Working papers in Information Systems

THE PLATFORMNESS OF DIGITAL IDENTITY PLATFORMS

Silvia Masiero

WP 4/2021

Working Papers Series Edited by Petter Nielsen
Information Systems Group
Department of Informatics
University of Oslo
Gaustadalléen 23b
P.O.Box 1080 Blindern
N-0316 Oslo
Norway
http://www.mn.uio.no/ifi/english/research/groups/is/

The Platformness of Digital Identity Platforms

Silvia Masiero
Department of Informatics
University of Oslo
Norway
silvima@ifi.uio.no

Abstract:
Digital identity platforms allow the construction of complements on a centralised core, enabling user identification for private and public services. While presenting all traits characteristic of innovation platforms, digital identity platforms are curiously understudied in the Information Systems literature, largely as a result of a limited focus on the properties that underscore their nature as platforms, or "platformness". In this paper we first present a taxonomy of the main perspectives from which digital identity platforms have been studied in the multidisciplinary literature around them. We then illustrate the properties underscoring their platformness, illuminating the construction of complements on such platforms' core and its implications for two outcomes – exclusion and undue surveillance of vulnerable groups – that the literature has widely discussed. We conclude with a reflection on the theoretical implications of adopting a platform perspective in the study of digital identity systems.

Suggested bibliographic references: Masiero, S. (2021). The Platformness of Digital Identity Platforms. Information Systems Working Paper Series at University of Oslo. Edited by Petter Nielsen. 4/2021. Retrieved from the website:
http://www.mn.uio.no/ifi/english/research/groups/is/publications/working-papers-in-information-systems

1. Introduction

The term *digital identity* indicates the result of the conversion of human identities into digital data. Such a process reduces human beings to data records, streamlining operations of user recognition and entitlement assignation in the private and public sector. By doing so, digital identity affords building schemes where "identification, authentication and authorisation are all performed digitally" (Nyst et al., 2016: 8), subordinating authorisation to access a certain product, service or entitlement to correct authentication of the individual. Such properties are at the basis of the fast diffusion of digital identity systems, within private and public services as well as global agendas for social protection and development (cf. Gelb & Clark, 2013; Gelb & Metz, 2018; World Bank, 2021).

Crucially, digital identity systems are platforms that constitute "technological building blocks" for the development of complements (Gawer, 2009; Cusumano et al., 2019). At the core of digital identity platforms is a repository of user data, on which complementors can build apps and services using boundary resources (Mukhopadhyay et al., 2019). In such innovation platforms, access to complements is subordinated to recognition of the individual as a subject entitled with access to given services. The authentication function enables the system to assert that the user is who they claim to be, thereby determining authorisation on the basis of correct authentication (Nyst et al., 2016: 8-9).

In spite of the innovation platform nature that characterises them, digital identity systems are curiously rarely studied from a platform perspective. While outside the Information Systems (IS) field digital identity systems are largely studied in terms of their outcomes on users, recognition of such systems as platforms and study of them from the point of view of their platform properties are limited. The result is that, with few exceptions (cf. Mukhopadhyay et al., 2019; Mir et al., 2020; Bonina et al., 2021; Madon & Schoemaker, 2021; Masiero & Arvidsson, 2021), digital identity platforms are essentially left out from the literature on platforms, with the effect that implications of their platform architecture for development of complements and service delivery, as well as users' access, are largely overlooked.

Against this backdrop, in this paper we conduct a research reflection on the platform nature, or "platformness", of digital identity platforms. Our reflection centers on the characteristics that qualify digital identity systems as innovation platforms, using existing research to illuminate the implications of such features for the delivery of services. By doing so, we illustrate how the platform perspective affords illuminating features of digital identity systems that perspectives centred on outcomes alone do not illuminate, thereby showing the importance of such features for producing beneficial or detrimental outcomes for users.

Specifically, we focus on the production of two outcomes – exclusions from essential services, such as social protection schemes, and undue surveillance of vulnerable subjects – that are widely studied in the multidisciplinary literature on digital identity. Social protection schemes, meaning all public and private programmes that provide benefit transfers to the poor and protect them against livelihood risks (Devereux & Sabates-Wheeler, 2004), are being largely augmented with the biometric authentication of users, a process that has resulted in user exclusions that the physical version of the same systems did not afford (Drèze & Khera, 2015, 2017; Khera, 2019; Muralidharan et al., 2020). Vulnerable subjects giving out data to public authorities, such as refugees on the move or displaced persons seeking assistance, are similarly subject to forms of data capture that enable surveillance mechanisms further endangering them (Latonero & Kift, 2018; Pelizza, 2020; Iazzolino, 2021). The core contribution of this paper is that of relating outcomes of exclusion and undue surveillance to platform properties, illustrating the importance of the platform perspective in the genesis and maintenance of such outcomes.

The paper is organised as follows. We first review the main perspectives from which digital identity platforms have been studied in the literature, showing how two perspectives, centred respectively on *datafication* and *mediated surveillance*, prevail over a platform perspective. We then illustrate the properties that underscore the "platformness" of digital identity platforms, illuminating the implications of such properties for the two perverse outcomes of exclusion and undue surveillance. We then exemplify our insights through two published papers that take a platform perspective on digital identity, explicitly illuminating the link between platform properties and outcomes of exclusion and undue surveillance for users. Finally, the discussion reflects on the contribution that a platform perspective on digital identity brings to the literature.

2. Digital Identity Platforms: Existing Perspectives

The need for secure identity verification is present across the private and public sectors. In the private sector, the Know-Your-Customer (KYC) principle requires to take measures to verify the identity of business partners and customers, to ensure the suitability of the relationship and avoid risks including fraud, diversion and illicit transactions. In the public sector, services are provided in virtue of user status, be it universal or targeted to users in a particular category, defined by income or other status markers. Across sectors, it is required to ensure that partners, customers or users accessing a given service (a) are who they claim to be, and (b) are entitled with the right to enter a business relation or access the product or service in point, includig social protection or emergency assistance.

