Routledge
Taylor & Francis Group

Information Technology for Development

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/titd20

Exclusion and inclusion in identification: regulation, displacement and data justice

Aaron Martin & Linnet Taylor

To cite this article: Aaron Martin & Linnet Taylor (2020): Exclusion and inclusion in identification: regulation, displacement and data justice, Information Technology for Development, DOI: 10.1080/02681102.2020.1811943

To link to this article: https://doi.org/10.1080/02681102.2020.1811943

Published online: 29 Aug 2020.

INFORMATION TECHNOLOGY FOR DEVELOPMENT
https://doi.org/10.1080/02681102.2020.1811943

Routledge
Taylor & Francis Group

Exclusion and inclusion in identification: regulation, displacement and data justice

Aaron Martin and Linnet Taylor

Tilburg Institute for Law, Technology, and Society, Tilburg University, Tilburg, The Netherlands

ABSTRACT

Around the world, regimes of identification regulate people's interactions with state and commercial institutions. These regimes promise access to resources and entitlements, while also facilitating people's visibility to states and therefore their governability. For many, proving one's identity presents no challenge; however, it is estimated that a billion people have no official proof of identity. Meanwhile, the humanitarian sector is undergoing a transformation in which digital identity, mobile connectivity and digital finance are central features. Through a data justice lens, this paper explores customer identification regimes in two country contexts in which large displaced populations are present: Uganda and Bangladesh. The two cases reveal divergent approaches to regulating refugee identification: while Uganda's policy environment has recently become more inclusive, Bangladesh's proves to be particularly restrictive. We reflect on what these cases mean for the future development of digital identity systems by the humanitarian sector and the implications for data justice.

KEYWORDS

Connectivity; data justice; digitization; identification; mobile money; refugees

1. Introduction

The contemporary expansion of digital modes of identification to lower and middle-income countries surfaces many of the central issues of development and justice. How should we balance the need to be counted, and thus potentially served and represented, against the potential for the abuse of power over those who are identified and monitored? When the populations in question are displaced, poor or otherwise especially vulnerable to the misuse of power, we might argue for applying the notion of data justice – a social justice-informed approach to data governance – to this problem. This approach (Heeks & Renken, 2018; Taylor, 2017) suggests that we need to bring together different bodies of theory to understand the implications of new practices of identification for affected people.

However, digital identification systems are a double-edged sword, particularly when applied to mediate access to much-needed resources such as Internet and mobile phone connectivity, financial services and such basic entitlements as food and shelter. By increasing the legibility (Scott, 1998) of poor or displaced groups to national and international authorities, they create new power asymmetries and vulnerabilities. One of the key features of identification as a tool of population governance is the power it brings to select, and thus to include and exclude based on particular criteria. Our analysis of two evolving identification regimes in this paper is framed by Foucault's notion of biopower, '[a] power that exerts a positive influence on life, that endeavors to administer, optimize, and multiply it, subjecting it to precise controls and comprehensive regulations' (1976,,

CONTACT Aaron Martin a.k.martin@uvt.nl PO Box 90153, 5000 LE Tilburg, The Netherlands

p. 137). Work from sociology and surveillance studies on technologically enabled classification and sorting (Bowker & Starr, 2000; Lyon, 2010) indicates the inevitable risk of function creep from identifying to controlling, which, we posit, is most likely to occur through the tendency of digitized and linked identification systems to expose their subjects to other forms of control.

The digital identification systems explored in this paper not only create greater visibility for the poor or displaced, which can be beneficial, but also expose them to possible manipulation by those interested in policing and optimizing their behavior. This type of function creep aligns with Foucault's accompanying concepts of biopolitics and governmentality – the transformation of diverse bodies into governable subjects (Muller, 2011). Displaced and dispossessed people have not traditionally been framed as a problem of governability and control, but rather a problem of aid distribution and assistance. We will argue that the evolving use of digital identification technologies in relation to such groups is a key modern tool of biopolitics. These technologies expose and mediate people's access to needed resources and spaces (Farraj, 2010) and as such can, as well as benefiting recipients, form a disciplinary regime that leads people to conform to the needs of governments, international non-governmental organizations (INGOs), national NGOs and the technology developers themselves. This construction of a disciplinary regime is, we will argue, the result of geopolitics and constitutes new forms of power over the subjects of aid and poverty relief. That is, that they should have digital identities that can be read by all kinds of actors for purposes of categorization and classification, but also potentially for purposes of security, verification and policing of their right to resources on the international level.

The power to identify has frequently been framed as the power to subdue: Amoore (2006, p. 337) argues that biometrics used on a mass scale tend to facilitate 'the exercise of biopower such that the body itself is inscribed with, and demarcates, a continual crossing of multiple encoded borders – social, legal, gendered, racialized and so on.' These borders may be national, as in the case of the refugee populations explored later in this paper. They may also be political: demanding individuals identify themselves is in itself a form of control because it establishes authority by making the demand – a form of authority that is the essence of Foucault's concept of governmentality. Although Foucault does not focus on identification per se, practices of identity verification are a good fit with the dynamics he describes: historians have shown how the digital manifestations of identification are a relatively recent addition to the long history of biopolitical control. Sengoopta (2003) describes how identification through fingerprinting in India at the turn of the twentieth century served as an indispensable tool for colonial control, while also leading to a formalization of the caste system that would pile domestic upon colonial injustice over the ensuing century. Fingerprinting was first developed for welfare provision, for example, where the colonial authorities used it as a verification process to check that Bengali pensioners collected their pensions only once (Rottenburg, 2009).

Despite the historical relationship between identification, classification and control, it is also possible to identify a more emancipatory strand of thinking with regard to counting and being counted. The notion of representation is a cornerstone of democratic theory, and newer visions of justice, such as Fraser's work on abnormal justice, for example (2008), advocates for a new vision of social justice that rests not only on redistribution but also on recognition and representation – all of which require some version of counting, whether top-down or bottom-up. These aims are key to the problem of identification addressed in this paper, i.e. whether current practices of digital identification promote necessary and beneficial forms of visibility (those which recognize needs and represent them fairly to those who can distribute resources) without violating people's right to privacy or autonomy. It is this idea of representation and recognition that the United Nations (UN) calls on in its declaration of the protective power of big data-enabled counting and knowing (UNSG, 2014, p. 3): 'Never again should it be possible to say "we didn't know". No one should be invisible. This is the world we want – a world that counts.'

