FUTURE AGENDA

Open Foresight

FUTURE OF DIGITAL IDENTITY

Insights from Multiple Expert Discussions Around the World

FUTURE AGENDA

Open Foresight

FUTURE OF DIGITAL IDENTITY

Insights from Multiple Expert Discussions Around the World

Conclusion

Digital identity is a complex idea, but that should not dissuade us from exploring its potential to transform our collective digital futures for the better. Even the immediate promise that interoperable Digital ID systems could allow us safe, secure and reliable passage through digital spaces and digital interactions and transactions is tantalising.

We are still in the early days of the human digital transformation and almost certainly do not yet have a grasp of how truly fundamental an understanding of digital identities will be to the future human experience. Digital ID, today understood as the slightly narrower aspect of digital identity related to the question of how we can prove that we *are who we say we are,* will likely become the primary mechanism through which we construct our digital selves and engage with and inhabit tomorrow's digital spaces. It could be the key to unlocking the true value behind "Big Data", providing unstructured data-sets with meaning and context, as well as providing the means by which we can all benefit from that. Similarly, the technologies and protocols associated with the development of Digital ID systems could become the pivot points for paradigmatic shifts in our digital society, rebalancing control over the data stream in favour of the individual, or opening us up to new mechanisms of social control.

We conclude with a summary of those areas of the Digital ID landscape and debate that are likely to provide the pivot-points for pathways toward the future. Given the number of different bets that are being placed, we cannot be sure if any (or even all) possible future realisations will come to pass, but we point to these crucial sites of decision as being the moments at which pathways will diverge. Digital ID stakeholders will make decisions related to them in different ways (including by omission), and for different reasons, but each will eventually have to confront the implications of them.

Collective purpose. For all the technical challenges behind the building of truly interoperable Digital ID systems, the challenge of defining their purpose will need to be met even earlier. The standards and protocols that emerge to allow the development of large-scale Digital ID eco-systems, will emerge thanks to their fitness to serve that purpose, so the need to tackle the question of exactly what it is, is urgent. Does Digital ID serve a mass-market consumer need around convenience? Is Digital ID necessary to unlock a wave of future digital innovation in financial and other services? Or is the primary purpose of Digital ID to rebalance the locus of power in a data-driven world? Is it the answer to societal exclusion? Or to the question of data ownership? Is it just a 'nice to have'? Can different stakeholders recognise a common purpose, or are they doomed to argue solely from within their niche?

Despite the fire and heat in much of today's current debates about implementation (centralised vs. decentralised, security and accountability vs. privacy, zero-knowledge principles and sovereignty etc.) the questions are most likely to be resolved by the resolutions made around this question of purpose. The loudest voices in the argument are likely to be consumers/users/citizens, commercial providers and governments. Their aims and goals today may not always coincide, and, in the case of end-users, may not yet be loud enough. Those stakeholders that are able to find a common thread between these competing interests, are likely to have the largest stake in defining and owning the future of Digital ID.

Agency and control. The precise mechanisms of agency and control that holders of Digital IDs come to have over their data, will matter. Small differences between different stakeholders' approaches to, for example, the collection of meta-data associated with Digital ID transactions, the implementations of consent management, the right to be forgotten, or to withdraw consent, the ability to travel in digital spaces incognito etc. may seem trivial today, but could have long-term consequences for the future of humanity. Different implementations have a number of different technical advantages and drawbacks today, but in the longer term, it is their effect on this aspect of Digital ID that is likely to matter most.

Flexibility and reversibility. Whether it be the need to incorporate a changing set of digital ethics and rights, the effects of unknown and unintended outcomes, the ways in which users adapt and innovate around the use of Digital IDs, or the impacts of devastating cyber-attacks; those Digital ID systems that are designed today to adapt to and accommodate change in the future, will likely prove the most resilient.

Collaboration. Truly interoperable Digital ID systems will require collaboration between different stakeholders from different sectors and cultural spheres. The strongest alliances and partnerships will be those that incorporate multiple different voices and in which the needs and achievements of one partner are recognised and understood by all.

The solutions we find to the difficult questions around Digital ID today could have far-reaching and long-term consequences that are difficult to envisage from where we stand now.

The Killer-App. Whilst the most obvious use-cases for Digital ID are easy to articulate ('a digital ID card'), a single 'killer app' that will drive investment into the development of a large-scale, interoperable Digital ID eco-system or mass user-adoption, is yet to be identified. Today there are still gaps perhaps in the understanding of how the various different capabilities of a Digital ID can meet genuine consumer, user and citizen need and demand. A single compelling use case may help to bridge this gap in a meaningful way, and could well provide a catalyst to collective action. It is worth remembering that Digital IDs can achieve multiple 'big' things all at once, from easing commercial transactions and enhancing digital security to providing transparency during data transactions; but the articulation of these benefits may need to be applied to more mundane and every day behaviours, or in small-scale, instantly recognisable user-rewards. As Digital ID moves ever closer to the boundary between being a technical challenge and a social one, the focus on the end user may need to be brought to the fore.

