The Alan Turing Institute

Workshop report

Researching digital identity in times of crisis

August 2021

Authors

Aaron Martin, Postdoctoral Research Fellow, Tilburg Institute for Law, Technology, and Society

Emrys Schoemaker, Research Director, Caribou Digital and Visiting Fellow, London School of Economics

Keren Weitzberg, Lecturer (Teaching), Department of History and Visiting Research Fellow, Institute of Advanced Studies, University College London

Margie Cheesman, DPhil Researcher, Oxford Internet Institute

Illustrations by Katie Chapell generated live during the workshop

This work was supported, in whole or in part, by the Bill & Melinda Gates Foundation [INV-001309].

The Institute is named in honour of Alan Turing, whose pioneering work in theoretical and applied mathematics, engineering and computing is considered to have laid the foundations for modern-day data science and artificial intelligence. It was established in 2015 by five founding universities and became the United Kingdom's (UK) National Institute for Data Science and Artificial Intelligence. Today, the Turing brings together academics from 13 of the UK's leading universities and hosts visiting fellows and researchers from many international centres of academic excellence. The Turing also liaises with public bodies and is supported by collaborations with major organisations.

The Alan Turing Institute
British Library
96 Euston Road
London
NW1 2DB

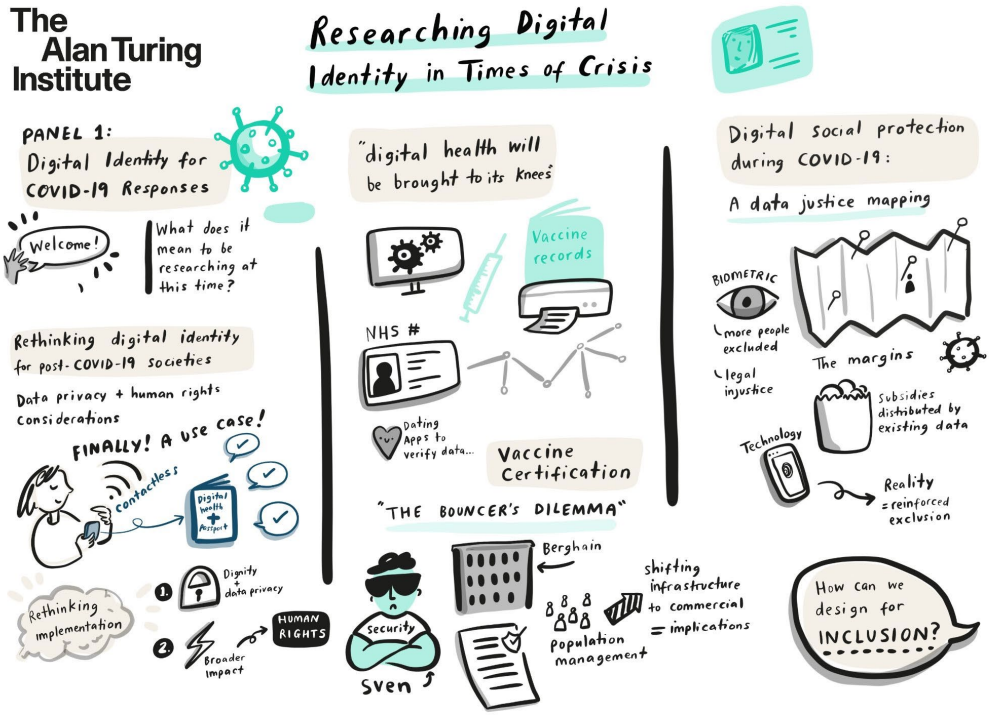
Table of contents

1 A critical research agenda

Digital identity—already a fascination of government and aid actors for many years—has taken on a renewed significance during the pandemic, particularly as different initiatives are emerging internationally to leverage digital and mobile platforms for vaccine certification and immunity passports.