The architecture of digital identity platforms is built in order to streamline both functions. Masiero and Arvidsson (2021) remark that digital identity platforms present a core and complements built on top of them by third parties, in particular:

- At the *core* of a digital identity platform is a repository of user data, where biometric and demographic details of users are accessible in a digital format (Mukhopadhyay et al., 2019). Such repositories vary in size, quality and shape across sectors, industries and geographies. For example the Central Identities Data Repository (CIDR), the core repository of India's Aadhaar which is the largest digital identity platform worldwide, stores biometric and demographic data for over 1.2 billion Indian residents (UIDAI, 2019).
- Enabling the construction of complements in digital identity platforms are *boundary resource*s made available to third-party actors, such as Application Programme Interfaces (APIs) and Software Development Kits (SDKs). Following the same generative logics of innovation platforms (Ghazawneh & Henfridsson, 2013), such resources provide authentication to verify the identity claim of an account holder, affording to match identity with entitlement markers (e.g. credit scores; citizen status; membership to vulnerable categories) of the user.
- Finally, third-party actors build *complements* on the platforms' core using the boundary resources in point. Complementors vary in nature and can belong to the private or public sector or regulated industries (Mukhopadhyay et al., 2019), with legal and regulatory frameworks defining parameters for ecosystem scope. For instance, national laws can limit scope by demanding specific features of complementors, or barring given types of third party-actors from participating in it (Addo & Senyo, 2021). Ecosystem scope hence results from a combination of openness and external limitations to its expansion.

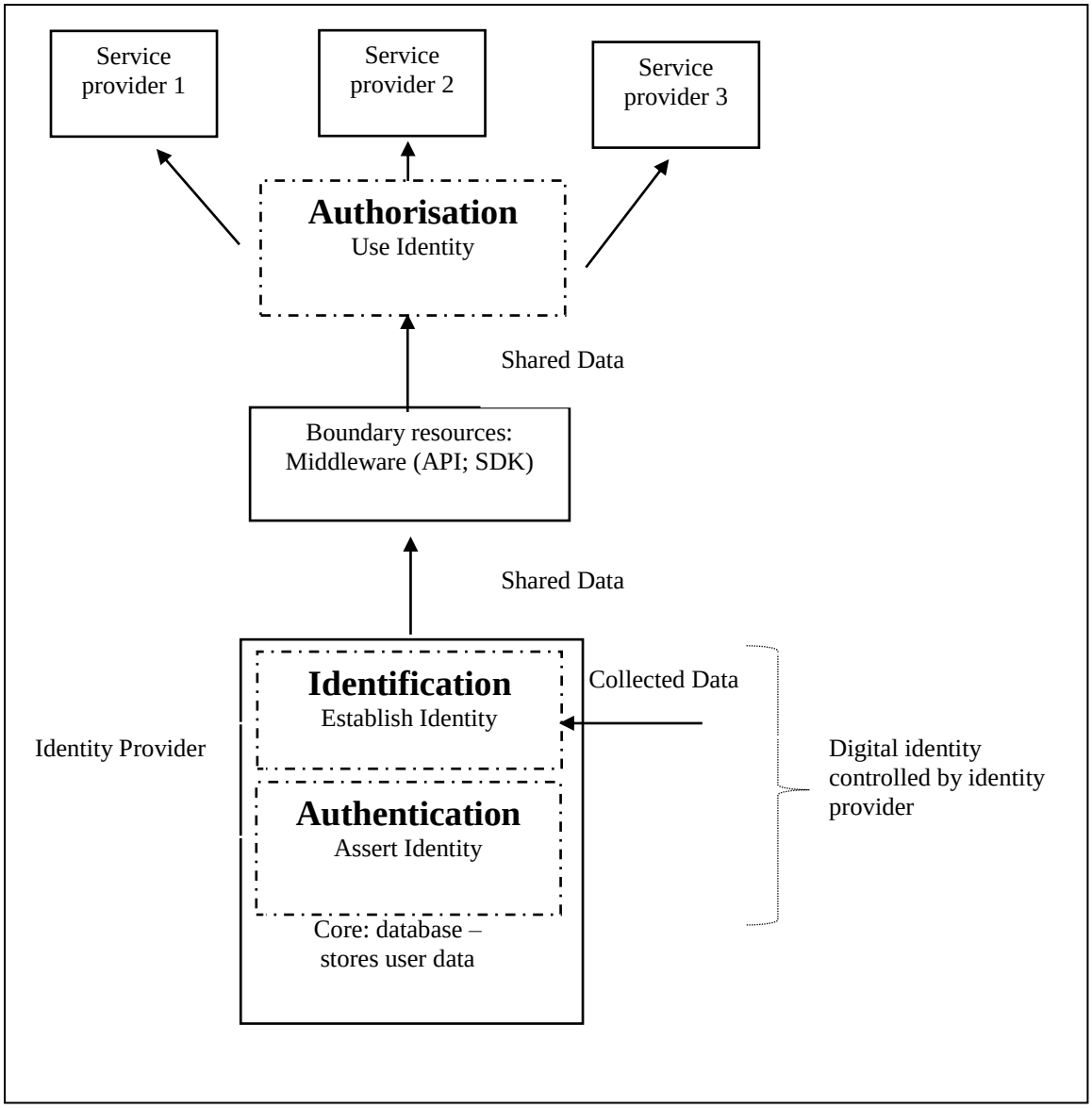

Figure 1: ***Digital identity platform architecture (Masiero & Arvidsson, 2021: 5)***

A stylised architecture of digital identity platforms is represented in Figure 1. A crucial question is on the nature of the digital identity provider, which can be private or public with diverse consequences on the ownership, treatment and usage of biometric and demographic data. A digital identity provider that delivers services based on biometric authentication needs to manage the trade-off between, on the one hand, exclusion errors, for which the system excludes genuinely entitled users (Devereux, 2016). On the other are inclusion errors, resulting in inclusion of non-entitled users in service provision. Matching user identities with their entitlements, digital identity platforms should ideally pursue both objectives, leading to the orthodoxy of "digital platforms for development" for which such platforms are designed (Masiero & Arvidsson, 2021; Nicholson et al., 2021).

In practice, however, limitations to the ability of platforms to realise such an orthodoxy are remarkable. A recent Special Issue of the journal Information Technology for Development articulates the link between digital identity and development along the components, promised by digital identity providers, of improved access to fundamental services, inclusion of vulnerable minorities, and ability to strengthen mechanisms of humanitarian assistance (Masiero & Bailur, 2021). The Special Issue proceeds, however, to problematise the link of

digital identity with all three components: limitations of digital identity are illustrated in terms of access to fundamental services (Chaudhuri, 2021; Effah & Owusu-Oware, 2021); inclusion of minorities and vulnerable groups (Bhatia et al., 2021; Krishna, 2021) and the strengthening and fairness of humanitarian assistance (Martin & Taylor, 2021a; Schoemaker et al., 2021). Such issues emerge, in all these accounts, through qualitative illustrations of the effects of digital identity on the lived reality of users.

