APPG ON DIGITAL ID

Meeting: 6th February 2019 5.30 p.m. Committee Room Ten

1) Present

Chair: Lord Arbuthnot

Secretariat: Andrew Henderson

Ruth Milligan, TechUK ;

Steve Pannifer, Consult Hyperion

Andrew Churchill, Technology Strategy

Julie Dawson, Yoti

2) Speakers

Ruth Milligan:

Introduced the paper and thanked the contributors. A joined up framework for digital iD across the public and private sector is needed. Interoperability across many sectors is also what is being argued for. Aim is to allow digital IDs to flourish, to enable the private sector to collaborate with the public sector to the benefit of all citizens in the UK. Digital ID is key to opening up a range of services and sectors.

Urgent issue for the UK and we need to address this as a matter of importance, other countries have taken the lead with this.

Steve Pannifer:

1) Economic imperative

There are numerous reports about the benefits of digital ID to an economy. Consistently they talk about the value of digital ID being a % point of GDP. The value comes from addressing the many inefficient identity related processes that exist present. These often involve repeating the same manual tasks, like checking documents. Digital services are often held back because we cannot get the data we need to give the service to the individual at the time it is needed.

2) What do we mean by digital ID?

Firstly, identification which is about determining who you are such as KYC in banks. This is a narrow scope though focusing on a limited set of data.

Many transactions, however, required a much broader set of data to make them work. We need to be broad in our thinking.

Secondly, who is identity for? Individuals have identities as do businesses. And identity needs to flow in all directions for all types of transaction – B2C, C2B, B2B, etc. We need to think of all of these to solve the problem.

3) Give some examples of some of those places elsewhere in the world where progress has been made.

Bank ID in the Nordics, there is a history of banks playing a role successfully in identity. Solved a pain point at a certain time so that Internet Banking could be offered.

Many schemes resolve a piece of the puzzle and are not as broad as they might be. They resolve an issue.

Could we do it in the UK? Bank ID worked in Norway due to a particular local set of conditions.

Needs to be a push and a pull to make this happen. The Govt needs to do the standards piece and the pull needs to come from the market. Therefore get behind the paper, important step in the right direction.

Andrew Churchill:

Paper says IDs not ID, as we have different uses and personas for our identities. We have many different online personas. The important part is to build on to those identities so that you can be sure that it is the same person coming back.

Financial Services have exemptions from some regulations as they have strong security. If you cannot trust the digital ID with which you have been presented then there is not much point in having one. A number of current best practises are easily circumvented as per Fintech's news yesterday about 2-factor authentication.

We are in an arms race, fighting against an opponent who only needs to win once. Joe Public has to trust in systems in order to use them. Come September 2019 we have the Reg Tech standard and Open Banking going live. This is a new way of managing our money and will be an exciting area going forward. AC did work on testing the Open Banking system and weaknesses need to be addressed by strong ID and authentication.

September also sees SIBOS in London. This is a major showcase for banking technology. We will be the only EU state that can roll out Open Banking, so a good time to beat the drum for the UK as a centre of technology.

On the public private aspect, given that some of the new standards are adopted, we already have the standards coming through to secure the eco-system. Is it more important to secure access to data that the Govt holds on us or a 30 EURO transaction? Surely if I have to go through a security assessment to make an Amazon purchase, surely the same needs to be true for access to Govt services. Digital ID absolutely crucial as is the authentication that underpins it.

What is the liability model for when it goes wrong? You need this to build up trust, all underpinned by standards and regulatory understanding of them. Needs to be kept up to date.

APPG ON DIGITAL ID

Julie Dawson:

Julie drew our attention to page 6 and the recommendation " Recognise approved digital age and identity verification methods on an equal footing with paper based and face-to-face' in particular looking specifically at convenience for consumers.

Just under 1M drivers licence and 400k passports are stolen p.a. In the UK, lost in pubs and clubs as they are the de facto ID document for young folk. We need to see parity between acceptance and enforcement of different types of ID - physical and digital online and offline. The Home Office has launched a digital ID for 3.5m people to prove their right to remain, immigration is a clear area for digital ID.

Strong ID is key to payments as well under Open Banking. The UK will be the first to bring in digital ID for access to pornography and gambling. Heathrow airport is looking at how to use digital ID to improve the journey through the airport. The market is already adopting digital ID in other areas:

Online dating – knowing who you are going to meet is important.

Classified sites – want to protect consumers through a verified profile

Social media sites – to check who is in which area of the site to ensure that children of the right age access the right content.