As scholars interested in understanding *why* and *how* technologies and platforms for digital identity, including those based on biometrics, are being applied to address development and humanitarian challenges, a primary concern for us over the past year has been assessing the implications of the ongoing crisis for digital identity in aid: in what ways has the pandemic reconfigured the motives for, and technologies underpinning, digital identity implementations in development and humanitarian contexts? But the pandemic is also forcing us to reflect carefully and critically on what the crisis means for *research* on digital identity. This is both a theoretical reckoning (how is the pandemic reshaping our framing and conceptualisation of the key issues?) and a methodological interrogation (how do we overcome the limitations that pandemic measures are imposing on empirical research?).

A starting point for us in this rethink is an April 2021 commentary published in *Big Data & Society*. In the commentary we confront a recurrent dilemma in discourses on digital identity in aid, which have amplified during the pandemic, and the implications for research. We find that debates on the potential value and drawbacks of digital identity all too often devolve into binarized positions: on one side, we observe certain proponents championing the inclusionary and empowering benefits of digital identity while downplaying the associated risks, especially to aid recipients. On the other side are critical voices including many digital rights activists and privacy advocates who critique digital identity in aid as a particularly egregious manifestation of 'surveillance humanitarianism', yet who sometimes overlook how aid subjects may associate digital identity with formal recognition and essential rights. As we discuss in our commentary, this state of polarisation is unfortunate, among other reasons, because it forecloses dialogue between the various actors involved in deploying digital identity systems and assessing their implications for aid, but also because it can have the unintentional effect of limiting opportunities for invaluable empirical research on the most pressing issues confronting so-called beneficiaries. In the commentary we sketch a future research agenda for digital identity in aid and call on the academic and practitioner communities to reflect on how to overcome this polarisation for the betterment of all those affected by the dynamics of datafication in aid.



Taking up this urgent call, and in light of a prolonged pandemic that has presented recurring challenges for field work, in May 2021 we convened an online workshop with The Alan Turing Institute, *Researching Digital Identity in Times of Crisis,* to bring together scholars, policy experts, civil society representatives and practitioners to discuss the wide-ranging implications of the crisis on both digital identity efforts and research in this space.[1] While the discussion at the half-day event was diverse and multifaceted—covering panels on COVID-19 responses, resistance to and contestation of digital identity systems, and possibilities for future digital identity interventions—here we offer three key takeaways and reflect on how they might feed into future research on digital identity in aid:

2 North/South divides

Our workshop revealed a notable disconnect between debates around digital identity in the 'Global North' and the 'Global South'[2]. Researchers are often siloed within their countries or regions of focus. We need comparative work that examines how digital identity schemes are taking shape in ways that may be similar—but also profoundly different—across global divides of socio-economic privilege and marginalisation (for example, by tracing flows and disparities in funding, infrastructure, political agendas and logics across international settings).

In many parts of Europe and North America, decentralised and privacy-by-design digital identity systems are not only championed, but are being actively implemented. The Pan-Canadian Trust Framework's federated model has become an exemplar for many Western countries. Meanwhile, the EU is looking to blockchain as a potential decentralised, cryptographic infrastructure for its evolving digital identity framework, and countries such as the Netherlands are exploring combinations of trust frameworks with self-sovereign identity