Overall, while digital identity platforms function as innovation platforms (Cusumano et al., 2019) by all accounts, different perspectives coexist in the literature on digital identity, with a platform perspective occupying just a niche, IS centred space in it. In what follows, three main perspectives on digital identity – datafication, mediated surveillance, and platform – are illustrated, following the classification by Masiero and Shakthi (2020). The literature reviewed here largely transcends the IS field, spacing the domains of critical data studies as well as geography, surveillance studies, development studies and media and communications, which have largely engaged with digital identity and its consequences.

2.1. Digital Identity as Datafication

One recurring perspective in the literature views digital identity in its role as a converter of individuals into machine-readable data, presenting digital identity as a mode of *datafication* (Masiero & Shakthi, 2020; Krishna, 2021). What is datafied, in the making of digital identities, is the complex human identity of the user: in the phase of identification (Nyst et al., 2016), the user's identity is converted into data, creating a digital record that can be administrated through machine readability. It is this transition from human identity to digital data that underscores datafication, and that characterises digital identity as the act of datafying humans, turning the citizen into a data subject (Singh, 2020).

A datafication perspective calls the question on the rationale for datafication, be it underpinned by the KYC principle or by the need to match public sector user identities with entitlements. As noted above, a "digital platforms for development" orthodoxy sustains such a rationale in terms of the platforms' ability to combat inclusion and exclusion errors at the same time. The core idea is that datafying individuals allows a secure match of identities with entitlements, so to include in service provision all entitled users and securely exclude all non-entitled ones. It is on the principle of matching users and entitlements that the World Bank's (2021) strategy on ID for Development is based, and that digital identity technologies are marketed as identity "solutions" to global challenges (Martin & Taylor, 2021b).

Studies of digital identity in practice have, however, revealed a very different reality on implementation of such schemes on the ground. Multiple studies explore the detrimental consequences of datafication, such as the exclusion of users that, previously entitled to access schemes of vital importance such as social protection, lost access in virtue of authentication issues (cf. Hundal et al., 2020; Muralidharan et al., 2020; Chaudhuri, 2021). Exclusions of genuinely entitled users have linked to consequences as severe as hunger deaths from denial of food rations (Singh, 2019) or barring of refugees from services due to exclusion by design (Janmyr & Mourad, 2018). When applied to large social protection systems, such as India's Public Distribution System (PDS) which is the largest food security scheme in the country, such systems have produced measurable exclusions, leading to the argument that such systems may cause "pain without gain" (Drèze et al., 2017) for the intended recipients.

In sum, a vast literature exists on digital identity as datafication, focusing on its exclusionary outcomes. But the platform features of digital identity implicated in such exclusions are remarkably understudied. As noted below, the few platform-centred papers on digital identity systems adopt the perspective of the platform owner, centred on the digital identity orthodoxy but risking, in doing so, to "ventriloquise for the poor" (Breckenridge, 2019; cited in

Weitzberg et al., 2021: 6). This makes it important to complement studies from an owner perspective with user-centred accounts of the implementation of digital identity schemes.

2.2. Digital Identity as Mediated Surveillance

Accompanying a datafication view, a perspective of digital identity as mediator of surveillance (cf. Khera, 2019; Martin, 2019; Krishna, 2021) is established in studies of digital identity. In opposition to orthodoxies linking digital identity to development (Gelb & Clark, 2013), this perspective centers on the surveillance power linked to digital identity databases, where biometric and demographic data of users are accessible by database owners. Combination of such data with databases owned by public authorities, for example in cases of refugees or violently displaced persons, results in surveillance affordances that endanger the user, defying the goal of "empowerment through digital identity" that the orthodoxy states (Cheesman, 2020; Iazzolino, 2021; Schoemaker et al., 2021).

A substantial literature exists on the surveillance affordances of digital identity. In surveillance studies, the racialisation of digital identification technology (Newell, 2020) and its connection to public authority databases with the power to profile rather than assist (Martin, 2021) have been widely remarked, with a recent focus on the issues of algorithmic opacity following the introduction of Artificial Intelligence (AI) in humanitarian assistance (Coppi et al., 2021). Also remarked are the effects of such technologies on vulnerable users' justified reluctance to enrol in digital identity databases (Pelizza et al., 2021), with authorities turn such a reluctance against users especially when personal data are traded for access to essential services. Examples are the multiple cases in which essential social protection schemes are made conditional to the registration of biometric data (Ramanathan, 2014; Srinivasan et al., 2018). The result, studies from the mediated surveillance perspective convene, makes digital identity a tool to police rather than assist, with "authoritarian surveillance" (Akbari, 2021) not only problematising the empowerment rationale, but creating layers of problematicity for exactly those users whose greater vulnerability calls for protection.

Works on digital identity as mediated surveillance are essential to illustrate the double-edged nature of identity registration. Identity mediation, note Martin and Taylor (2021b), is purported by industry players and international development organisations as a route to achievement of development goals, especially SDG 16.9 to provide "legal identity for all including free birth registrations". Digital identity is built, in the industry rhetoric, as a necessary condition to the provision of essential services, requiring identification to identify the needful and promptly assign aid to them. Such a rhetoric is however criticised by accounts from the lived reality of users, portraying cross-checking of databases in opaque ways and lack of clarity in handling vulnerable people's data when assigning entitlements (Cerna Aragon, 2021; Lopez, 2021).

While vast and extending across disciplines, the literature on digital identity as mediated surveillance does not contemplate the platform features of digital identity systems. Important, in this respect, is the fact that boundary resources (Eaton et al., 2015) enable the shift of surveillance agency from platform owners to complementors, making it possible to triangulate social protection data with national or supranational authority profiling (Pelizza, 2020; Trauttendorff et al., 2021). The role of platform features, explored by the IS literature, is underexplored in studies of digital identity as mediated surveillance, leading to a need to greater unpacking of the role that platform features and design properties take in such outcomes.

2.3 Digital Identity as Platform

As noted above, digital identity systems have platform features just as other innovation platforms. They consist of a core, complements and boundary resources as in the

classification by Cusumano et al. (2019) and benefit from the openness and generativity that characterises such platforms, giving rise to vast digital identity ecosystems (Mukhopadhyay et al., 2019). In virtue of this, it is curious to note how the platform perspective is taken by only few studies of digital identity, with just a few more recognising the platform features of digital identity systems.

