APPG ON DIGITAL ID

Meeting: What next to create a healthy Digital ID eco-system in the UK?

19TH June 2019 16.00

Present

Chair: Eddie Hughes MP

Present: Lord Arbuthnot of Erdrom; Lord Lucas of Crudwell

Speakers: Dr Robin Pharoah, Future Agenda; Julie Dawson, Yoti

Speakers

1) Dr Robin Pharoah (RP):

Introductory thoughts: the promise of digital identity is one which is said to lead to cost reductions, saving time on the verification of people and that it can increase cyber security greatly as we know who people are. There is the inclusion promise, giving access to those who do not have the necessary documents. It will lead to new service innovation and brings convenience into a state of affairs that is inconvenient.

What is digital ID and what will it become? No answer to the first question, assumption by many is that they are digitising something that exists in the real world. It will become something different to any notion of identity that we have now. Underestimating digital ID is a huge mistake, it is not some sort of subdomain. It will be what humanity is.

Post-Brexit, sees that the UK could lead on digital ID and play a part globally in its digital future.

There are multiple bets going on in the digital ID space, there are many ways of identifying ourselves online. The ways in which the bets are playing out depend on different factors such as companies believing that "I have a clever solution". Different stakeholders with different priorities are leading to different ways of doing digital ID. Some are unpinned ideologically.

What is the purpose of digital ID? The answer is not a single one. To verify that you are the person who has clicked "agree" to a set of T&Cs. Digital ID is usually about agreeing something and being held to it.

Some different ways these are playing out:

1) Payments are often cited as a route to digital ID as it has a global infrastructure.
2) National ID schemes such as Aadhaar in India through which the Government has taken control and allows for mass interoperability between Govt service. Or Verify in the UK. Totally different in model and formulation.
3) Proxy digital IDs (aka ad hoc ID) – We start to move away from digitising a document as a basis for ID to a collection of different bits of data about us. Many people turn on their location finder so systems know where you live. Amazon knows where you live and Google search information helps to build up a strong identity but this is done unwittingly. The purpose of this proxy ID is different from National ID or payments.

Robin is worried that we may take the path of least resistance. We could allow our IDs to become what Google and Facebook want. It is termed the cost of convenience. The introduction of biometrics starts with looking into the phone to unlock it, are we teaching people to trust facial biometrics?

China's social scoring system uses the eco system of WeChat. T

his is ubiquitous and enables the Govt in China to score citizens and judge them according to their lifestyles. We are seeing this in the UK through Uber, banning drivers with a poor record for instance.

Need to think about privacy and super surveillance, Robin is always curious about the lack of understanding about this. People can remember fewer events than machines, Facebook probably knows who supports which Conservative leadership candidate through the metadata. We ought to be taking this very seriously

That Identity does not have a good history with mankind is another idea e.g. the Holocaust, Rwanda. You never know how attributes will be used in the future and how redress will be handled. Omidyar is seeding a movement called good ID. We need to think about this principle as we build up a system. Can we set a model for the world?

We can learn from bio-ethics, for example reproductive technologies, which have a number of bodies which talk internationally and provide oversight. As ID becomes normalised, many of the technical questions will drop away. The idea of accountability and redress will come to the fore. Strong and robust punishment will be necessary.

Future Agenda deals in 10 year time periods. Identity is a social question and not a technical one. We need to think through what might happen, the first immortal Digital ID probably exists now. IDs being created now for teenagers will last for 80+ years. Is this property? Who has the right to delete it? We need a new ethical principle for data technology – reversibility How can you take back what you have done and / or delete something? Mass deletion should be explored.

Nothing is inevitable, we should not just let things happen to us. We could create a National ID Centre to research this. Regulators when it comes to data are not suitable as the way they approach regulation is not fit for purpose

2) Julie Dawson (JD)

The public sector wants to be able to consume good value, secure age and identity verification at scale, representative across society, including the 24% of adults who do not have photo ID in the UK. **HMT** wants good value as well.

The public are looking for trustworthy, secure ways to prove their age and identity conveniently to do the things they want to do in life, including the 33% of under 18s who do not have photo ID.

The general public aka the taxpayer also wants value for money in terms of what Government is spending.

Citizens /Individuals want convenience, will expect interoperability. Redress options. Consumer bodies involved.

Private sector providers want their digital identity offerings to be usable across the economy - in retail, in financial services, in travel, in health, across Government, in recruitment & right to work, right to rent -across both public and private sector.

Think if you were a VC investing in this space you would want to know that there were places that a digital identity could be consumed; not blocked by legislation.