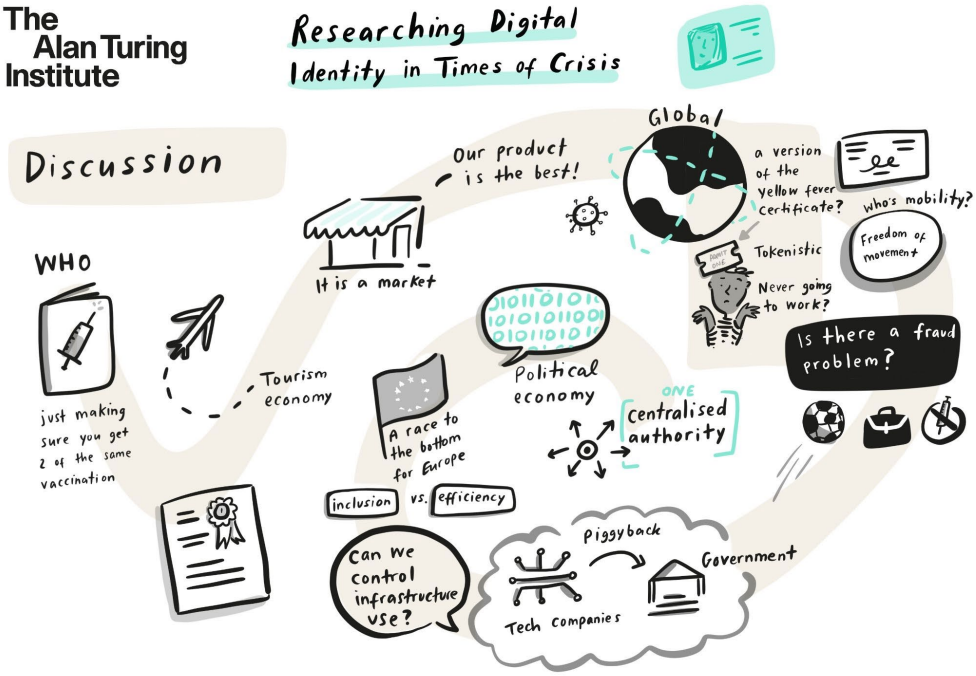
[1] This workshop was part of The Alan Turing Institute's Trustworthy Digital infrastructure for Identity project. This work was supported, in whole or in part, by the Bill & Melinda Gates Foundation [INV-001309].
[2] We use the term Global North/South to distinguish the wealthier and poorer parts of the world over terms such as less-developed, developing, underdeveloped or Third World—while recognizing that 'there are Souths in the geographic North and Norths in the geographic South" (Mahler, 2018: 32).

platforms. With the notable exception of border and immigration enforcement, many European governments and private sector players—compelled by growing public interest in data protection and laws like GDPR—are turning toward privacy-enhancing digital identity systems. The implications of this paradigm shift are nascent and yet to be evaluated.

In much of the Global South, however, we have seen the entrenchment of centralised and state-led biometric identity systems, such as India's landmark Aadhaar initiative and Kenya's nascent Huduma Namba project, both of which have provoked concerns about government overreach and data protection. In 2019, civil society organisations challenged the constitutionality of Huduma Namba before the Kenya High Court, partly on the grounds that its centralised data architecture posed the risk of state surveillance, data breaches, and data misuse. The second panel of our workshop—which featured presentations by Zehra Hashmi, Ngozi Nwanta, Azadeh Akbari, and Eve Hayes de Kalaf—highlighted the extent to which people in countries like Pakistan, Uganda, and the Dominican Republic are governed through biometric IDs and databases. In the humanitarian and aid sectors, the dominance of centralised biometric models is also evidenced by the scale and ubiquity of the UNHCR's biometric identity system, which contains the data of millions of refugees across almost 60 countries. While there is an increasing interest in decentralised and privacy-centric digital identity systems (like the ICRC's policy approach to biometrics) and consortia (e.g. the Smart Africa Trust Alliance), we are yet to see their claims substantiated.

This bifurcation speaks to broader global inequalities, evincing how political-economic structures shape technological design. For example, the prioritisation of mobile ID wallets assumes the existence of robust data protection laws or near-universal use of smartphones. This is out of touch with social realities even within wealthier, industrial countries. As Keith Breckenridge, one of the participants in our workshop, noted, current debates in Europe around digital vaccine passports (which revolve around questions of international standardisation, the merits of different designs, and attendant privacy concerns) are irrelevant to regions where simply accessing vaccines is an impossibility for many people. Digital identity schemes in the Global South are also shaped by very different institutional forces. Within the aid sector, large humanitarian organisations must navigate a patchwork of country-specific data-sharing agreements while, at the same time, operating beyond the remit of regional data protection regulations (like GDPR) and other legislative frameworks typically applied to companies and institutions in Europe.

Accounting for these disparities is critical for future research on digital identity whether within or outside the aid sector. Better understanding the forces that have enabled centralised biometric systems to proliferate across the Global South can also help researchers determine whether the privacy-enhancing, decentralised models currently being championed elsewhere are truly living up to their promises, and what new problems they instantiate—for example, in increasing the aid industry's reliance on private sector logics and technology providers (see more below).