In the IS literature, two studies of India's Aadhaar (Mukhopadhyay et al., 2019; Mir et al., 2020) take a platform perspective focusing, respectively, on the ability of the Aadhaar platform to guarantee privacy and security (Mir et al., 2020) and on its scalability for services to the poor (Mukhopadhyay et al., 2019). Both studies are representations of Aadhaar as platform rather than datafier and surveillance, and are complemented by Bonina et al.'s (2021), Madon and Schoemaker's (2021), and and Masiero and Arvidsson's (2021) explicit recognition of digital identity systems as platforms. While confined to Aadhaar, which is a single identity platform, these studies illuminate platform properties by focusing on the platform's core-complements architecture, illustrating its affordances for service delivery and expansion of service agency to actors outside the government.

Nevertheless, both Mukhopadhyay et al. (2019) and Mir et al. (2020) take an owner's perspective on the platform, centering research on the platform's features and not including user perspectives in the study dataset. The result, especially when studying a platform that mediates access to essential services for millions of Indian poor, is an unfortunate risk to take user perspectives for granted, falling into the issue of "ventriloquising for the poor" flagged by Breckenridge (2019). As a result, the researcher is placed in front of a scenario of missed complementarity: while perspectives of datafication and surveillance take the users' view as central, they miss the platform features that largely shape users' situation. Conversely, while the platform perspective takes the design properties of platforms as central, it seems to overlook the user perspectives which are central to the lived experience of digital identity. It is this missed complementarity, of user-inclusive perspectives and focus on platform features, that inspires the reflection on the "platformness" of digital identity platforms conducted below.

3. The Platformness of Digital Identity Platforms

As noted here, curiously little focus exists on the platform features of digital identity platforms. This is ironic especially as most of the studies that recognise such platform properties adopt the platform leader perspective, rather than one that encompasses the views of digital identity users. Conversely, unpacking the "platformness" of digital identity platforms illuminates user consequences that a platform owner's perspective alone does not capture in full.

Against this backdrop, Figure 1 above highlights the properties that underscore the "platformness" of digital identity platforms. With user data repositories at the core, such platforms enable the construction of complements in virtue of the core's function as "technological building block" (Cusumano et al., 2019). Digital identity platforms hence enable governance models in which the provision of products and services is distributed across complementors, rather than centralised within the platform owner. This has important consequences both in the private sector, where business relations are facilitated through KYC, and in the public sector, where third parties are enabled to subordinate access to services to secure identification of citizens or residents.

Important are the implications of such "platformness" for service delivery. The problem lies in what perspectives centred on datafication and mediated surveillance do not capture: these perspectives, centred on the point of view of users, do not contemplate platform properties, and are thus unable to capture their relevance in the outcomes of digital identity for users.

Without a platform perspective it is therefore difficult to understand how platform properties are linked, in particular, to exclusions from essential services and undue surveillance of vulnerable groups.

A focus on the "platformness" of digital identity affords illuminating both problems. On exclusions, the datafication literature contemplates many exclusionary outcomes, ranging from failed authentication attempts (Muralidharan et al., 2020; Chaudhuri, 2021) to systems purposively designed to exclude some groups, such as migrants or refugees, from service delivery (Martin & Taylor, 2021a; Weitzberg et al., 2021). Complementing such a literature, a platform perspective captures how platform properties may enable such outcomes: figure 1 illustrates, indeed, how digital identity platforms are built *to subordinate* authorisation to successful authentication. This design property affords combating erroneous inclusions, but no features exist to tackle the erroneous exclusion of the non-authenticated, or those left out by design. The issue, Formici (2019) argues, becomes more acute in contexts of lacking data protection laws, such as that of India's Aadhaar where the tie of UIDAI with the country's Central Government (Anand, 2021) takes place in a vacuum of data protection legislation.

A platform perspective details, as a result, the direct link of platform architecture with the perpetuation of exclusionary outcomes in the services in which digital identity platforms are incorporated. Such outcomes may be particularly severe for vulnerable users, as cases of hunger deaths by exclusion from digitally-enabled food security systems (Singh, 2019), barring of displaced persons from essential services (Weitzberg et al., 2021), or silencing of marginalised communities in the statistics of the COVID-19 pandemic (deSouza, 2020; Milan & Treré, 2020; Milan et al., 2021) reveal. By making authorisation conditional to successful authentication, the platform architecture does not contemplate the situation of genuinely entitled users for whom authentication may fail, as it is, for example, for the elderly or workers of the construction sector, whose fingerprints can be unreadable to biometric scanners. In the absence of back-up mechanisms to guarantee delivery to entitled users who cannot authenticate, the risk of perpetuated exclusions is real, and reflected in the spikes in exclusions that coincide with the adoption of digital identity (Muralidharan et al., 2020).

Perspective	**Issues**	**Role of platform properties**	**Consequences**
Datafication	Users genuinely entitled to services are excluded from access (due to failed authentications or exclusion by design)	-Platforms are designed to subordinate access authorisation to successful authentication of users -Such an architecture combats inclusion errors, but not the erroneous exclusions of users who fail to authenticate or are excluded by design	-For complementors: can build services with inbuilt authentication functions, but cannot tackle exclusion errors in service delivery -For users: platform design enhances vulnerability to exclusion from essential services
Surveillance	Users enrolling for essential services (e.g. social protection) can be unwillingly profiled by public authorities	-Platforms are designed to enable interoperability, making it possible for external authorities to access biometric and demographic user data	-For complementors: can access user data from the core on the basis of interoperability (within the limits posed by legal and regulatory systems)

		-Such an architecture does not protect user data from access by third parties, though legal or regulatory systems may do so	-For users: enhanced vulnerability to surveillance, inducing vulnerable groups (e.g. refugees) to refrain from essential services

Table 1: ***Role of platform properties in issues of user exclusion and surveillance***

Similarly, platform properties play a role in the outcome of undue surveillance of vulnerable groups, such as migrants and displaced persons required to enrol in biometric databases for social protection (Iazzolino, 2021). As illustrated in figure 1, the ability of third parties to construct complements on the core is integral to platform architecture, and limited only by the legal and regulatory systems within which platforms operate. Relations between digital identity systems, such as the interoperability of Eurodac – the European database that uniquely identifies asylum seekers – with national police authority databases Europe-wide (Pelizza, 2020; Argyriou & Tympas, 2021; Trauttmansdorff, 2021), generate forms of surveillance that stem exactly from third-party intervention, inducing surveilled individuals to seek to avoid profiling (Pelizza et al., 2021). The same scenario, argue Taylor et al. (2020), became more acute during the COVID-19 pandemic, where public-private hybrids built surveillance technologies where the data protection rights of the surveilled are, at best, left in doubt (Böröcz, 2020; Lucero, 2020). Platform properties, on which the digital identity orthodoxy is grounded, hence result in detrimental outcomes for surveilled individuals, with the result that digitally-mediated access to essential services may result in unwanted exposure to potentially dangerous profiling.