Given the tension between these competing visions of counting and identification, a data-justice line of thinking might question the association currently being made between the two in the context

of vulnerable and displaced populations. Sen has argued passionately that identity is flexible (2007) and should not be allowed to influence people's entitlements and rights. Similarly, we find a thread of resistance and counter-power in the sociological literature on identification. Arora, for instance (2019), argues that 'projects such as [India's] biometric identity scheme fail to consider the constructed nature of data and the mobility within the caste system' (p. 43). This argument for autonomy in the face of optimization is borne out by Cassan's economic analysis (2015) of the Indian population's response to the 1901 'Punjab Alienation of Land Act,' which, by basing resource allocation on caste, provoked people to manipulate their official identity in order to access land. In the Brazilian context, Murakami Wood and Firmino (2009) show that official identification has two poles related to the nature of citizenship: repression and inclusion. In their analysis, reactions from citizens to new identification schemes can be attributed to how they view the purpose of the ID cards in these terms.

This recurring tension between, and within, theories of classification and justice is worth investigating if we care about how people become included or excluded by digital systems, and with what results. To what extent do contemporary practices of counting and identifying vulnerable populations align with practices of control and manipulation and require resistance (Dencik et al., 2016; Martin et al., 2009), and to what extent can they be protective or even emancipatory (Heeks & Renken, 2018)? How is this question being framed in relation to new technologies of identification in fields where the most vulnerable populations are the targets? And where should we look for evidence of how this tension is playing out? This paper posits that access to mobile connectivity and financial services can serve as a central case for exploring Lyon's care-control tension and how it is unfolding in the humanitarian domain, where both care and control are expected and neither is policed: refugees, like migrants and the poor, constitute a population that has both extraordinary needs and extraordinary vulnerabilities. They are particularly impacted by a lack of access to services, including but not limited to the ability to make financial transfers, while they are in a state of displacement and disconnected from formal country authorities and institutions.

Research on the use of mobile phones by refugees demonstrates a link between access to connectivity and better mental health, positing that contact with friends and family decreases the stress of displacement (Latonero et al., 2018). However, refugees and other forcibly displaced people are the least likely to have access to meaningful connectivity and struggle with access to devices, Subscriber Identity Module (SIM) cards, reliable network signal and electricity (UNHCR, 2016).

In relation to lack of access to banking and payment services, mobile phones potentially provide much-needed access, but also come with demands for identification that are often difficult for displaced persons to fulfill (UNHCR, 2019a). Countries with a substantial refugee population are taking different approaches to regulating access to mobile financial platforms, given the dual priorities of allowing refugees and other displaced people the means to manage their resources and support those in their networks, while keeping track of transfers and payments for security purposes and to stop the emergence of a black market in financial transactions (cf. Martin, 2019).

In this paper, we interrogate the strategies of two countries dealing with this challenge: Uganda and Bangladesh. As of 31 December 2019, Uganda was home to over 1.38 million refugees and asylum seekers (UNHCR, 2019c) mainly due to conflict in neighboring South Sudan and the Democratic Republic of Congo. Refugees in Uganda have mostly been present for a longer term than those in Bangladesh, which received a massive influx of Rohingya people from neighboring Myanmar starting in 2017, bringing its total refugee population to over 900,000 (UNHCR, 2019d). Uganda is a party to the 1951 Refugee Convention, and UNHCR, the UN Refugee Agency, has been involved in its reception and service provision for refugees. Bangladesh, however, is not, and has been managing the refugee population through domestic agencies. This has given rise to different strategies for identity and service provision, which we explore below. This analysis allows us to expose the tensions between serving and controlling refugees through digital services and data collection, and to draw conclusions for the provision of IDs and regulation of data in the domain of humanitarian action.

It is at the intersection of policy and practice where the tensions between serving and monitoring play out. In this paper, we take the humanitarian sphere as our focus for several reasons: first, because humanitarian organizations have become the meeting place between analog and digital systems, and as translators between paper and code they have particular power to define and (re)classify. Second, because the sector's diversity enables us to see identification practices and systems being formed in real time between very different actors: national governments, international organizations, the UN system, technology firms and local NGOs. As Singh and Jackson (2017) argue, 'rather than an all-or-nothing state, inclusion in ICTD [information and communication technology for development] infrastructures is an ongoing and fragile process, achieved (unevenly) at the seams of multiple interconnected systems' (p. 4776). In this paper, we explore examples of such multiple interconnected systems that play into digital inclusion and exclusion, looking at the systems that emerge in digital interventions from the political, regulatory and experiential viewpoints.

A final reason to look at the inclusion and exclusion effects of digital identification on refugee and displaced populations is that these groups have not so far been the focus of research on such systems.[1] The resulting contribution is that not only can this context tell us something about how the most vulnerable experience such systems. It can also illuminate the increasing overlap between refugee and domestic populations where large-scale digital identification systems are concerned, and predict the possible future uses of these technologies on the latter. The systems Sandvik et al. term 'humanitarian experimentation' (2017) are becoming normality for people in low- and middle-income countries: refugees and other displaced people are the canaries in the coalmine of digital identification systems, and can tell us something about the issues we should expect to see surfacing in developing countries more broadly. The next sections contextualize the case studies by providing an overview of the state of both practice and research on our two issues of focus: first, the overall shift toward digitization in the targeting, provision and monitoring of humanitarian aid, and second, legal mandates for the identification of customers of mobile and financial services. We outline the interplay between innovation and regulation for both, and connect this to the research that has been conducted on each.

2. Humanitarian context: digitizing aid

Aid actors' increased use of digital technology is transforming both how humanitarian assistance is delivered but also how aid itself is understood. This digitization of aid provides new possibilities for humanitarian agencies to communicate with and help to protect those in need. In particular, the growing importance of mobile devices among those affected by crisis, including the displaced, has encouraged providers of aid to leverage mobile platforms for the distribution of aid in different forms including protection-related information and cash.