The solutions we find to the difficult questions around Digital ID today could have far-reaching and long-term consequences that are difficult to envisage from where we stand now; one foot still planted in an analogue world.

The key questions

Below we list some of the questions for society, regulators, stakeholders, and individuals in relation to the issues raised in this paper.

Some Key Questions for Digital ID Stakeholders:

Who are the other key digital identity stakeholders that can help enable our vision?

What role do we wish to play in the identity ecosystem?

How should we understand the purpose of Digital ID and how do we build to reflect that?

How does personal data mesh with machine data?

What is our ethical position regarding digital identity?

How can we contribute to the prevention of unintended and negative long-term consequences?

Some Key Questions for Individuals and Society:

How can my personal digital information facilitate my life?

How will I manage my digital attributes?

Who do I trust to help me do this?

Do I want my personal data to help society?

What are my digital rights and who protects them?

When do I want and need to be identified and when can I remain anonymous?

How can I better understand the role my data plays in a digital society and economy?

Some Key Questions for Industry:

In a world of Digital ID, will customers still want to share data with us?

How will we ensure that we are 'trustworthy'?

What data do we need to collect in the future?

How will we be able to comply when customers assert digital rights?

Can we develop new, privacy-preserving customer propositions?

What potential new products and services does widespread adoption of Digital ID unlock?

How can we benefit from increased cyber-security and better accountability in digital transactions?

Do we need to understand the impacts of Digital ID on our business models better?

Some Key Questions for Government and Regulators:

Would a government mandate around Digital ID help to accelerate the benefits of a secure and interoperable ID system?

How should we properly regulate Digital ID systems, and how can we ensure we create a dynamic and responsive regulatory environment for Digital ID going forward?

What kind of identity ecosystem do we wish to support?

What role will Government data about individuals play?

How can we ensure that digital identity benefits all of society?

How do we ensure that no citizen is excluded?

What steps must we take to prevent unintended consequences?

How can we think about the ethics of digital identity early?

How can access to and delivery of public services be improved by widespread adoption of Digital ID?

References

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[2] We clarify the use of different terms related to digital identity, such as 'Digital ID, in the next chapter.

[3] https://www.chathamhouse.org/chatham-house-rule

[4] https://www.libertyglobal.com/wp-content/uploads/2017/06/The-Value-of-Our-Digital-Identity.pdf

[5] Ibid., p36

[6] The BCG report does in fact recognise the importance of the relationship between personal data and a real person, but sees it as largely being about a trade-off between consumer privacy and the ability of service providers to personalise (and therefore further monetise) their services.

[7] Or, as pointed out by one of our workshop participants, that it is the same person who has agreed to a set of terms and conditions when they first made an 'account'.

[8] Cf. "The Presentation of Self in Everyday Life" (Goffman, 1956)

[9] This somewhat innocuous and amusing news story, shows how a failure in passport authentication led an airline to make a robust public defence of its entire approach to security and safety: https://www.independent.co.uk/travel/news-and-advice/klm-flight-airline-passport-friend-prague-amsterdam-newcastle-airport-security-a8789481.html Digital ID of course, should make situations like this a thing of the past.

[10] https://en.wikipedia.org/wiki/Know_your_customer

[11] https://worldpaymentsreport.com/

[12] http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

[13] https://sustainabledevelopment.un.org/sdg16 Target 16.9 "By 2030, provide legal identity for all, including birth registration"

[14] http://www.undp.org/content/undp/en/home/blog/2017/6/1/Moving-towards-digital-technology-for-legal-identity.html

[15] https://www.experian.com/assets/decision-analytics/reports/global-fraud-report-2018.pdf

[16] To give an idea of the scale of the problem, at the time of writing, cyber-security blogger Troy Hunt's https://haveibeenpwned.com/ project currently hosts details of at least 6,931,949,148 individual identity credential thefts. The number will be higher at the time of reading.

[17] For more detail see https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market investigation-full-final-report.pdf

[18] For a more detailed discussion of the concept of interoperability in relation to Digital ID, see https://cyber.harvard.edu interop/pdfs/interop-digital-id.pdf

[19] http://www.undp.org/content/undp/en/home/blog/2017/6/1/Moving-towards-digital-technology-for-legal-identity.html

[20] This report from Caribou Digital produced in partnership with the Omidyar Network illustrates the complexity of the Digital ID marketplace in 2016. The landscape has only become more complicated since: http://cariboudigital.net/new/wp-content/uploads/2016/08/Caribou-Digitial-Omidyar-Network-Private-Sector-Digital-Identity-In-Emerging-Markets.pdf "Private Sector Digital Identity In Emerging Markets" (Caribou Digital Publishing, 2016)

[21] We fully accept that many of the concepts we introduce deserve deeper consideration.

