The Money Charity Response – DCMS-Cabinet Office Digital Identity Call for Evidence (September 2019)

The Money Charity is a financial capability charity whose vision is to empower people across the UK to build the skills, knowledge, attitudes and behaviours to make the most of their money throughout their lives.[1]

We welcome the opportunity to respond to the Digital Identity Call for Evidence issued in July 2019. This is a call for evidence that raises a wide range of issues relating to digital identity, digital business, government and the digital world in general. We will focus on the financial capability aspects we have observed in our financial capability work, in particular on inclusion and public confidence in a digital ID.

Needs and problems (Questions 1, 2, 3 and 6)

In principle, we support the concept of a digital ID. We see and hear about many of the inconveniences arising from analogue ID systems, for example:

- Misalignment of ID processes within a single organisation, for example the digital/online banking side running smoothly, while consumers have to present in

[1] See box on back page.

person multiple paper documents in order to complete an application for a mortgage or to open an account.

- In application processes, banks rejecting print-outs from some online systems of other companies, though they themselves have stopped sending paper statements and encourage their customers to bank online.
- A consumer having to re-identify themselves to their bank when requesting the bank to confirm their identity to another bank for money transfer purposes.
- Firms taking an inconsistent or too strict an approach to alternative documentation when customers do not have passports or drivers licences.

Banks and other firms have conflicting incentives. They have service aspirations but also a desire to reduce costs via digitisation. They would like to create an easy customer journey but have a statutory and commercial need to 'know their customer' in order to bear down on fraud, money laundering, cybercrime, etc.

In principle a digital ID could simplify and speed up the process of confirming identity, enabling a consumer to complete application and other processes in a single visit or remotely via Internet and mobile technology. In aggregate, this could sum to a large cost saving to individuals and the economy. We say 'in principle' however in order not to minimise the considerable practical challenges in establishing an effective digital ID that would win public trust.

Inclusion (Question 4)

In our financial capability work we meet individuals and groups with a wide range of financial, digital and other capabilities, including people in marginalised and/or vulnerable situations such as Travellers, migrants, refugees and offenders. Some people would adapt quickly to using a digital ID, but others would find it challenging and intimidating. For example, as DCMS and Cabinet Office will be aware, in 2019, 1.94 million households do not have access to the Internet, including 27% of one adult households aged 65 and over.[2] According to Ofcom, 79% of UK adults in 2019 used a smartphone,[3] but this leaves 11.1 million adults still not using a smartphone.

For this reason it is essential that use of a digital ID be voluntary, not compulsory. This means not just technically voluntary, but practically voluntary as well, ie not presented with conditions of access that make setting up a digital ID de facto compulsory.

Those who wish to continue to ID themselves by traditional means should have the right to do so.

[2] The Money Charity, *The Money Statistics September 2019*, page 17, quoting ONS data.

[3] Ofcom 2019, *Communications Market Report*, page 4.

Trust (Question 7)

A key aspect of establishing trust is creating a digital and Internet environment in the UK that people can have confidence in. This is still not the case. Key issues are:

- The high rate of cyber-crime (fraud, scams, hacking etc)
- Misuse of data by large companies, such as in the Facebook-Cambridge Analytica scandal.
- Accidental data breaches.
- On-selling of data in ways that are not transparent to consumers.
- IT meltdowns.

The vulnerability of people to cyber-crime is a particular challenge for digital ID systems, because cyber-crime frequently targets identity, for example when scammers pose as banks, police officers or legitimate firms to lure members of the public into transferring money into accounts controlled by cyber-criminals.

The UK police and other law enforcement agencies do not yet appear to have got to grips with the burgeoning field of cyber-crime. For the public to place their confidence in a digital ID system, there needs to be a step-change in the performance of law enforcement in intercepting cybercrime and catching and prosecuting cyber criminals. This is a vital foundation for our present and future digital economy.

The digital ID activation path (Question 7)

A related challenge arises from the way the consumer will grant access to their digital ID. In the analogue world, a person presents certain documents (a passport, a drivers' licence, bank statements, etc) face-to-face, so the receiving firm or agency can both check the documents and the person presenting them, for example by comparing the photo on a document with the person in front of them, asking questions, seeking further information etc.

In the digital world, this second check is removed and replaced with a person (not visible to the firm or agency) entering a password and/or other access details. Or, vice versa, a firm or agency presenting itself to the consumer via a web page or email, without the consumer being able to make a bricks-and-mortar check of the identity of the firm or agency.

This is a weak point in the system, which is being exploited by scammers, fraudsters and/or abusers. For example, a relative, carer or 'friend' of a person with dementia accessing their digital ID in order to steal money, sell property or carry out other financial transactions without authorisation.

The designers of the digital ID system need to come up with a solution for this point of weakness in the system. Again, this is a matter of public confidence. If people feel it will be too easy for their digital ID to be accessed without their consent, they will protect themselves by not setting one up.