Humanitarian actors are as well treating the provision of mobile phones and Internet connectivity as a form of aid per se. There is growing consensus on the part of researchers and humanitarian organizations (see, for a review of the evidence, Latonero et al., 2018) that, during a humanitarian crisis, being connected on digital networks can help affected persons communicate with family members from whom they are separated, plan safe routes during migration, find shelter, engage with humanitarian agencies and share experiences, among other needs. As concerns the role of mobile phones for the displaced in particular, the United Nations High Commissioner for Refugees has stated that,

> a connected refugee population can play a critical role in enabling organizations such as UNHCR to innovate effectively and to improve the quality of services that we provide. Connectivity has the potential to transform how we communicate, the way in which we respond to the protection needs of displaced people, and our delivery of humanitarian services. Most significantly, better connectivity can promote self-reliance by broadening the opportunities for refugees to improve their own lives. Access to the Internet and mobile telephone services has the potential to create a powerful multiplier effect, boosting the well-being of refugees and of the communities that host them. (UNHCR, 2016, p. 5)

The International Committee of the Red Cross (ICRC) has also recognized the value of connectivity as aid and the importance of ensuring data protection therein (ICRC, 2020).[2]

Other actors are working on this issue from different perspectives: Internews, for instance, is addressing access to information as a digital connectivity issue, with the aim of creating greater digital and political literacy in areas where misinformation is causing harm (Internews, 2016). The Communicating with Disaster Affected Communities (CDAC) network bases its mission on the notion of connectivity as an integral component of effective humanitarian relief, connecting affected people to humanitarians and to each other (CDAC, 2016).

Digital innovation is also transforming the provision of humanitarian cash assistance, specifically the use of mobile money platforms to deliver aid in the form of digital cash, whereby aid agencies can directly transfer funds to a beneficiary's digital wallet on a mobile device. This modality is said to reduce the costs of cash distribution, result in more timely transfers and be easier to track and audit that physical cash (GSMA, 2017), though there are still costs associated with cashing out, i.e. converting digital funds into hard currency, which are borne by beneficiaries. And as we detail in the next section, legal and regulatory requirements pose another barrier to access in humanitarian contexts.

3. Connectivity and finance: regulatory requirements for customer identification

In this section we review two bodies of regulatory policy that mandate identification requirements for accessing mobile connectivity and finance, while drawing attention to the academic and grey literature that examines these topics, before turning to discuss their implications for humanitarian aid. SIM registration requirements are the remit of national telecommunications regulators, while national financial regulators including Central Banks oversee Know Your Customer (KYC)/Customer Due Diligence (CDD) rules that implement global recommendations concerning the prevention of money laundering, terrorist financing and other illicit financial activity.

3.1. Identification and mobile connectivity

Over the past decade, governments globally have implemented legal requirements that mandate mobile subscribers to prove their identity before activating a SIM card or, in some cases, to whitelist their device for use on local cellular networks (i.e. IMEI registration). According to the GSMA, the mobile industry's main trade association, as of January 2019 SIM registration was mandatory in at least 150 countries (GSMA, 2019a). This regulatory trend has been especially acute across the Global South, and most notably in Africa. Before 2006, nowhere in Africa had legally mandated SIM registration; one could purchase and use a prepaid SIM card in relative anonymity (Donovan & Martin, 2014). However, as of August 2019, just a few African countries had not introduced mandatory SIM registration into law (Privacy International, 2019).

These registration rules specify which forms of ID are acceptable to activate a SIM card (usually a national ID credential or equivalent in countries with national identification schemes) and penalties for non-compliance. Governments did not strictly enforce these rules during the first wave of registration mandates. However, in 2015 MTN (a South African multinational mobile telecommunications company, operating in many countries) was spectacularly fined $5.2 billion USD by the Nigerian Communications Commission for not complying with a government order to deactivate unregistered and improperly registered SIM cards (BBC News, 2015), inflicting lasting financial repercussions for the company (Kazeem, 2019). In response, mobile operators have more stringently enforced SIM registration rules and regulators continue to police non-compliance and mete out considerable financial punishments. For example, in 2019 Cameroon's regulator fined Orange Cameroun $2.6 million, and MTN Cameroon and Viettel Cameroun (Nexttel) $1.7 million each, for failing to abide by subscriber identification regulations (Atabong, 2019).

3.2. Regulating access to financial services

The global adoption of recommendations for financial customer identification has also created barriers to access bank accounts for those who lack recognized ID credentials. These requirements originate with the Financial Action Task Force (FATF), an intergovernmental body whose purpose is to set standards, recommend policy and promote effective implementation of law, regulation and operational measures to prevent money laundering, terrorist financing and other financial 'threats.'[3]

FATF has published a series of Recommendations, which have become the global standard for anti-money laundering (AML) and combating the financing of terrorism (CFT). As these Recommendations are non-binding, FATF must generate political will among its members to introduce national policy reforms. FATF Recommendations include 'risk-based' standards for KYC/CDD measures. Accordingly, certain activities should be undertaken when business relationships are established or relevant occasional transactions are undertaken, including the identification of customers and verification of customers' IDs using reliable, independent sources. The expectation is that countries implement FATF's high-level recommendations at the national level through legislation or other legally binding measures. National law and policy will specify how to carry out customer identification and verification in the jurisdiction based on local realities, including the particularities of national identification systems (where they exist) and availability of ID credentials among the population.

Sensitive to the potential for financial exclusion resulting from AML/CFT regulations and KYC/CDD measures in particular, the FATF has made occasional adjustments to its framework by introducing 'progressive' or 'tiered' KYC/CDD requirements. These permit national regulators to distinguish between lower-risk and higher-risk scenarios through tailored KYC/CDD procedures and could potentially be useful in addressing the needs of displaced persons.[4]

Scholars have analyzed the effects of these identification requirements on access to services in various parts of the world, including in OECD member countries (Gow & Parisi, 2008), Africa (de Koker & Jentzsch, 2013; Donovan & Martin, 2014; Jentzsch, 2012; Sumbwanyambe & Nel, 2013) and Bangladesh (Ahmed et al., 2017). They have found that in countries where identification requirements are introduced, legal access to services typically declines, specifically among those who lack valid forms of ID. Moreover, these authors have highlighted the surveillance, privacy and security risks associated with SIM registration and KYC/CDD infrastructures, particularly in countries that lack appropriate data protection laws and enforcement. Policy actors are also starting to explore the consequences of registration requirements on the mobile services market (GSMA, 2016, 2018), digital rights (see Diaz, 2017 for a Latin American perspective) and humanitarian programing (UNHCR, 2019a).

