of the product or service.[9]

The Pan-Canadian Trust Framework lists inclusivity as one of its guiding principles, stipulating that digital identity services and tools must be affordable, standardised and create value for users in the interest of broad adoption and benefit to all Canadians.[10]

The World Bank released the second edition of their principles on identification for sustainable development in 2021 to reflect the quickly evolving nature of the identity sector as part of the Identity for Development (ID4D) initiative. The principles are based around three key pillars, the first of which is inclusion. Within this pillar, two key points are called out; (i) *Ensure universal access for individuals, free from discrimination and (ii)Remove barriers to access and use*.[11]

At Women in Identity we are currently carrying out a piece of research that seeks to understand the societal and economic impact exclusion in the context of digital identity within the financial services sector.[12] This research will inform the creation of a code of conduct, designed to help solution providers identify and mitigate potential areas of bias and exclusion in digital identity product design, to ensure that the industry is building products that work for everyone, not just the select few.

To conclude, we believe that in order to achieve the full potential of digital identity systems, inclusion requirements must be specifically mandated within any regulation or legislation and measured on an on-going basis. I've mentioned a number of examples of how this is being done elsewhere, and I strongly believe there is benefit in sharing best-practices and lessons learned with other industry bodies and consumer advocacy groups to ensure that we can deliver systems that enable all citizens equally.

Thank you.

---

9 https://ico.org.uk/media/about-the-ico/documents/2619686/ico-digital-identity-position-paper-20210422.pdf

10 https://diacc.ca/trust-framework/

11 https://id4d.worldbank.org/principles

12 https://womeninidentity.org/2021/07/13/code-of-conduct-launch/