To enable a vibrant marketplace for Id and innovation there are a few areas that need knitting together. There is a maze of Government departments all working on different parts of the jigsaw. Not an easy landscape.

Soon we will have an audit framework for access to adult content but not decided if this can be used for other areas such as alcohol purchase. Why reinvent the wheel when we should look at parity of systems and schemes across departments.

The FCA sandbox is a good idea. TechUK will be trying to get different sandboxes to work together and internationally. We must remember the consumer in all of this.

The reason that the APPG came together was because Julie met the head of the APPG on Beer who commented about the number of passports found in bars and clubs. Consumers and voters will find a mismatch of approaches difficult and frustrating. Digital identity is both an enabler of our economy (consider right to work and right to rent checks) and also a great export opportunity for the UK.

3) <u>Comments from the floor:</u>

David Happy, 5G expert – for all these things to work we need to think about how to get the service to the device. Core infrastructure is not here and do not have security in IOT to give us confidence. Can speakers reassure him that this is all taken care of.

SP – completely right that it is fundamentally important that people trust and believe in the system. Agrees in part as they do offer an appropriate level of security. There things that can be done now in ways that are good enough. This is about a mindset change, it will be a journey.

APPG ON DIGITAL ID

AC – Cannot give you an assurance but we know the problem. Do we have a perfect solution? Not yet. We have seen what happens when trust is broken.

Derek Wyatt – a wider point, after Brexit my sense Is that we may lose our UN veto to India. That means that we only have soft power not hard power left. Here we have the opportunity, have we thought about framing it in this way?

AC – Digital Trust is a perfect example of soft power. London is the world centre for arbitration so we could expand on this.

JD – we lead the way in data ethics and transparency.

John Bullard – Pleased to see on page 17 a reference to a trust model. With trust goes liability. What happens if it goes wrong? Trust and liability require rules. Does the panel think that private or public law making is the best way forward to govern liability?

AC – Financial Services already control best practice in liability and security standards. That is the way forward.

SP – Having written a couple of trust frameworks (the rule set governing a scheme), these can be complex so we need to be pragmatic.

Paul Simmonds, Global Identity Foundation – supports 95% of the aims of the documents. What are we going to do differently now? If you look at the history of digital ID systems, there are those that have failed, those that have failed spectacularly and those that have survived and struggled on. This last covers Verify

The US had a go at a National Strategy for Trusted Identities in Cyberspace[1] which was sponsored by Barack Obama and failed. Question: why do we want to add another ID system into the mix? What will we do differently?

SP – No simple answer, but does not mean that we do not keep trying. Look at Yoti they are creating use cases and trying to make things work. So is the Post Office. There will be no masterplan, need to encourage people to keep going, recognise the economic and societal value.

JD – Carpe diem, the Digital Economy Act and Financial Services innovations mean that consumers will start to ask why can't I use my ID overall.

PS – Added one more form of digital ID into the system, what are we going to get rid of?

AC – interoperability is key. If you have parity it does not mater if you have a choice of schemes, the market will sort it out. As long as you know the credential will work, that is key.

SP – this is normal life. We still have cheques, why? Will eventually vanish, digital payments are pushing cheques out slowly. It would be ridiculous to not do payments digitally because we have cheques

[1] https://www.nist.gov/itl/tig

APPG ON DIGITAL ID

RM – This question is the next thing we need to address.

Craig Kersey –Some observations on the KYC and AML comments at the bottom of page 7 of the white paper. It is not just large financial institutions that perform KYC and AML checks. Many SMEs ranging from accounting, legal and other professional firms to tech firms seeking investment also perform KYC checks on clients, suppliers, investors etc. Digital ID technology needs to be universally available and solutions need to be built with all users in mind, particularly when it comes to cost.

SP – 5th AML directive will bring more organisations into the fold. There are start-ups working in this space. Sees AML and KYC is adopted by the Fintechs before the banks.

JD – the more we grow the market, the more the cost comes down.

Simon Sabel, Landscape Software – in my business I deal with multiple purchasers for a particular transaction and when one fails an ID check then they are lost in terms of fixing the data to make the deal. Does not seem to be a body to help you with an appeal. How might this be addressed to avoid a sub class of people who fall through the net? The example is people whose names are too long to fit into a standard form and therefore fail the cross-checking..

JD – accessibility is an issue now. Some people have no ID document or device. Arbitration is needed.

Simon Sabel – lack of standards.

Patrick Curry – our organisation has some 20+ groups, 3 running on different aspects of ID. Our work in UK has to connect with eIDAS and the EU Commission (Verify has successfully notified under eIDAS). This document is good for someone coming into this for the first time, but does not reflect demands arising from emerging legislation, significant developments in new technologies and new business requirements.