3.3. Implications for digital aid

As humanitarian agencies in particular are becoming more reliant on mobile networks and the Internet to fulfill their mandate, the legal barriers represented by registration rules complicate these efforts. Providing mobile connectivity as aid can be legally challenging in a context in which displaced persons, for example, lack documentation with which to register a SIM card in their own name. While both formal and informal workarounds are possible, including for example the bulk registration of SIM cards by humanitarian agencies for distribution to beneficiaries (which is often permitted by law) or the less legal but nonetheless commonplace practice of a crisis-affected person using a SIM legally registered in someone else's name (UNHCR, 2019a, p. 29), these techniques are arguably suboptimal from an inclusion perspective. SIM cards registered using a humanitarian organization's legal identity may be restricted in terms of the range of services available to the beneficiary. As concerns informal (i.e. illegal) measures for accessing connectivity, as UNHCR notes, 'such methods are precarious because these workarounds can put displaced persons in a vulnerable position and increase their chances of being taken advantage of, for example by being forced to pay a fee demanded by the legal registrant for continued access' (UNHCR, 2019a, p. 29).

Likewise, as with the provision of connectivity as aid, in countries in which mobile money is popular, registration requirements that accompany the provision of SIM cards and associated mobile money accounts can create barriers for those who lack valid ID. The mobile industry has argued that KYC/CDD requirements for activating a mobile money wallet have stunted the use of this modality by humanitarian agencies (GSMA, 2019a). While these studies prove helpful in linking identification requirements to the humanitarian enterprise, what is missing from in the literature is a theoretically informed exploration of these identification requirements for displaced persons themselves. Such an analysis is timely, given that claims are being made that digital identification can open up access to economic participation (Songwe, 2019) and to enable 'all people' to 'exercise their rights' (ID4D, 2019).

4. Research questions

The central questions we aim to answer with our research are these. First, a scoping question: what policy responses are emerging to address displaced persons' lack of legally valid forms of ID for service access? Next, we ask whether these responses amplify dynamics of inclusion and exclusion among displaced populations. Finally, we reflect on the implications of our findings for data justice, by which we mean the process of orienting digital techniques of counting and monitoring exclusively toward the interests and needs of affected people.

4.1. Research methods

This qualitative research follows a two-pronged methodological approach: First, we present case studies (Yin, 2003) of Uganda and Bangladesh based on a policy analysis and series of focus group interviews (for the Uganda case). This permits a thick description of the two contexts and helps to surface a range of concerns relating to refugee digital identification, specifically the inclusionary and exclusionary effects. Second, the discussion is further guided by an ongoing institutional ethnography informed through elite interviews (Richards, 1996) to discern key trends and controversies within the humanitarian sector's evolving approach to advancing digital identification. Table 1 summarizes our methods and what they offer to the joined-up analysis.

First, the policy analysis aims to scrutinize the causes and consequences of government public policies (Dunn, 2008) around refugees' legal access to mobile connectivity and banking accounts in the two countries. This analysis, undertaken during 2018-2019, involved the extensive collection and critical assessment of laws, regulations and policies from both Uganda and Bangladesh concerning SIM registration and KYC/CDD rules for financial services. It also engaged other relevant grey literature including policy reports by organizations such as Human Rights Watch and local press coverage on policy developments and emergent challenges.

As a means to validate our findings from the policy analysis, in October 2019 a member of the research team conducted a dozen focus group interviews with refugees in both urban and rural settings in Uganda to explore their use of connectivity and mobile financial services, and the role of identification systems and processes in facilitating or impeding access.[5] Extensive notes were taken during these interviews and subsequently manually reviewed for salient observations. Due to both the vulnerabilities of the interviewees and sensitivity of the topic under discussion, the decision was taken not to audio record the interviews.

Table 1. Summary of methods.

Method	Object of scrutiny
Policy analysis	Law and regulations governing refugee access to services
Focus group interviews	Experiences of refugee users of mobile services
Elite interviews	Perspectives of humanitarian innovation and data governance practitioners

Second, and as part of a wider research project on data governance in the humanitarian field, we are conducting an ongoing institutional ethnography[6] of the humanitarian sector. This ethnography is primarily informed through elite interviews with expert representatives of aid agencies regarding their use of data and technology in humanitarian intervention. These interviews, conducted with innovation specialists in humanitarian organizations and those working on data regulation in the humanitarian sector, provide background and inform how we interpret the events and policy literature on which we draw for our analysis, as well as our understanding of how institutions shape practice in the field. The institutional ethnography allows us to draw generalized findings about the institutional dynamics at play in propagating 'solutions' for the digital identification of refugees.

5. Case descriptions

The presence of different factors of interest in two specific locations, namely Uganda and Bangladesh, guided our case selection. Both countries have substantial refugee populations, and both wish to reduce the reliance of these populations on the receiving state, given that they are lower-income countries and lack the resources to support a large refugee population. The opportunity to compare how these two countries, which otherwise are very different in their characteristics, have managed this challenge, led us to choose them as our case studies. Both countries have taken different approaches to instituting and reforming identification requirements for refugee connectivity and accessing bank accounts: we show how they also begin to reveal different dimensions of inclusion and exclusion, which are explored more deeply in the following discussion.

The responses of governments in each of the countries to the presence of refugee and displaced populations demonstrate the dual concerns of care and control examined above: there is a responsibility to care, but also a strong incentive for states to control and govern the ways in which resources are distributed to those within their borders. This challenge also situates the displaced and dispossessed as a problem of governmentality: states must manage the insertion of new groups into existing systems of government when, as citizens of other countries (in the case of Uganda's refugee population) or people of disputed citizenship (in the case of the Rohingya in Bangladesh) they do not fit neatly into those systems.

In both cases, identification technologies become a fix for the problem of how to exert governmentality in the absence of belonging and citizenship. Technologies of identification, as a way of controlling and distributing access to resources while monitoring how that access is used, start to substitute for legal and constitutional power over these non-citizen residents. The policy responses we examine below should be read in this light: as ways in which states govern and manage non-citizens by managing their access to (digital) resources. While being framed by technology providers as giving people access to rights and entitlements, along with financial inclusion via various forms of digital ID, these identification technologies also serve as articulation points for biopower and political control.

