Will 2021 be the year that digital identity finally takes off?

Blog post by Associate Megan Stagman, 4 March 2021

After a recent history that is best described as stop-start, the first few months of 2021 have seen new momentum for the roll-out of digital identity schemes, with fresh legislative initiatives in the pipeline for both the UK and EU. The question is whether this time will be different. Public apathy and scepticism towards online identity schemes, combined with a number of failed public sector schemes, have not made for a supportive environment for the fledgling industry. But if legislation moves ahead and the technology does manage to take hold, we should expect it to permeate into a broad range of different sectors, including social security, financial services and healthcare, to name just a few.

The past year has seen renewed calls for adoption of digital identity technology, driven in part by the way that covid-19 has moved lives online. The World Economic Forum argues that digital identity could play a key role in mitigating the risks to health, movement, travel and trade arising from the pandemic. Among the most notable of these risks is the fact that as more activity shifts online, identity fraud has surged. Research suggests that identity document fraud increased by as much as 41% over the course of 2020, providing a clear use case for digital identity to increase security online.

In this context, the wheels of legislative change are finally starting to turn. At the EU level, the European Commission is expected to present its plan for a secure European digital identity in April. The EU's executive body will make clear whether it will seek to: strengthen current legislation (and extend its application to the private as well as the public sector); require electronic identification systems to meet the criteria of its eSignature Directive; or come up with a fully-fledged "self-sovereign identity" system. Depending on the approach taken, this could result in member states being required to provide citizens with eIDs, new data protection requirements for digital ID service providers, and established guidelines on issues like cost and interoperability for the private sector.

In the UK, the Department for Digital, Culture, Media and Sport (DCMS) unveiled a new policy paper and corresponding consultation on its proposed framework for digital identity last month. Although the Government cites a variety of potential use cases including age verification, pre-employment screening or accessing financial services, the framework is deliberately non-specific. It is intended as a first stage industry prototype (or "alpha"), to be tested and iteratively developed before being underpinned by legislation that will enable it to certify organisations as providing "good" digital identities. With the framework seeking to introduce rules on data protection, security and inclusivity for both identity service providers and users, this will establish new certainty for the full ecosystem of actors involved in digital identity provision and use.

Although these developments place the spotlight primarily on the private sector, after a few false starts the public sector is also moving towards uptake. In February, UK Cabinet Office minister

Michael Gove wrote to all government departments making clear that central government services will be required to migrate onto "a single sign-on and identity assurance system" currently being developed by the Government Digital Service (GDS). Gove called on departments to coordinate on delivering a shared, jointly-owned solution rather than pursuing a fragmented approach which would "lead to further disappointment".

That said, the same obstacles which have prevented digital identity from taking off in previous years will not simply vanish. For starters, there is a legacy of political scepticism among parliamentarians about any new initiatives in the identity space, given the multi-billion pound failed attempts to roll out national ID cards in the 2000s.

Moreover, digital identity specifically brings with it new concerns. A Liberal Democrat policy briefing on the topic this month raised fears around data protection, mission creep in terms of user profiling, and the risks of enforced conformity. Such views will be shared by parliamentarians in parts of both the Conservative and Labour parties, and supported by civil liberties advocacy groups such as Liberty, who are wary of a project they feel could be "intrusive, insecure and discriminatory".

In addition to concerns about rights, digital identity may not even have administrative convenience on its side. As a result of persistent technical issues, digital identity initiative GOV.UK Verify was infamously only able to support 38% of Universal Credit applications in 2019, compared to an initial target of 90%. Not only did this foster frustration amongst online users who tried and failed to use the service but raised significant doubts among public sector officials as to whether digital identity was up for the task after all.

Digital identity companies will therefore still have critics to reassure, but it could be that 2021 is the watershed moment that industry has been waiting for. Successes in other regions and specific sectors (such as Nordic banks' high penetration rates of 75%) are beginning to stack up, and policymakers' familiarity with homegrown industry players such as Yoti and Onfido continues to grow almost a decade after they first came to market. In this context, Digital Infrastructure Minister Matt Warman has openly acknowledged that digital identity "has the potential to add billions to our economy" by accelerating the rate of transactions. As such, if an enabling regulatory framework can be put in place to establish trust and accountability, and government starts to lead by example, we may just (finally) see a rise in the deployment of digital identity technology.