Table 1 illustrates the relation of platform properties with the outcomes of exclusion and disempowering surveillance that the datafication and surveillance perspectives reveal. The role of platform properties in such outcomes illuminates the importance of unpacking the "platformness" of digital identity systems. Datafication and surveillance perspectives grasp users' view of digital identity, but alone cannot account for platform features: the platform perspective, in reverse, has so far been applied to capture the platform owner's view, but not observing the effects of such platforms on users. By studying digital identity systems as platforms, such relations become evident and greater articulations of user perspectives are afforded.

4. Digital Identity as Platform in IS Papers

We now turn to two examples of how the platform perspective, taken on digital identity systems, can illustrate the genesis of exclusion and undue surveillance. The two papers in point are chosen due to (1) their focus, respectively, on exclusions of users from social protection and handling of refugees by a biometric platform, and (2) the fact that they represent engagements of the IS field with digital identity systems. To do so both papers take a platform perspective, applying it to the study of platforms – India's Aadhaar and a biometric system for the distribution on in-kind aid in a refugee camp in Kenya – on which multiple works from the datafication and mediated surveillance perspectives exist.

Masiero & Arvidsson (2021) study the degenerative outcomes of Aadhaar for the PDS, India's largest food security system which its core to national social protection. Through ten-year qualitative data on the biometric PDS, collected from the early stages of computerisation till the recent Aadhaar-enabled authentication of users across Indian states, the authors find outcomes of exclusion of entitled users, distortion of the monitoring system towards one actor

– the ration dealer – only partially responsible for diversion of goods, and redirection of social policy towards a cash transfer system that is seen with fear and suspicion by PDS users. The study shows that beyond exclusions, Aadhaar is implicated in degenerative outcomes at the levels of monitoring and development policy, which reshape the course of food security in problematic and ultimately, undesired ways for the intended recipients. Implications for fairness of digital social protection systems are hence drawn beyond the authentication layer that is at the core of datafication studies (cf. Nyst et al., 2016).

Beyond IS, Aadhaar has been widely studied in terms of its exclusionary outcomes. A wide array of survey research (cf. Drèze & Khera, 2015, 2017; Drèze et al., 2017; Muralidharan et al., 2020) shows, in quantitative terms, the exclusionary effects resulting from the conversion of the old, physical PDS into its biometric form, first implemented through state-level biometric schemes and then through the Aadhaar implementation. Quantitative studies are accompanied by qualitative research on the biometric PDS, which shows the anxieties of user recognition and the dire impact of exclusions (Masiero & Das, 2019; Hundal et al., 2020, Chaudhuri, 2021). All these studies point towards exclusion as a known effect of the turn to biometrics, leading to accounts (cf. Muralidharan et al., 2020) framed in terms of "balancing" exclusions with reduced level of diversion. With exclusions being a known fact, the question becomes framed in terms of their balancing with the alleged "reduced diversion" from biometrics, for which the matching of users with their entitlements should reduce leakage outside the system, a finding that is itself problematised by ethnographies of the PDS (Hundal et al., 2020).

The platform perspective taken in Masiero & Arvidsson (2021) takes the argument to a different level. Different from other studies, concentrated on outcomes of the PDS as the dependent variable, the study shows how platform properties – in particular, a platform design that subordinates authorisation to authentication – are implicated in degenerative outcomes, in primis the exclusions generated by a design that cautions for inclusion errors, but not for exclusion ones. Building on this, the authors observe how degenerativity pervades monitoring – steering it all towards ration dealers – and even policy, creating the backbone for a cash transfer system towards which users express preoccupation (Ragahavan, 2021). Framed under this light, the platform perspective allows unpacking of two crucial links: the one between platform properties and exclusion, and the one between such properties and degeneration at deeper levels, which affect the very way the food security system is organised.

Iazzolino (2021) studies a Biometric Identity Management System (BIMS) for the distribution of food aid to refugees in Kakuma, one of Kenya's largest refugee camps. Drawing on fieldwork with Somali refugees and United Nations High Commissioner for Refugees (UNHCR) staff responsible for system implementation, he studies the outcomes perceived from refugee users, illustrating the twofold rationality of *managing* and *policing* implicit in the system. Making people with refugee status eligible for food aid, the platform subordinates the right to food to registration, a process made increasingly difficult in the Kakuma camp for the Somali ethnic population, whose relation with the Kenyan state has often resulted into violence (Iazzolino, 2021: 112). Iazzolino's ethnography of biometrically delivered food aid shows the surveillant nature experienced by Somali refugees in BIMS, putting it into explicit relation with the design properties that subordinate assistance to recognised refugee status.

Studies of biometrics in the humanitarian sector illustrate, as noted in Weitzberg et al. (2021), the tension between the binary logics of surveillance and recognition. Weitzberg et al. (2021: 1) note how the same logics of profiling implicit in surveillance become, for humanitarian bodies involved in registration, constitutive of a "politics of empowerment" that grounds the registration discourse. Such a politics, Taylor and Martin (2021b) observe, creates and expands a market for the digital identification industry, where such technologies are traded

within a teleology of "empowering" the "unidentified masses" subjected to adversity. Research from a users' perspective illuminates, conversely, the policing side of the logics: besides opaque processes of attribution of entitlements (Janmyr & Mourad, 2018; Coppi et al., 2021), biometric registration involves risks that were not perceived before its advent (Pelizza et al., 2021). The result is a tension between the logics of aid and the perceptin of dangerous policing by interested subjects, a duality whose intrinsic tension permeates the debate on biometric aid (Weitzberg et al., 2021).

Within this tension, Iazzolino (2021) shows that it is the matching enabled by the platform, combining identity with the refugee status that affords entitlements, to result in the undue surveillance perceived by refugees. The need for refugee household heads to register their fingerprints for identification at food distribution points affords the coexistence of managing and policing rationalities, subordinating the right to food to a form of refugee profiling ridden with historical complexities (cf. Weitzberg, 2017, 2020). The study illuminates the platform properties that attach surveilance to care, ultimately making the former a necessary condition for the latter. Extreme consequences of this conditionality emerge when fear of surveillance, and of the dangerous consequences attached to it, lead people in danger to avoid seeking assistance due to pervasive fear of profiling (Pelizza et al., 2021: 70).