Privacy (Question 9)

A key issue for consumers is that their digital ID is secure and not being accessed for purposes other than intended. In particular, there needs to be assurance that:

- Whoever holds the record of the digital ID is completely reliable and will not release any part of it other than as authorised by the consumer whose identity it is.
- The ID is not going to be exploited commercially, for example by being on-sold in some form.
- The ID is not going to be used by state authorities for purposes other than the consumer providing their digital ID in order to access a service.

Given the range of data abuses that have already come into the public domain (the Facebook-Cambridge Analytica scandal, the Snowden papers, etc) and techniques known to be under development in the UK and internationally,[4] it will take some effort to assure the public that their ID profiles will not be used in surprising ways or by actors not authorised by the consumer to use their information.

We recommend that DCMS and Cabinet Office pay particular attention to this issue.

One of the challenges is the amplification of perceived risk caused by the availability bias: a single event (eg a data breach, a hack, an unauthorised sharing) has a disproportionate effect on the public's attitude to a certain activity, because people generalise from available information rather than making statistical assessments.[5] The airline industry realised this some decades ago and it became one of the drivers of improved air safety, with the result that the risk of death in an air crash is now extremely small: in 2018, there was one fatal air accident for every three million flights. In 2017, it was one in 18 million.[6] This means that when getting on a flight in 2017, a passenger had a 99.999994% chance of not being involved in a fatal accident. Conversely, two crashes of the Boeing 737 MAX plane have led to the prolonged grounding of all 737 MAXs, at huge cost to Boeing and the airline industry.

[4] For example, face recognition technology being developed by police forces, the 'social credit' surveillance and assessment system being developed by China.

[5] Daniel Kahneman 2012, *Thinking, Fast and Slow*, pp 142-144.

[6] https://www.theguardian.com/world/2019/jan/02/plane-crash-deaths-jump-sharply-in-2018-but-fatalities-still-rare

At present, and reflecting the relatively immature stage of its development, Internet safety feels more like a game of Russian roulette than taking a flight on a commercial airliner. The digital industry needs to aim for a much higher rate of cyber security than it currently achieves. This applies to digital ID most of all, where a very few lapses could kill public confidence completely.

The role of government (Question 19)

The government has a particular challenge in leading the creation of digital ID, in that from the point of view of the consumer, it has potentially conflicting motivations:

- It wishes to set up a digital ID system for the benefit of consumers, firms and agencies.
- It wishes to surveille UK residents and visitors for the purposes of preventing crime and terrorism.
- It wishes to enforce rules relating to tax liability, benefit entitlement and other aspects of the financial relationship between the citizen and the state.
- Some people within the governmental system may be interested in the political behaviour of UK residents as revealed by their digital footprints.

It was not helpful, for example, when the media reported in September 2019 that a senior political aide (not a career civil servant) had ordered that ‘targeted and personalised information from Gov.uk be gathered, analysed and fed back actively to support key decision-making’ in relation to the government’s Brexit preparations. This type of request sets off alarm bells –whether justified or not – in the public’s mind and undermines promises of data security that are routinely made on government websites.

Officials were reported to have responded that ‘anonymised user data currently collected by individual departments will now be collated across the Gov.uk website, allowing better information on how the site is used as a whole.’[7] But this response does not make clear whether it is an exercise in combining statistics, or involves linking different datasets using unique personal identifiers and then summarising the results.

The idea that one’s digital ID might be linked to other government datasets without authorisation (or perhaps with a blanket ‘authorisation’, required as a condition of access to the service, the way tech firms get users to accept their terms and conditions) undermines the promise of data privacy and security.

To counter this, the government needs to pass strong legislation placing digital ID in a ‘hermetically sealed’ digital location assuring that use of the ID can only be activated by

[7] https://www.theguardian.com/world/2019/sep/10/no-10-request-user-data-government-website-sparks-alarm

authorisation of the consumer whose ID it is. If digital IDs are to be provided by private sector digital Identity Providers (IDPs), then they too need to be subject to strong legislation, with convincing enforcement.

The Money Charity is the UK's financial capability charity providing education, information, advice and guidance to all.

We believe that everyone achieves financial wellbeing by managing money well. We empower people across the UK to build the skills, knowledge, attitudes and behaviours to make the most of their money throughout their lives, helping them achieve their goals and live a happier, more positive life as a result.

We do this by developing and delivering products and services which provide education, information and advice on money matters for those in the workplace, in our communities, and in education, as well as through influencing and supporting others to promote financial capability and financial wellbeing through consultancy, policy, research and media work.

We have a 'can-do' attitude, finding solutions to meet the needs of our clients, partners, funders and stakeholders.

Tel: 020 7062 8933

hello@themoneycharity.org.uk

https://themoneycharity.org.uk/