5.1. Uganda: the policy response

SIM registration is required by law in Uganda as detailed in *The Regulation of Interception of Communications Act, 2010*.[7] The Uganda Communications Commission (UCC), the national telecommunications regulator, oversees the country's SIM registration policy. According to the regulation, mobile subscribers must present an original national ID in the case of Ugandan citizens, a valid passport for those visiting the country for a short period or a refugee ID for recognized refugees, in order to activate a SIM card.

Since 2010, the UCC has become increasingly active in its enforcement of SIM registration rules. In early 2018, it warned operators of penalties or license withdrawal for not disconnecting unregistered SIMs (Telecompaper, 2018). In March 2018, the regulator imposed a temporary ban on the sale of SIMs due to concerns about lax registration practices. Operators must now verify the authenticity

of the national ID card presented at the point-of-sale using an electronic biometric card reader, matching the applicant's live biometrics against those on the national ID card, and verifying in real time the customer's information, including a valid national ID number, against the National Identification and Registration Authority database (Malakata, 2018). However, a separate verification process applies to refugee ID cards, managed by the Office of the Prime Minister (OPM), the government agency responsible for refugee affairs.[8]

The Bank of Uganda, the country's financial regulator, has issued KYC/CDD guidance for mobile money: *Mobile Money Guidelines, 2013*, according to which a mobile money account can be opened with a Ugandan national ID card, passport, driving permit, voter card or local administration letter. Following the passage of the *Registration of Persons Act, 2015* and the issuance of several directives in 2017 by the UCC, a Uganda national ID number, Uganda national ID card, refugee ID card or valid passport is required both to register a SIM card and to open a mobile money account, thus harmonizing the requirements for both connectivity and mobile money.

While by law, refugee ID cards are acceptable for SIM registration, since 2016 the majority of displaced persons in Uganda have not been issued these ID documents due to internal backlogs within the issuing agency, the OPM. Coping mechanisms and workarounds have become common among refugees who sometimes ask individuals who hold a recognized form of ID to register a SIM card on their behalf (UNHCR, 2019b, p. 75).

In light of this situation and after considerable advocacy by UNHCR and other stakeholders including the mobile industry, in August 2019 the UCC issued a new directive to mobile operators detailing a policy shift that aims to create a more inclusive framework for refugee access to connectivity. This guidance specifies that, in the absence of a valid OPM-issued refugee ID card, a SIM card may now be issued to refugees who present an Attestation Letter.[9] Importantly, compared to the refugee ID card, this document is easier to access and thus more commonplace among displaced persons in Uganda.

In response to this policy change, a UNHCR spokesperson stated that,

> The new directive will enable the majority of refugees to legally access SIM cards and ease communication with families and also with UNHCR through the refugee helpline. Communication is a fundamental part of humanitarian response and is essential in ensuring accountability, transparency and operational effectiveness. (UNHCR, 2019e)

This policy measure is likewise expected to open up legal access to mobile money among refugees (GSMA, 2019b).

However, shortly after the UCC announced its new directive, an investigative journalist published a report exposing weaknesses in the verification of refugee ID cards for SIM registration (Daily Monitor, 2019). In response, the UCC temporarily suspended refugees' access to SIM cards. The suspension was to remain in place until a stronger verification process could be established for the refugee ID card. Importantly, the suspension affected holders of both the refugee ID card and the Attestation Letter, even though it was the former that was exploited by the investigative journalist.

As regards the latter credential, while the technical details are still being finalized as of early 2020, it is understood that a new verification procedure would likely require agents of mobile operators to connect with UNHCR's systems, or a copy thereof, to authenticate the validity of Attestation Letters for SIM registration purposes. The role of biometrics, if any, is still being determined, though a January 2020 operational update on the project stated that UNHCR is supporting the UCC and OPM 'to establish a live linkage to authenticate refugee biometrics and documentation for the issuance of SIM cards' (UNHCR, 2020).[10] Significant for our analysis, such a configuration increases refugees' access to mobile connectivity and mobile money. But it also repositions UNHCR as an identity broker for access to these services for those under its protection. It also arguably represents a form of function expansion, as data originally collected during registration for protection reasons is becoming valuable for other identification purposes.

5.2. Bangladesh: the policy response

Bangladeshi law requires SIM registration as specified in the *Cellular Mobile Phone Operator Regulatory and Licensing Guidelines, 2011*.[11] The country's SIM registration process requires subscribers to provide a copy of their national ID card or passport, as well as fingerprint biometrics verified against a national database, in order to activate a mobile connection (Ahmed et al., 2017; bdnews24, 2015). The Bangladesh Telecommunication Regulatory Commission (BTRC) oversees compliance with this process. The law prohibits subscribers from registering more than 15 SIM cards against the same ID credential. In 2017, the BTRC proposed to reduce the number of SIM cards that an individual can register from 20 to five. However, mobile operators resisted this due to concerns that a cap would affect legitimate connections and negotiated the current limit of 15 SIMs per person as a compromise. The BTRC regularly blocks SIM cards that are registered in excess of this limit (Bushell-Embling, 2018) and issues fines of $50 for each unregistered SIM it discovers. In 2016, a legal challenge motivated by privacy concerns and sensitivities about access to SIM registration data by foreign entities was unsuccessful (Dhaka Tribune, 2016). In January 2019, the BTRC launched an International Mobile Equipment Identity (IMEI) registry, taking aim at the use of illegally imported and 'fake' mobile devices in Bangladesh (The Daily Star, 2019).

Bangladesh's key regulation driving identification requirements for financial services is the *Money Laundering Prevention Act, 2012*, which defines basic KYC/CDD expectations including customer identification and identity authentication based on a national ID card, citizenship certificate or a driving license/passport, as well as proof of address (Vassas & Laïda, 2018). The Bangladesh Financial Intelligence Unit (BFIU), situated within the Bangladesh Bank (the country's Central Bank), is responsible for enforcing compliance with the regulation. In late 2019, BFIU introduced guidelines for electronic Know Your Customer (e-KYC) by which bank accounts can be opened without completing paper forms (BFIU, 2019).

As concerns displaced people in particular, refugees' legal access to SIM cards in Bangladesh is extremely challenging mainly due to their lack of access to required forms of ID. As Myanmar does not recognize their citizenship, Rohingya do not receive any form of official document from their home country to attest their identity (e.g. a passport). Moreover, the Bangladeshi regulator has reportedly been explicit in banning the sale of SIMs to the Rohingya. It has also allegedly criminalized the provision of previously registered SIMs to Rohingya (bdnews24, 2017). Police have arrested people for selling both mobile devices and SIMs to Rohingya. The regulator has also repeatedly warned mobile network operators not to provide connections to refugees in contravention of the law (The Daily Star, 2017). However, despite these efforts to deny the Rohingya mobile access, the buying and selling of mobile phones and SIM cards reportedly remains common in camps (AFP, 2019).