	Platform	**Platform Properties**	**Outcomes**
Masiero & Arvidsson (2021)	Aadhaar (India)	Subordination of authorisation (access to the PDS) to authentication of residents as entitled users of the programme	-Exclusion: entitled users excluded from access to the system due to failed authentication or lack of recognition as entitled subjects -Distortion: programme monitoring distorted towards ration dealers, away from all other actors in the PDS supply chain -Redirection: food security policy redirected from food subsidies to cash transfers, feared and suspected by users
Iazzolino (2021)	Biometric Identity Management System (Kenya)	Food aid in general food distribution points made conditional to recognition of refugee status	-Surveillance: food aid made conditional to profiling of refugees, made particuularly complex for the Somali population -Polarisation of biometrics in Somali refugee views, associating biometric profiling to the authoritarian policies

			conducted against them

Table 2: ***Digital identity platform properties and their outcomes – examples from the literature***

Table 2 illustrates platform properties discussed, respectively, in Masiero and Arvidsson (2021) and Iazzolino (2021), showing links with the outcomes of exclusion and undue surveillance. The table also illustrates the further outcomes that a platform perspective allows to visualise: these are, for Masiero and Arvidsson (2021), visible in the outcomes of distortion of monitoring and redirection of policy through Aadhaar, in ways that end up hurting the beneficiaries. For Iazzolino (2021), what is uncovered is a further polarisation of biometrics in refugees' views, who suggest an association of BIMS with the authoritarian measures taken against the Somali population. Taken together, these insights illustrate the power of a platform perspective in explaining outcomes, associating them to the architecture of the platform design behind them.

5. Discussion: A Platform Perspective on Digital Identity

This paper has illustrated how digital identity platforms allow the construction of complements on a centralised core, enabling user identification for private and public services. We have noted that, despite their nature as platforms, these systems are mostly studied through perspectives of datafication and mediated surveillance, which focus on user positions, but do not unpack their platform properties. Such properties are however linked to problematic outcomes of digital identity, such as the exclusion of entitled users from services and the undue surveillance of vulnerable groups. The platform view hence needs strengthening in studies of digital identity in the private and public sector, as well as in the humanitarian context where digital identity technologies are increasingly pushed (Coppi et al., 2021; Taylor & Martin, 2021b).

This argument has several implications. First, one of the reasons for understudy of digital identity from a platform perspective is a lack of this perspective in the multidisciplinary literature on digital identity beyond IS. At the same time, the few IS contributions adopting a platform perspective focus on the platform owner, as it is common in studies of platforms – but overlooking, in doing so, the perspective of users. As a result, the different perspectives would benefit from dialogue with each other, to leverage complementarities and illuminate what are still blind spots in knowledge on how digital identity platforms are experienced by users.

Crucial to such a dialogue is the perspective proposed by Bonina et al. (2021), which reflects the new IS focus on digital platforms for socio-economic development. Studies taking such a view offer greater openness on the conceptualisation of platforms, studying their implications for socio-economic development processes (Koskinen et al., 2019; Madon & Schoemaker, 2021; Masiero & Arvidsson, 2021; Nicholson et al., 2019, 2021). Such perspectives, which expand the conceptualisation of platforms from the commercial focus proper to the IS literature, are of help in theorising digital identity platforms and studying their implications for users.

Secondly, the absence of focus on digital identity as platforms may be a symptom of a greater problem, lying in the overarching identification of "platforms" in IS with a for-profit platform logic. Notwithstanding the theoretical and practical importance of such platforms, the IS field is squarely centred on them, which leaves out considerations that transcend the domains of

business and innovation in platforms. The incoming focus on socio-economic development offers an important alternative to this view, leading to encompass systems, such as digital identity platforms, that mainstream IS literature has not yet expanded on. In this perspective, platform properties may explain outcomes of high social relevance, such as the exclusion and surveillance outcomes discussed here.

This point needs to be combined with the implications of our research reflection for justice in digital identity systems. Studies of digital identity are increasingly taking a *data justice* perspective, defined with Taylor (2017: 2) as "fairness in the way people are made visible, represented and treated as a result of their production of digital data". On the one hand, guaranteeing data justice in digital identity means ensuring people are treated fairly through their data representations, combating mishandling of their information when triangulated with entitlements. It is, in effect, due to the ability to guarantee "solutions" to essential challenges that the industry of digital identity technologies creates a market for private providers to thrive (Taylor & Martin, 2021b).

But on the other hand, the study of biometric social protection has brought to light new forms of data injustice, specifically interconnected with the biometric profiling of social protection users. Masiero and Das (2019) offer a taxonomy that contemplates *legal*, *informational*, and *design-related* forms of data injustice: in biometric social protection, *legal* data injustice refers to how fundamental rights such as the right to food and emergency assistance, become subordinated to registration in biometric databases. *Informational* data injustice pertains to opacity in the treatment of user data, leaving doubts on hoe such data are used and in particular, how these are combined towards the assignation, or not, of essential subsidies. Finally, design-related data injustice pertains to system design that does not meet user needs, such as biometric systems designed against inclusion errors, but not against inclusion ones (Masiero & Das, 2019: 927).

All these forms of injustice have been abruptly brought to light by the social protection systems of the COVID-19 pandemic (Milan et al., 2021). For example in India, as Hriscu (2021) notes, social protection users are still requested to link their Aadhaar number with their mobile phone numbers or authenticate through iris recognition, to obtain essential social protection. Cerna Aragon (2021) and Lopez (2021) offer precise accounts of informational injustice in Peru and Colombia during the COVID-19 pandemic, showing the cross-checking of data across systems as means to assign, in opaque ways, subsidies to households on the basis of existing data records. Spanning across systems that design biometrics for reinforcing exclusion of non-entitled users, design-related injustice acquires a new value in the emergency posed by COVID-19, with the consequences of exclusions being brought to bear on new masses of users thrown into need (Milan et al., 2021: 16).

Against such new needs, this research reflection seeks therefore to initiate a dialogue among perspectives, centred on the "platformness" of digital identity and its implications for users. A platform perspective, which unpacks platform properties in digital identity, complements datafication and surveillance perspectives in underscoring how outcomes for users are enabled. We hope this reflection can foster such a dialogue, ultimately framing digital identity platforms as an object of study in platforms research.

References

Addo, a., & Senyo, P.K. (2021). Advancing E-governance for Development: Digital Identity and its Link to Socioeconomic Inclusion. Government Information Quarterly, 38(2), 1-15.