Landmarks and progress

Landmarks:

EU Settled Status scheme uses a digital identity app for over 3 million people to prove their right to remain - sadly no ' standard published' sadly cannot use the same approach once set up across other areas of the economy…issues Android, IOS

Gauntlet laid down Ed Vaizey - join up more June 2018

TechUK & APPG White paper Feb 2019

> 1 Establish a Government policy to facilitate the creation of a fully functioning digital identity **ecosystem**, which operates across public and private sectors.

> 2 Nominate **one point of contact within Government** charged with leading this policy, in close collaboration with the private sector and full consultation with users.

> 3 Publicly release plans now for the **future development of Gov.UK Verify,** towards the creation of a **framework of standards**, which can be used by all players.

> 4 Provide plans for the further **opening up of Government data** (e.g. DVLA; HMPO; lost, stolen and fraudulently obtained documents, through services such as the Document Checking Service.)

> 5 Enable examinations, membership and utilities bodies to **issue attributes digitally** to enable thin file consumers to build up a track record of their activities: e.g. their qualifications, memberships, employment and paying customer status.

> 6 Recognise approved digital age and identity verification methods on an equal footing with paper based and face-to-face verification. **Consistency** is required in terms of online and offline.

> 7 Set up a new lawful basis for processing biometric data for identity verification and authentication in order to support legislation such as the Digital Economy Act and **recognise that biometrics are being used to increase security and combat fraud.**

8 Nominate a **competent independent authority for digital identity.**

9 Plans should be put in place for government-led **communications** to raise public awareness of the importance of digital identity.

Progress

New GDS Director Lisa Barrett appointed and DCMS Identity team re formed.

May 2019 Dialogue has commenced between DCMS, GDS, supported by techUK, OIX

Private sector companies are engaging in working groups: OIX & TechUK and TISA and APPG

List of the working groups set up:

1   Interoperability
·   Standards: building on the GPG45 framework
·   Biometrics
2. Inclusion
·   To examine alternative methods to support thin-file citizens
·   Broader access to government data.
3. Liability and trust models
4. Alternative architectures for ID
·   This group will look at the pros and cons of federated identity management, self-sovereign identities (with or without distribute ledger technologies) and dynamic attribute exchange.. Interoperability and standards

June 2019 Age Appropriate Design Code consultation

June 12th London Techweek Oliver Dowden announcement

- Consultation to be issued in the coming weeks on how to deliver the **effective organisation of the digital identity market**. Through this consultation the government will **work with industry**, particularly with sectors who have frequent user identity interactions, to ensure **inter-operable 'rules of the road' for identity**
- The creation of a **new Digital Identity Unit**, which is a collaboration between DCMS and Cabinet Office. The Unit will help bring the public and private sector together, ensure the adoption of interoperable standards, specification and schemes, and deliver on the outcome of the consultation
- The start of engagement on the commercial framework for consuming digital identities from the private sector for the period from April 2020 to ensure the continued delivery of public services. (read Universal Credit) GDS will continue to ensure alignment of commercial models that are adopted by the developing identity market to build a flourishing ecosystem that delivers value for everyone.

APPG ON DIGITAL ID

July 2019 Digital Economy Act - no adult activities please we're British

What can the APPG do to help advance matters?

Still to happen

- Clarity as to what will happen in spring 2020 with Verify
- Clarity as to timeline for opening up of Document Checking System
- RECOGNITION OF PARITY across sectors - sandboxing ahead
- ISSUANCE of ATTRIBUTES, verifiable claims
- Redress, oversight, governance, accessibility

<u>Open discussion</u>

Mark King – Two questions: What has happened in Scotland? Secondly, there have been some very damaging reports recently but the policies have not really changed and many have dropped out as they have not found the ROI. Moreover March 2020 is the date by which systems will be in place.

JD – Quite a bit of work between the Scottish Government and the Improvement Service. Steve Pannifer who works on the project confirmed that the minutes and blog are shared regularly. Over the last 6 months have undertaken an exercise to build a proof of concept demo. The OIX will report within three weeks.

As regards the consultation period, the team at the DCMS has said that they need to bring on board other Govt departments, hence the consultation that is due soon.

In terms of investing, the work is taking place.

MK - TScheme has not got the facility to deal with the work and the question of who is paying or what is key is unanswered. We don't have anything that we can recognise as a market. We are getting conflicting information from the Civil service about interoperability with Europe

John Bullard – have been involved in this for more than 10 years. The UK has an obligation to become the Greenwich Meridian of global trust. We are in the right place, have the right language, Common Law and the right, clever people. This should be owned by Number Ten.

EH – no reason why we should not do this. We have the enthusiasm and the intellectual basis. Somethings are just of their time and this is one of them.

Geoff Goodell, UCL London - Identity is a collection of transactions and attributes that are bound to each other. When we reveal data to the Internet we should be aware of what is happening. Seems to be a preponderance of interest in building identifies in this way. We need to link the higher the insurance of the identity to a more limited use case. We should not have a single ID as this leads to control. Should not use high assurance credentials for lesser transactions.