In response to this situation, and amidst a broader clampdown on Rohingya's freedom of movement (Human Rights Watch, 2019), in September 2019 the BTRC sought to apply additional pressure on operators to deny access to subscribers located in and around refugee camps by again ordering service providers to cease the sale of SIM cards to Rohingya. In addition, it made an unprecedented demand that operators degrade and/or deactivate mobile networks accessible by people in refugee camps. Operators were given a week to report back to the regulator on the actions they had taken to deny the Rohingya access to mobile connectivity (The Economist, 2019). As of June 2020 and during the COVID-19 pandemic, access to connectivity remained severely limited among the Rohingya (Human Rights Watch, 2020; Ratcliffe & Ahmed, 2020).

As with access to SIM cards, refugees in Bangladesh face severe challenges in accessing financial services. The Bangladesh Bank has indicated that the ID card that comes out of an ongoing UNHCR verification exercise would be sufficient to meet KYC requirements (UNHCR, 2019b, p. 8), but until the government allows refugees legal access to cash, this is stalled. As concerns mobile money, since refugees in Bangladesh cannot legally access mobile connectivity or financial services, legal access to mobile money is also severely restricted.

This problem is exacerbated by the politics of legal identification in the Rohingya community in Bangladesh. Having been subject to attempts by the Myanmar government over the last decades to make them accept official ID cards which exclude them from full citizenship, their refusal to accept this ID prevents them from repatriation as it is now a condition for any returning from Bangladesh (Milko, 2019). As UNHCR attempted to register Rohingya with 'smart cards,' the Rohingya resisted on the basis that they did not identify them as either formal refugees (a step resisted by Bangladesh because it would place an obstacle in the way of repatriation) (Brinham, 2018), or as Rohingya (since UNHCR does not conventionally identify refugees by ethnic group). The Rohingya wanted both these things in order to support their claim that they were Myanmarese refugees returning from Bangladesh, rather than Bengali refugees seeking to enter Myanmar (Brinham, 2018).

6. Discussion: inclusion and exclusion dynamics

The complexity of these cases indicates how nuanced the question of identifying the displaced in order to provide access to digital services becomes. This is particularly so when those services are not part of official relief provision but still form one of the most essential components of refugees' ability to create opportunity and exert agency in relation to their economic and social existence. The dynamics of inclusion through identification are important in producing opportunity to benefit from the protection of, and resource distribution by, international authorities, as with Uganda's refugee population, but also as a source of political agency and autonomy, as with the Rohingya. Digital identification does not only provide opportunity to refugees, it also offers opportunity to the authorities who provide, process and use it. Organizations that offer services to refugees begin to assemble databases that can be seen as multi-purpose: as much as an aid to efficient resource distribution, they constitute currency in the increasingly competitive world of international humanitarian funding. Databases can, in theory, pivot from identifying refugees for aid distribution to become population and labor statistics for the countries where refugees reside (for an example of this translation between mobile data and population statistics, see Data for Refugees[12]), but also may form the basis for other indices such as credit worthiness, security and risk, providing an informational resource that can be transacted with governmental and commercial actors. This potential repurposing of humanitarian databases has the potential to support inclusion, but it is necessary rather than sufficient for greater inclusion of displaced people in the national systems they need to access. If, due to political factors, the policy context is inflexible, as in the case of the Rohingya in Bangladesh, there is no reason why existing registration and identification systems should feed into a more just approach to serving and supporting refugees. Where inclusion is the aim, however, this repurposing of databases could serve as an important tool for translating refugees and the displaced into residents able to claim entitlements.

Moving from the political to the operational perspective, these new digital identification systems carry the potential to exclude even as they include. In Bangladesh the exclusion of the Rohingya is effectively encoded in any ID they are offered: they need ID to do both more (support claims to ethnic identity and citizenship) and less (not mark them with an excludable identity) than they currently do, while also providing access to services and the necessities of everyday life in their refugee situation. Despite the promise of improving efficiency, the new verification procedure in Uganda still involves a standalone process for refugees and creates possibilities for discrimination and exclusion, given that people can be graded according to risk and marked for scrutiny of other kinds. The three-way solution that articulates between the government, UNHCR and mobile network operators (and their agents) reconfigures refugees' relationship with UNHCR as the e-KYC provider and identity broker, and positions UNHCR as an actor which, through their database management decisions, can include and exclude (possibly inadvertently) people from commercial services.

This arrangement also raises the question of whether and how refugees are included in data rights frameworks, such as the Fair Information Practice Principles (FIPPs). These core principles are designed to shape data processing worldwide, and have formed the basis for the OECD Privacy

Guidelines, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the EU's General Data Protection Regulation (GDPR). If refugees are interacting with commercial providers through UNHCR, this implies that UNHCR must align with the principles of giving people access to their own data, allowing them to check and correct it if it is wrong, and to delete it if they so choose. Although exclusion from the FIPPs is clearly problematic from a rights point of view, inclusion is disruptive because of UNHCR's mandate to register international refugees. Is a refugee entitled to take themselves out of the database if they choose, or alter the information UNHCR holds on them? At this early stage, these issues are unlikely to come up, but if the agency becomes a platform for identification for other state or commercial services, tensions between civil, political, economic and more basic functions based on fundamental human rights may emerge.

These cases may be seen as the international humanitarian sphere's version of the continuing push by technology actors to break the connection between citizenship and identification. Self-sovereign identity system developers such as Hyperledger are part of the ID2020 coalition, which aims to provide legal digital identification to people worldwide.[13] Separating out identity services for economic activity and financial platforms from the business of identifying citizens for state or humanitarian provision of resources, and for the purposes of claiming rights, may be easier technically than it is politically.