3 Dynamics of data-sharing and interoperability

In spite of the implications of centralised biometric systems, the push towards data sharing in the form of institutional agreements, and growing interoperability between ID and data management systems, there is a notable disparity in the level of attention given to data sharing across the Global South and the Global North. In much of the Global North, the data protection and privacy dimensions of digital identity systems from both regulatory (e.g. GDPR) and technical (e.g. privacy-by-design) perspectives are the subject of significant attention, which far outstrips that given to data management practices in the Global South. This was underlined in the first panel of our workshop through a presentation by Ana Beduschi on COVID-19 vaccine credentials. She suggested that the increased attention such systems garnered had prompted a much deeper consideration of the broader impacts of digital ID on human rights, pre-existing inequalities, and accountability mechanisms.

The workshop highlighted the need to understand how dynamics of power and control shape the governance of data sharing enabled by identity systems. Some participants felt that efforts to support digital identification in the Global South were failing to address the wider problems of data governance and protection introduced through the development of these systems. As one participant flagged, far greater funding is allocated to implementing identification systems than to building appropriate data protection authorities, institutions, and capacities across many countries. Two approaches to addressing this emerged as priority areas—namely, an approach that stressed political economy and one that emphasised technical standards rather than panaceas.

A political economy analysis provides important tools for understanding how and why data sharing takes place, the significance of which was underscored by the recent controversy over the UNHCR's treatment of Rohingya data in Bangladesh. Increasingly digitised systems of identification often lead to new agreements around how data is managed. Yet we frequently have little understanding of the details of such agreements—which can enable data sharing between humanitarian organisations, different government agencies, private

partners, and other third parties—or the politics shaping these arrangements. Zehra Hashmi, for example, described how Pakistani citizens in Islamabad with family ties to Afghanistan experienced deep anxiety about their biometric data being recorded by Pakistan's National Database and Registration Authority (NADRA), since Pakistani citizenship status is linked to kinship and the security and national identification agencies have close ties. It was, Hashmi reported, critical "not to fall into the binary between surveillance and inclusion."

The technical dimensions that enable data sharing also require further critical analysis. One of the main benefits promised by digital identity systems comes from interoperability—linking humanitarian ID systems with social protection registries, for example, which is claimed to enable better targeting and reduce fraud. Yet this very benefit introduces a key risk to individuals: the sharing of personal data in ways that people do not know/understand or cannot give 'informed' consent to.

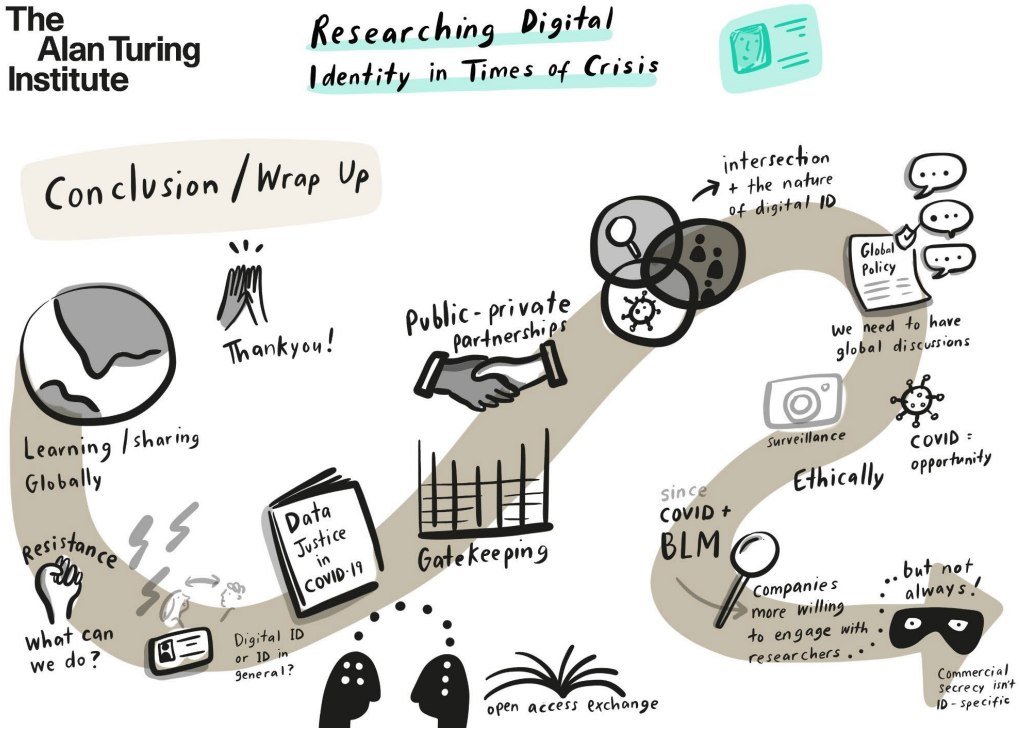
A deeper understanding of digital interoperability in the context of ID systems could help identify ways to deliver on the promised benefits of digital identity systems while ensuring that those benefits do not come at the cost of individual and group protections. This could serve not just approaches to identity systems, but also the systems and applications that IDs are associated with. This is particularly the case for digital cash transfers, which have introduced new demands for personal data collection to meet KYC/AML requirements and often depend upon multiple competing government, humanitarian, and private-sector systems. While 'integrated', interoperable systems are common in the social protection sector, the humanitarian sector has seen only one such model—the LOUISE platform in Lebanon—and even that largely operated through dominant UN agency platforms rather than a wider array of systems. The interests and institutional makeup of states, the private sector, and humanitarian organisations all determine how interoperability does (or does not) shape digital transformation in the Global South.