[22] We have deliberately included attributes that might be more or less socially contentious to illustrate that the term 'attribute' itself is neutral as to what they might consist of.

[23] The idea is expanded on here https://medium.com/mydex/unleashing-the-potential-of-verified-attributes-fe001e01b091 "While all individuals and almost all organisations would benefit greatly if a wide range of verified attributes were available for quick, easy, safe sharing and checking there is no immediate particular benefit to any single attribute provider to incur the costs of providing citizens/customers with these verified attributes about themselves."

[24] Specifically, we explore potential user benefits with regard to personal cyber-security, privacy and the ability to exercise more control over the flow of personal data, even the ability to exercise 'data rights', later in the report.

[25] http://cariboudigital.net/new/wp-content/uploads/2016/08/Caribou-Digitial-Omidyar-Network-Private-Sector-Digital-Identity-In-Emerging-Markets.pdf (2016)

[26] https://gizmodo.com/facebook-is-giving-advertisers-access-to-your-shadow-co-1828476051

[27] For an example of the kinds of ambitions around identity and self-sovereignty see for example https://medium.com/lifeid/lifeid-self-sovereign-identity-bill-of-rights-d2acafa1de8b

[28] Here we are in danger of being too casual with philosophical, anthropological and social-psychological theories of 'self'. In the interests of brevity and readability we have made the decision to simply assert that the purpose of Digital ID and also the broader idea of 'identity' itself, are fundamentally social constructs and concepts. For further references it may be worth starting here https://en.wikipedia.org/wiki/Intersubjectivity

[29] For a fuller and more technical discussion of all that we have introduced here see https://bitsonblocks.net/2017/05/17 gentle-introduction-self-sovereign-identity/ and "The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them" (Lewis, 2018)

[30] In the next section, we take this a step further to explore how future Digital ID implementations could move on to become fully-fledged consent and privacy managers

[31] One point worth remembering here is that use of a Digital ID, thanks to the greater privacy afforded by the translation of personal attributes into anonymised entitlements, greatly reduces the number of sensitive personal data points that organisations need to store and maintain, reducing liabilities under laws and regulations such as those laid out in the EU's GDPR.

[32] Consider for example the efforts being made around the ethical development of AI at places like Oxford University https://www.cs.ox.ac.uk/efai/ or the Ada Lovelace institute https://www.adalovelaceinstitute.or/

[33] Arguments are already being made in this regard. For a clearer articulation of the arguments, see for example: "Digital Citizenship and the Right to Digital Identity Under International Law" (Sullivan, 2015) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2519806

[34] The report and data presents economy-level aggregates on the share and number of the population without a foundational/national ID, based on surveys covering over 100,000 people in 99 economies—representing 74 percent of the world's population.

[35] With the emergence perhaps, at least in the short term, of different kinds of Digital ID attribute collection and verification based on for example, the corroboration of peers, behavioural data and even self-assertion (up to a point).

[36] https://www.eff.org/deeplinks/2018/02/can-indias-aadhaar-biometric-identity-program-be-fixed

[37] See here for a longer version of this argument https://hbr.org/2017/11/how-india-is-moving-toward-a-digital-first economy

[38] See for example the argument over blinding being made here https://diacc.ca/wp-content/uploads/2017/02/Consumer-Digital-Identity-Companion-Paper.pdf or the kinds of claims and promises being made here https://spideroak.com/no-knowledge/

[39] We do recognise that there are also genuine attempts to develop the use of ZKPs in Digital ID protocols, see for example https://www.itu.int/dms_pub/itu-t/oth/06/04/T06040040040001PDFE.pdf and https://digify.com/a/#/view/55d40168f67c4676bed9e49ed99832fc

[40] ThreatMatrix, Q2 2018 Cybercrime Report and is based on actual cybercrime attacks from April – June 2018.

[41] We recognise that 'digital identities' and 'digital identity' technologies have always been on the front line of cyber security, criminality and attack, but here we are specifically referring to emergent forms of digital identity, i.e. 'Digital IDs', as becoming a new frontline.