Given the complex web of ID provision between the commercial and governmental spheres, and the emerging phenomenon of hybridization of ID provision we chart here, what are the options for ensuring that problems of political exclusion do not arise from commercial logics of inclusion? One option would be to end KYC requirements for SIM cards and payment platforms. While increasingly improbable, this would separate out humanitarian from commercial ID provision. Another is to understand what IDs people hold, including the displaced, and reform policy to suit their needs and situations. For example, making hybridization context-specific so that the risks are limited to particular sections of humanitarian databases. It is hard to come up with a process that would not require a unique means of identification for refugees to access services, regardless of how they prove their identity to states and aid providers. This has the risk of generating new forms of exclusion, since whenever a refugee is identified as such, that identification sets them apart from the general population.

This is arguably in contravention of the spirit of the 1951 Convention, which states that refugees should have access to services and to opportunities to exert their rights equivalent to that of the rest of the population of the country where they are resident. Conversely, the provision of special IDs for refugees to access services that are not refugee-specific creates the risk of excluding locals in countries where ID provision is not universal. This is the larger problem: how to achieve universal provision of ID, whether digital or otherwise.

In West Africa, ECOWAS countries are sponsoring a World Bank-funded project to provide digital IDs to all citizens across the bloc (World Bank, 2018). This West Africa Unique Identification for Regional Integration and Inclusion (WURI) approach aims to provide a formal version of ECOWAS identity that remedies individual countries' shortcomings in providing ID credentials to their residents. This would also incorporate refugees as part of ECOWAS countries' populations, and would therefore address the problem of timely and efficient ID provision for refugees (though the connection between identification and equal rights and access to services is tenuous at best in the case of frequently marginalized refugee populations). WURI, however, is unique in that it is built on a fairly long-established regional association of free movement, currency and trade, where borders and service provision have already, to different degrees, started to become porous to non-nationals. Constraints have already been relaxed. That this could be achieved in other parts of the world is not a given, and it is possible that a scheme like WURI is only currently possible in areas where substantial regional integration is already present.

The integration of identification systems and provision between humanitarian, state and commercial actors also presents risks. If the Ugandan approach were applied to the Rohingya, for example, an already vulnerable population would be exposed to commercial and state actors in ways that could

have unpredictable negative consequences, as can be seen from the exclusion they experience in Bangladesh. ID can exclude as easily as include, and when seen as an undesirable token can end up being functionally worse than transient residence and informal status.

Crucially, the approach in Bangladesh of blocking and downgrading networks for refugees has important spillover effects on non-Rohingyas living in the area. Refugee populations are never clearly bounded: the Rohingya interact with local residents to acquire SIM cards and phones. The government's blocking of mobile access, while not directly related to identification concerns, was deemed a necessary measure due to the ease with which Rohingya have been able to gain access to functioning SIM cards through local residents and others. Moreover, connectivity is shared by neighborhoods regardless of ethnicity and origin. Blocking or throttling cellular service in areas where Rohingya camps are located, namely Cox's Bazar, affects more than just the Rohingya. Humanitarian aid providers, other residents of the district and those needing to contact people inside the camps are also negatively affected (Rahman, 2019).

7. Conclusion

Regardless of how many technical fixes are proposed for the provision of IDs for the displaced, if we are interested in ensuring that data justice is served in the use of technology in displacement contexts, then the underlying problem is one of politics, law and regulation. Prioritizing refugees' access to services is likely to bring up political contestation anywhere in the world, because of the implication that where there are winners, there are also losers – not least because refugees tend to end up in areas of receiving countries where they are potentially in competition with the local poor for resources. For this reason, effective approaches to identification, digital or analog, have the advantage of potentially spilling over benefits to the citizen population. They also require active and dynamic governance choices by both humanitarian organizations and country institutions to ensure that benefits and disadvantages are shared in a fair and accountable way.

As can be seen from both our case studies, the politics of supporting refugees in a country context have strong effects on which technological systems become established and what they can contribute. As current projects such as the ID2020 alliance and the World Bank's ID4D project show, there is a tendency toward scalable, transnational approaches to digital identification. Both this scale and the presence of powerful multilateral sponsors have created a marketplace for vendors such as Accenture, Microsoft and blockchain application developers. Where the approach envisaged is a technical one, the involvement of commercial actors is inevitable, but also effectively constitutes market-making that invites opportunism, suggesting that conveners of such initiatives will have to be careful to distinguish between what serves refugees and what generates productive partnerships for high-level actors. One high-profile example of this problem is Facebook's Libra cryptocurrency project.[14] which aims to 'develop and promote an open identity standard' as an essential underpinning for a cryptocurrency designed to be available to the poor and displaced worldwide (Libra Association, 2019, p. 8). The Libra partnership includes humanitarians (Mercy Corps) but is mainly composed of commercial firms, in an alliance that, in terms of data flows, may result in uneasy bedfellows and has already generated criticism (see, for example, Kaurin, 2019) for its conflation of humanitarian rhetoric with a for-profit structure.

Law and regulation, though slower moving than Big Tech's solutionism, are the ultimate answer to ID reform, and therefore to the just use of data technologies in this context. Ultimately, workable solutions are likely to focus on identification that is linked to citizenship rights and protection, although in the short term noisier, more commercial projects are gathering the attention. The points of overlap between national and refugee-specific ID provision studied here are both problematic because they create grey areas and uncertainties, and positive because they are indications that ID may be able to operate in similar ways for citizens and non-citizens. The digital systems component may, if based on needs rather than narrow entitlements, enable greater access to national systems rather than further siloing into those who belong and those who do not. A data-justice vision of refugee ID is one that

multiplies and stabilizes entitlements, and does not offer up the refugee to systems that can rate or assess them. It is also an ID that does not create a permanent definition for that person: identity systems should translate between types of legal status without disadvantaging people's opportunities as they transition into, or back to, citizenship.

A just identification system is also independent of the goodwill and sustainability of commercial or nonprofit actors. Any identification project has to connect individuals to authorities, and the ultimate authority (regardless of the promises of self-sovereign ID vendors) will be either a state, or an international humanitarian organization that can substitute in certain key dimensions for the state. Rights cannot be granted, they can only be claimed and accessed (or denied), making identification, digital or not, the territory of politics and law rather than technical innovation. Where these can be aligned, refugees are likely to benefit, but technical fixes cannot substitute for 'the right to have rights' (Arendt, 1958, p. 258), which constitutes the main function of any meaningful identification system.