APPG ON DIGITAL ID

RP – push back on the idea of transactions creating an identity, example: a digital ID may not be the same ID that someone uses for their gender orientation. Also cited changing your name by deed poll which is self-regulating.

JD – different approaches – financial services leave a trail behind. In terms of ID platforms you can have a non-relational database at the core. This can be set up from the outset so that the attributes are stored separately and the access to that data is controlled by the user.

Paul Simmonds, GIF – if you don't learn from history you are doomed to repeat it. The past 20 years is littered with examples of failed global and national systems. We are repeating the same old stuff that has failed. Need to understand why things failed. Two key ones:

1) 100% anonymity at the root of an identity
2) Identity has to work across people, companies, things, agents and code

JD – Facebook – people chose to build on this and many people would use this as their preferred ID.

PS – our duty is to build a better system with more privacy and functionality. It is up to us as an industry to do this.

SP – Scotland has a vision but lack the products and the services that will help to get there. The result this year may be simplistic but will take us on the journey.

GG – collective action needs a response from the Govt

PS – part of a global economy so we need to bring the world with us. Danger that a system becomes a zombie system used by a few people. Online tax offers five ways to identify ourselves. How do we reduce this number?

Craig Kersey – it is a pain when you are filing tax returns for a number of people.

Robin Pharoah – firstly you talk about the need for a globally interoperable system, so what about China? PS - A UK system will need to interoperate with China, US etc.

Singapore is moving towards a solution to counter WeChat.

Anonymity and privacy from the outset was mentioned by PS. Anonymity and ID are counter each other. How can you vote anonymously but prove that you voted. In NZ your voting record is tied to access to Govt services. MK – the point of compulsory voting in Australia was to make sure that people could not be coerced to stay at home and not vote.

Geoff Llewellyn – Been involved since 2002 in ID. RP said that we are not sure what identity is? What is wrong with the proposition that a unique biometric identity can be linked to a digital signature? Fan of iris recognition.

RP – what the biometric is associating to is the problem.

PS – you can subvert an iris. Many systems rely on matching the iris in the eye to a database for checking.

APPG ON DIGITAL ID

SP – if you think about identification as one of the results you want from a digital ID scheme, one way to do this is to do something biometric. The fingerprint on my device might be appropriate in a certain context. Can we establish language around what the functional components are and in this context what might be appropriate?

RP – not having solved identity means: socially speaking there is no agreement on who a person is. We can agree a physical piece of material in space.

GL – isn't there a benefit to identifying a certain human being with a digital trace. What about redress, that is where Government comes in

GG – might be benefits but there are grave risks with having a root to everything as you are undermining human autonomy. Why link everything I do to biometrics?

SP – if you can link attributes etc back to a physical person then some transactions do not need major ID.

MK – In the UK we do not use identity in a way other people do.

Lord Arbuthnot – this period of peace which we have had is an anomaly. We are benign at the moment, how long will it last? Need to be very careful about giving powers to the State.

David Rennie – have to have a governance model approved by the state and underpinned by the rule of law.

Robin Tombs – firms like Google or Alipay will offer consumers an easy ID that they will take up and when a few hundred million people will have adopted this then the market will have gone a certain way. The governance will be run through these organisations. Danger that the big players become inevitable.

Nicky Hickman – two reasons for ID: access control and service personalisation.

You mentioned that companies should be sanctioned and rewarded. How would the rewarding work?

RP – the reward would be the ability to offer services

NH – people do not pay for identity, they pay for services or access. Need to understand how people make money.

RP – are you talking about the money to set up a scheme or run it?

NH – it is the ongoing business case for companies offering ID in the commercial world that is difficult.

RP – possible to think of a world in which people do pay for services Think of the world of gaming, some are free and others are paid for games. When people understand the cost of giving away data, then they might pay for it.

RT – role of the State to ensure that anyone in society can participate.

APPG ON DIGITAL ID

JD – in the UK we going to be in the spotlight globally for access to pornography and gambling as age verification will come in. There is a lot of scrutiny as to how organisations will enable people to prove their age to access services.

NH – really important to address this.

RP – technology changes our behaviour in different ways. Fascinated that identity is one of the most complex areas of human life, we will see an enormous amount of innovation taking place. People will learn about VPNs, ToR etc. Appl's new ID offering promotes obfuscation and will promote this sort of behaviour.

RT – role of regulators to be smart. BBFC were aware that age estimation was coming along when they wrote the regulations. UK firms are denied innovation and a home market because regulators are not regulating smartly.

Conclusion: Eddie Hughes MP: new and exciting. Let's push the Govt in the right direction.