[42] We refer to this example later in the report but it is worth mentioning here. As the cyber-security writer Bruce Schneier put it after the theft of biometrics in the OPM data breach: *"…many systems don't store the biometric data at all, only a mathematical function of the data that can be used for authentication but can't be used to reconstruct the actual biometric. Unfortunately, OPM stored copies of actual fingerprints."*

[43] For examples see https://en.wikipedia.org/wiki/EIDAS or https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2DjfY standards could also emerge from de facto commercially driven identity systems

[44] See for example https://www.dataversity.net/rwdg-slides-three-approaches-data-stewardship/

[45] See for example https://cordis.europa.eu/project/rcn/88243/reporting/en

[46] AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations, Minds and Machines (2018) 28:689–707; November 2018. In the paper, the authors cite the four bio-ethic principles of Beneficence, Non-maleficence, Autonomy and Justice as representative of a range of recommended AI ethics from other sources and then add the fifth principle of Explicability.

[47] http://nuffieldbioethics.org/wp-content/uploads/Biological_and_health_data_web.pdf

[48] https://en.unesco.org/news/unesco-panel-experts-calls-ban-editing-human-dna-avoid-unethical-tampering-hereditary traits

[48] https://id2020.org/

[50] https://www.omidyar.com/blog/launching-good-id-dialogues

[51] https://www.eff.org/

[52] https://theodi.org/article/exploring-good-common-principles-for-a-digital-identity-system/

[53] https://www.internetsociety.org/issues/identity/

[54] The old adage that 'if the service is free then you are the product'.

[55] https://en.wikipedia.org/wiki/Social_Credit_System

[56] See for example, https://securekey.com/wp-content/uploads/2017/07/SecureKey_Whitepaper_Telecom_FINAL Feb2018.pdf

[57] https://auspostenterprise.com.au/content/dam/corp/ent-gov/documents/digital-identity-white-paper.pdf

[58] https://www.gemalto.com/govt/identity/5-reasons-electronic-national-id-card

[59] https://id4d.worldbank.org/

[60] https://www.omidyar.com/our-work/digital-identity

[61] https://fidoalliance.org/

[62] https://ipfs.io/

[63] https://www.inrupt.com/

[64] There is some surprisingly early precedent for this in the form of European driving licenses https://europa.eu/youreurope/citizens/vehicles/driving-licence/driving-licence-recognition-validity/index_en.htm and the APEC business travel card https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Business-Mobility-Group/ABTC

[65] See for example https://factordaily.com/aadhaar-india-stack-export/

[66] As in non-digital spaces, this will only ever be a 'measure' of control. We would be unlikely to have full control of the ways in which we are understood in digital spaces, just as we do not have full control over others' perceptions of us in the offline world.

[67] For a journalistic account, see https://www.engadget.com/2016/03/04/multiple-online-identities/

[68] https://en.wikipedia.org/wiki/Usenet

[69] Interestingly, the idea of a digital or internet 'sockpuppet', a deliberately false identity used to manipulate discussions, were also among the earliest forms of digital identity https://en.wikipedia.org/wiki/Sockpuppet_(Internet)

[70] These need not be physically close communities such as neighbourhoods or villages. It could include 'communities of interest' that are 'local' in the sense of being self-contained.

[71] An analogy here might the way in which former employers provide personal references for job-seekers. Whilst general characteristics are always sought by prospective new employers, a reference from a similar employer, in an industry they know well, is likely to have more meaning. The 'further away' the industry supplying the reference is to the new employer's industry, the less meaningful and therefore 'trustworthy' as a verification of the job-seeker's skills it becomes.

[72] The World Economics Forum's "Global Risks Report 2019" outlines these scenarios in more detail and suggests that large-scale data crime and cyber-attack are among the more likely risk scenarios https://www.zurich com/_/media/dbe/corporate/knowledge/docs/the-global-risks-report-2019-executive-summarypdf?la=en&hash=6B7B 3A8BAC42C7DA05C33D7B914D46256D17B00

[73] "Dawn of the Code War" (Carlin, 2018)

[74] https://e-estonia.com/estonia-to-open-the-worlds-first-data-embassy-in-luxembourg/

[75] https://www.hindustantimes.com/tech/aadhaar-breach-everything-you-need-to-know/story-VhCKHDIL8lziw6OcnhL4wO html

[76] https://en.wikipedia.org/wiki/Commission_on_Elections_data_breach

[77] https://en.wikipedia.org/wiki/Office_of_Personnel_Management_data_breach

[78] https://en.wikipedia.org/wiki/Equifax

[79] https://newsroom.fb.com/news/2018/09/security-update/

[80] https://www.blog.google/technology/safety-security/project-strobe/

[81] https://www.schneier.com/essays/archives/2015/09/stealing_fingerprint.html

Contact details

To discuss this project further please get in touch

Dr. Robin Pharoah

Director | Global Insights

Future Agenda

robin.pharoah@futureagenda.org

www.futureagenda.org

@futureagenda

FUTURE AGENDA

Open Foresight