Akbari, A. (2021). Authoritarian Surveillance: A Corona Test. Surveillance & Society, 19(1), 98-103.

Anand, N. (2021) New Principles for Governing Aadhaar: Improving Access and Inclusion, Privacy, Security, and Identity Management. Journal of Science Policy & Governance, 1-14.

Argyriou, V., & Tympas, A. (2021). The Techno-Politics of Smart Borders in the EU. Presented at Biometrics on the Move 4S Annual Meeting – Society for the Social Study of Science, 8 October 2021.

Bonina, C., Koskinen, K., Eaton, B., & Gawer, A. (2021). Digital Platforms for Development: Foundations and Research Agenda. Information Systems Journal, published online 28 January 2021.

Böröcz, I. (2020). Suspending rights and freedoms in a pandemic-induced state of danger. In Taylor, L., Sharma, G., Martin, A., and Jameson, S. (Eds.), Data Justice and COVID-19: Global Perspectives (pp. 146-153), London: Meatspace Press.

Breckenridge, K. (2019). Lineaments of biopower: the bureaucratic and technological paradoxes of Aadhaar. South Asia: Journal of South Asian Studies, 42(3), 606-611.

Cerna Aragon, D. (2021). On not being visibile to the state: The case of Peru. In Milan, S., Treré, E., & Masiero, S. (Eds.), COVID-19 from the Margins: Pandemic Invisibilities, Policies and Resistance in the Datafied Society (pp. 120–125). Amsterdam: Institute of Network Cultures.

Chaudhuri, B. (2021). Distant, opaque and seamful: Seeing the state through the workings of Aadhaar in India. Information Technology for Development, 27(1), 37-49.

Cheesman, M. (2020). Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity. Geopolitics, 1-26.

Coppi, G., Jimenez, R. M., & Kyriazi, S. (2021). Explicability of humanitarian AI: A matter of principles. Journal of International Humanitarian Action, published online 7 October 2021.

Cusumano, M. A., Gawer, A., & Yoffie, D. B. (2019). The business of platforms: Strategy in the age of digital competition, innovation, and power. New York: Harper Business.

de Souza, S. P. (2020). Invisibilising migrant distress in times of COVID-19. Data and Pandemic Politics series on data justice and COVID-19, https://globaldatajustice.org/covid-19/data-silences-invisibility.

Devereux, S. (2016). Is targeting ethical? Global Social Policy, 16(2), 166-181.

Devereux, S., & Sabates-Wheeler, R. (2004). Transformative social protection. Working Paper 232, Institute of Development Studies, Brighton, Sussex.

Drèze, J., Khalid, N., Khera, R., & Somanchi, A. (2017). Pain without gain? Aadhaar and food security in Jharkhand. Economic & Political Weekly, 52(50), 51.

Drèze, J., & Khera, R. (2017). Recent social security initiatives in India. World Development, 98, 555-572.

Drèze, J., & Khera, R. (2015). Understanding leakages in the public distribution system. Economic & Political Weekly, 50(7), 39-42.

Eaton, B., Elaluf-Calderwood, S., Sørensen, C., & Yoo, Y. (2015). Distributed Tuning of Boundary Resources: The case of Apple's iOS Service System. MIS Quarterly, 39(1), 217-244.

Formici, G. (2019). Sistemi di riconoscimento e dati biometrici: una nuova sfida per i Legislatori e le Corti. DPCE Online, 39(2), 1107-1132.

Gawer, A. (Ed.). (2009). Platforms, Markets and Innovation. Cheltenham, UK: Edward Elgar Publishing.

Gelb, A., & Metz, A. D. (2018). Identification Revolution: Can Digital ID be Harnessed for Development? Yale, Brookings Institution Press.

Gelb, A., & Clark, J. (2013). Performance lessons from India's universal identification program. Centre for Global Development (CGD) Policy Paper 20.

Ghazawneh, A., & Henfridsson, O. (2013). Balancing platform control and external contribution in third-party development: The boundary resources model. Information Systems Journal, 23(2), 173-192.

Hriscu, A. M. (2021). Biometric ID in India and Kenya. Paper presented at the TILTing Perspectives Conference, Tilburg University, 19-21 May 2021.

Hundal, H. S., Janani, A. P., & Chaudhuri, B. (2020). A conundrum of efficiency and inclusion: Aadhaar and fair-price shops. Economic & Political Weekly, 1-8.

Iazzolino, G. (2021). Infrastructure of compassionate repression: Making sense of biometrics in Kakuma refugee camp. Information Technology for Development, 27(1), 111-128.

Janmyr, M., & Mourad, L. (2018). Modes of ordering: labelling, classification and categorization in Lebanon's refugee response. Journal of Refugee Studies, 31(4), 544-565.

Khera, R. (2019). Dissent on Aadhaar: Big data meets big brother. Hyderabad: Orient BlackSwan.

Koskinen, K., Bonina, C., & Eaton, B. (2019). Digital platforms in the Global South: Foundations and research agenda. In International Conference on Social Implications of Computers in Developing Countries (pp. 319-330). Springer, Cham.

Krishna, S. (2021). Digital identity, datafication and social justice: Understanding Aadhaar use among informal workers in south India. Information Technology for Development, 27(1), 67-90.

Latonero, M., & Kift, P. (2018). On digital passages and borders: Refugees and the new infrastructure for movement and control. Social Media & Society, 4(1), 1-18.

López, J. (2021). The case of the Solidarity Income in Colombia: The experimentation with data on social policy during the pandemic. In Milan, S., Treré, E., & Masiero, S. (Eds.), COVID-19 from the Margins: Pandemic Invisibilities, Policies and Resistance in the Datafied Society (pp. 126–128). Amsterdam: Institute of Network Cultures.

Lucero, M. (2020) Fast tech to silence dissent, slow tech for public health crisis. In Taylor, L., Sharma, G., Martin, A., and Jameson, S. (Eds.), Data Justice and COVID-19: Global Perspectives (pp. 224-231), London: Meatspace Press.

Madon, S., & Schoemaker, E. (2021). Digital Identity as a Platform for Improving Refugee Management. Information Systems Journal, published online 18 June 2021.

Martin, A., & Taylor, L. (2021). Exclusion and inclusion in identification: Regulation, displacement and data justice. Information Technology for Development, 27(1), 50-66.

Martin, A., & Taylor, L. (2021). Give us your poor, your unidentified masses. Global Data Justice, https://globaldatajustice.org/2021-09-29-identity-week-2021/.