On the US side there have been a series of initiatives. Whereas Europe has focussed on citizen ID, the US came from an approach for Federal, State and local employees and major regulated industries. The Real ID Act was passed in 2004 but is only just having an impact. For US domestic air travel US citizens need a Real ID compliant driving licence (about 60% are compliant today), and a compliant mobile driving licence app is being developed. The alternative is a US passport for domestic air travel. Internationally, there is a growing trend towards developing compliant mobile driving licences and passports, which is being reflected in ISO standards (ISO/IEC JTC1 SC27).

Lord Holmes' report makes it clear that UK Passport data should be available for validation, not access. We have more passport holders (70M) than any other document. An open debate on Verify would be worthwhile.

We should avoid people having too many documents. There are pilots taking place for those who do not have a Passport or a Verify credential - the "thin file" cases.

Would ask TechUK and the APPG to help foster greater communication and collaboration. How does one work with other bodies?

APPG ON DIGITAL ID

Dave Birch – the issue about using a Yoti or a passport as alternatives is apples and oranges. The bouncer has no idea how to check a passport, it is pointless and the only outcome is lost passports. Wrong to compare using it to a digital ID which is more secure, this is just theatre.

DCMS have come up with a system for people to prove that they are adult by going to Sainsbury to get a code[2]. Export potential?

JD – this creates a market for youngsters to sell these codes. It is also the case that checking passports is theatrical. Too many documents to choose from and bouncers are untrained in reading them.

Diana Biggs, HSBC – number of pilots going on, curious about how the input from all these initiatives can be collated and if there is a general action plan.

RM – TechUk is open to working with all organisations. There is no action plan at the moment. The paper is to engender discussion.

SP – where there are initiatives underway we want them going in the same direction. In Canada they have the Digital ID and Authentication Council which was initiated by the Government as a Public / Private partnership. They have got everyone together in one forum.

JA – the Darwinian principle suggests that we allow these initiatives to develop in whatever direction so the best succeed.

Patrick Curry – our organisation has some 20 groups, 3 running on different aspects of ID. Connected to eIDAS and the EU Commission. This document is good for someone coming into this for the first time. On the US side there have been a series of initiatives Europe has focussed on citizen ID. US came from a federal approach for State employees and major industries. 2004 Real ID Act was passed. For domestic air travel you need a Real ID driving licence. The alternative is a US passport (60% of US people are compliant). Mobile driving licences and passports are being developed.

Lord Holmes' report makes it clear that UK Passport details should be opened for validation. We have more passport holders than any other document. An open debate on Verify would be worthwhile, want to avoid people having too many documents There are pilots taking place for those who do not have a Passport and would therefore fail Verify. Would ask TechUK and the APPG to help foster collaboration. How does one work with other bodies?

Robin Tombs, Yoti – will matters go down a rules basis or a private sector one? Certain regulations forbid certain sectors which mean that area gets left behind which leaves the consumer puzzled. The consumer will begin to use digital ID where they can and that is how momentum starts. Situation is messy due to regulation. Danger is that large companies are able to solve this due to market power and penetration. Messy but will be solved in a few years by big firms leaving them in control and smaller firms pushed out.

[2] http://www.gizmodo.co.uk/2018/09/pornhubs-ageid-is-going-to-let-you-access-porn-with-cards-available-at-your-local-newsagent/

APPG ON DIGITAL ID

Irina Shevsky– couple of mentions of the scope of digital ID (person, company, thing). We need to start to break things down into a better language and talk about them separately. AML checks have a particular set of risk profiles around them for instance when compared to Govt usage or accessing websites. Requirements are all different and a systemic ID solution confuses the issue and is a mistake.

Standards require multi stakeholder investment, how do you compensate for power imbalances? Who pays for it? How does the governance work?

Robin Tombs – risk is that standards take a long time. Consumers can find their way through particular uses which become de facto.

AC – Paypal fraud levels were atrocious when they were founded. They had the investment to fix things and become a market leader.

David Happy – Significant load of funding through bodies like ETSI. Multinationals will go where the money is.

4) <u>Conclusion</u>

JD – We should also commend the US AAMVA Driving License Authority for allowing data checks and hope that DVLA and HMPO follow suit.

AC – Fed Reserve is looking to adopt UK standards.

SP – Let's keep doing this, I know it feels like a talk shop, but let's keep going.

RM – Thanks to everyone for your comments.

JA – it is clear that there is a lot expertise in the room. Must do this again.