4 The digital identity industry: Methodological concerns

Several participants were vocal about the need for more research on the supply side of digital identity, specifically the industry actors that provide technology 'solutions' to the varied 'problems' of identification. Why and how are technology providers targeting their offerings at aid actors? In what ways has the aid sector become a new market for digital identity tech?

In this regard, civil society organisations have broken important ground in the investigation of the surveillance industry, which is notoriously secretive and reluctant to engage publicly with critics. Activists have used such methods as covertly attending trade conferences to gain insights into the operations of the surveillance industry, in addition to parsing marketing materials and press releases to understand the global growth of surveillance systems. While there are some important similarities here with the digital identity trade (namely the reliance on non-disclosure agreements and the opaqueness with which certain deals are struck with authorities), it is important to distinguish systems for covert surveillance from digital identity applications, especially those procured for aid purposes.

In terms of researching the industry, the pandemic has made in-person attendance at digital identity conferences nearly impossible, and press releases issued by both vendors and authorities are often sanitised: it can be difficult to grasp specific details about how new initiatives operate. The challenge for researchers is to explore creative methods for investigating *how* the industry is manoeuvring to drive digital identity investments by the aid sector. Or, alternatively, on what basis and in what ways are aid authorities courting industry players? One source of methodological inspiration for this line of inquiry is the [European AI Fund-sponsored project on 'sphere transgressions'](), which is exploring how the technology sector has seized the pandemic as an opportunity to innovate in new areas like public health. Workshop participant Laura Bingham remarked that holding digital identity technology developers and vendors to account for unethical business practices will require accountability mechanisms "with teeth" so that human rights are adequately protected.



5 Future directions

We look forward to being part of a growing research network that takes heed of the disparities between digital identity systems in different international settings and tackles pressing methodological, technical, and conceptual questions, including the politics of data-sharing and the role of private sector actors. We look forward to building research networks and projects that can better merge solutions-oriented technical expertise with theoretical and methodological insights from the realms of surveillance studies, critical data studies, the study of law, regulation and technology, and disciplines like anthropology. Ideally, better research praxis would also go hand-in-hand with greater transparency in the industry. Imagine, for example, how research might change if tenders and data-sharing agreements were to become more readily accessible. The research process itself can play a role in promoting such transparency. Ultimately, a renewed research agenda must go beyond simply identifying the harms of digital identity systems. We have to think much more critically about how globalised funding flows, data protection discourses, and competing private, governmental, and humanitarian actors are developing and reinventing digital identity solutions to meet an array of twenty-first century crises.