Martin, A. (2021). Aadhaar in a Box? Legitimizing Digital Identity in Times of Crisis. Surveillance & Society, 19(1), 104-108.

Martin, A. (2019). Mobile money platform surveillance. Surveillance & Society, 17(1/2), 213-222.

Masiero, S., & Arvidsson, V. (2021). Degenerative outcomes of digital identity platforms for development. Information Systems Journal, published online 7 June 2021.

Masiero, S., & Bailur, S. (2021). Digital identity for development: The quest for justice and a research agenda. Information Technology for Development, 27(1), 1-12.

Masiero, S., & Shakthi, S. (2020). Grappling with Aadhaar: Biometrics, Social Identity and the Indian State. South Asia Multidisciplinary Academic Journal, 23: 1-8.

Masiero, S., & Das, S. (2019). Datafying anti-poverty programmes: Implications for data justice. Information, Communication & Society, 22(7), 916-933.

Masiero, S., & Prakash, A. (2019) ICT in Social Protection Schemes: Deinstitutionalising Subsidy-Based Welfare Programmes. Information Technology & People, 33(4): 1255-1280.

Milan, S., Treré, E., & Masiero, S. (2021). Introduction: COVID-19 Seen from the Land of Otherwise.

In Milan, S., Treré, E., & Masiero, S. (Eds.), COVID-19 from the Margins: Pandemic Invisibilities, Policies and Resistance in the Datafied Society (pp. 14-21). Amsterdam: Institute of Network Cultures.

Milan, S., & Treré, E. (2020). The Rise of the Data Poor: The COVID-19 Pandemic Seen From the Margins. Social Media & Society, 6(3), 1-5.

Mir, U. B., Kar, A. K., Dwivedi, Y. K., Gupta, M. P., & Sharma, R. S. (2020). Realizing digital identity in government: Prioritizing design and implementation objectives for Aadhaar in India. Government Information Quarterly, 37(2), 101442.

Mukhopadhyay, S., Bouwman, H., & Jaiswal, M. P. (2019). An open platform centric approach for scalable government service delivery to the poor: The Aadhaar case. Government Information Quarterly, 36(3), 437-448.

Muralidharan, K., Niehaus, P., & Sukhtankar, S. (2020). Balancing corruption and exclusion: Incorporating Aadhaar into PDS. Ideas for India, https://www.ideasforindia.in/topics/poverty-inequality/balancing-corruption-and-exclusion-incorporating-aadhaar-into-pds.html.

Newell, B. C. (Ed.). (2020). Police on Camera: Surveillance, Privacy, and Accountability. London: Routledge.

Nicholson, B., Nielsen, P., & Sæbø, J. (2021). Digital platforms for development. Information Systems Journal, published online 13 August 2021.

Nicholson, B., Nielsen, P., Sæbø, J., & Sahay, S. (2019). Exploring Tensions of Global Public Good Platforms for Development: The Case of DHIS2. In International Conference on Social Implications of Computers in Developing Countries (pp. 207-217). Springer, Cham.

Nyst, C., Makin, P., Pannifer, S., & Whitley, E. (2016). Digital identity: issue analysis: executive summary. Consult Hyperion, Guildford: UK.

Pelizza, A, Milan, S., & Lausberg, Y. (2021). The dilemma of undocumented migrants invisible to COVID-19. In Milan, S., Treré, E., & Masiero, S. (Eds.), COVID-19 from the Margins: Pandemic Invisibilities, Policies and Resistance in the Datafied Society. (pp. 70–78). Amsterdam: Institute of Network Cultures.

Pelizza, A. (2020). Processing alterity, enacting Europe: Migrant registration and identification as co-construction of individuals and polities. Science, Technology, & Human Values, 45(2), 262-288.

Raghavan, M. (2021). Transaction failure rates in the Aadhaar-enabled payment system. Dvara Research, https://www.dvara.com/research/wp-content/uploads/2020/05/Transaction-failure-rates-in-the-Aadhaar-enabled-Payment-System-Urgent-issues-for-consideration-and-proposed-solutions.pdf

Ramanathan, U. (2014). Biometrics use for social protection Programmes in India violating human rights of the poor. Geneva: United Nations Research Institute for Social Development. http://www.unrisd.org/sp-hr-ramanathan.

Schoemaker, E., Baslan, D., Pon, B., & Dell, N. (2021). Identity at the margins: data justice and refugee experiences with digital identity systems in Lebanon, Jordan, and Uganda. Information Technology for Development, 27(1), 13-36.

Singh, R. P. (2020). Seeing like an Infrastructure: Mapping Uneven State-Citizen Relations in Aadhaar-Enabled Digital India. PhD thesis, Cornell University,

Singh, S. (2019). Death by digital exclusion? On faulty public distribution system in Jharkhand, The Hindu, https://www.thehindu.com/news/national/other-states/death-by-digital-exclusion/article28414768.ece.

Srinivasan, J., Bailur, S., Schoemaker, E., & Seshagiri, S. (2018). The poverty of privacy: Understanding privacy trade-offs from identity infrastructure users in India. International Journal of Communication, 12, 20.

Taylor, L., Sharma, G., Martin, A., and Jameson, S. (2020). What does the COVID-19 response mean for data justice? In Taylor, L., Sharma, G., Martin, A., and Jameson, S. (Eds.), Data Justice and COVID-19: Global Perspectives (pp.8-18), London: Meatspace Press.

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. Big Data & Society, 4(2), 1-14.

Trauttmansdorff, P. (2021). Making biometric borders interoperable. A necessary Political Fiction? Presented at Biometrics on the Move 4S Annual Meeting – Society for the Social Study of Science, 8 October 2021.

UIDAI (2019). UIDAI Annual Report 2018-2019. https://uidai.gov.in/images/AADHAR_AR_2018_19_ENG_approved.pdf.

Weitzberg, K., Cheesman, M., Martin, A., & Schoemaker, E. (2021). Between surveillance and recognition: Rethinking digital identity in aid. Big Data & Society, 8(1), 1-7.

Weitzberg, K. (2020). Biometrics, race making, and white exceptionalism: The controversy over universal fingerprinting in Kenya. The Journal of African History, 61(1), 23-43.

Weitzberg, K. (2017). We do not have borders: Greater Somalia and the predicaments of belonging in Kenya. New York: Ohio University Press.

World Bank (2021). Identification for Development Annual Report. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/625371611951876490/identification-for-development-id4d-2020-annual-report