Notes

1. One notable exception is Weitzberg's emerging research on the exclusionary effects of double registration in Kenya: https://www.codastory.com/authoritarian-tech/kenya-biometrics-double-registration/
2. The ICRC Handbook on Data Protection in Humanitarian Action, revised in 2020, includes a chapter dedicated to data protection concerns within connectivity as aid.
3. https://www.fatf-gafi.org/about/
4. It is worth noting FATF's 2020 guidance on digital identity, which includes an extensive discussion on the role of digital ID in identifying refugees (see pp. 73–75): https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html.
5. Accessing Cox's Bazar for a research visit is part of a future phase of the project, but has not been possible within the timeframe of the current study and due to travel restrictions during the COVID-19 lockdown. Instead, we have used interviews and literature from the field to understand the dynamics of identification systems and connectivity provision in that area.
6. Walby (2013) argues that institutional ethnography is neither a theory nor a methodological technique, but more like an agenda for inquiry that is guided by particular theoretical and methodological commitments (p. 141).
7. See Section 9 on Duties of telecommunication service provider in relation to customer.
8. For foreigners visiting Uganda, SIM cards can only be issued upon presentation of a valid passport and visa. By law, the operator must deactivate the SIM cards upon the expiration of the customer's visa or work permit.
9. Attestation Letters are also issued by OPM with support from UNHCR (which manages the process and underlying registration system). These letters contain the pictures and identity information of the entire family (UNCDF, 2018, p. vii).
10. The update goes on to explain that 'A Data Protection Impact Assessment (DPIA) was carried out for the initiative and the main recommendation of the assessment is the finalization of a Data Sharing Agreement between UNHCR, OPM and UCC, prior to the live launch. Meanwhile, testing is ongoing with challenges being addressed by the UNHCR headquarters development team.'
11. See section 38 on Registration of Subscribers.
12. http://d4r.turktelekom.com.tr/.
13. https://id2020.org/alliance.
14. Libra was rebranded as 'Novi' in May 2020: https://techcrunch.com/2020/05/26/facebook-rebrands-libra-wallet-service-calibra-to-novi.

Acknowledgements

The authors would like to thank the organizers of the 2019 Data Power Conference in Bremen, Germany, where a version of this paper was first presented, as well as Wainer Lusoli for inviting us to present a working paper at the Building Resilient Democracies workshop at IHEID in Geneva, Switzerland in December 2019. We would like to acknowledge Shaz Jameson and Gargi Sharma for their feedback on earlier drafts of the paper and Victor Nyamori of Amnesty International for his updates on the Uganda situation. We are grateful to the UNHCR Innovation Service for facilitating access to refugee sites in Uganda for focus group interviews. Finally, we are deeply indebted to the guest editors and anonymous reviewers for their extensive comments on the initial versions of the article.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

The authors have received funding from the European Research Council under the European Union's Horizon 2020 research and innovation program (Grant Agreement n° 757247). https://cordis.europa.eu/project/id/757247

Notes on contributors

Aaron Martin is a postdoctoral researcher on the ERC Global Data Justice project at TILT, Tilburg University.

Linnet Taylor is an associate professor at TILT, Tilburg University. She leads the ERC Global Data Justice project on data governance, representation and social justice.

References

AFP. (2019, September 9). Bangladesh halts new SIM card sale in Rohingya camps. Agence France-Presse. https://news.yahoo.com/bangladesh-halts-sim-card-sale-rohingya-camps-130352363.html

Ahmed, S. I., Hoque, M. R., Guha, S., Rifat, M. R., & Dell, N. (2017, May 6-11). Privacy, security, and surveillance in the Global South: A study of biometric mobile SIM registration in Bangladesh. *Proceedings of the 2017 CHI conference on human factors in computing* systems (pp. 906–918), Denver, Colorado: Association for Computing Machinery.

Amoore, L. (2006). Biometric borders: Governing mobilities in the war on terror. *Political Geography*, *25*(3), 336–351. https://doi.org/10.1016/j.polgeo.2006.02.001

Arendt, H. (1958). *The origins of totalitarianism*. Harcourt Brace.

Arora, P. (2019). Politics of algorithms, Indian citizenship and the colonial legacy. In A. Punathambekar & S. Mohan (Eds.), *Global Digital Cultures: Perspectives From South Asia* (pp. 37–52). University of Michigan Press. https://doi.org/10.3998/mpub.9561751

Atabong, A. B. (2019, July 8). Cameroonian telcos in hot water over SIM card registration. IT Web Africa. http://www.itwebafrica.com/security/797-cameroon/246112-cameroonian-telcos-in-hot-water-over-sim-card-registration

BBC News. (2015, October 26). Nigeria telecom giant MTN fined a record $5.2bn. *British Broadcasting Corporation*. https://www.bbc.com/news/business-34638595

bdnews24. (2015, December 6). Bangladesh launches registration of mobile phone SIMs with biometric details. https://bdnews24.com/bangladesh/2015/12/16/bangladesh-launches-registration-of-mobile-phone-sims-with-biometric-details

bdnews24. (2017, September 23). Bangladesh regulator bans selling mobile SIMs to Rohingya refugees. https://bdnews24.com/bangladesh/2017/09/23/bangladesh-regulator-bans-selling-mobile-sims-to-rohingya-refugees

BFIU. (2019). *Guidelines on electronic Know Your customer (e-KYC)*. Bangladesh Financial Intelligence Unit.

Bowker, G. C., & Starr, S. L. (2000). *Sorting things out: Classification and its consequences*. MIT Press.

Brinham, N. (2018, October 30). "Genocide cards": Rohingya refugees on why they risked their lives to refuse IDs. Truthout. https://truthout.org/articles/genocide-cards-rohingya-refugees-on-why-they-risked-their-lives-to-refuse-ids

Bushell-Embling, D. (2018, March 6). Bangladesh to block 3m registered SIMs. Telecom Asia. https://www.telecomasia.net/content/bangladesh-block-3m-registered-sims

Cassan, G. (2015). Identity-based policies and identity manipulation: Evidence from colonial Punjab. *American Economic Journal: Economic Policy*, *7*(4), 103–131. https://doi.org/10.1257/pol.20130290

CDAC. (2016). Strategic framework. Communicating with Disaster Affected Communities. http://www.cdacnetwork.org/contentAsset/raw-data/044f39c0-3c2c-4583-815b-7e8ea53b2522/attachedFile

Daily Monitor. (2019, October 7). Refugee cards, OPM attestation letters no longer valid for SIM card registration, says UCC. https://www.monitor.co.ug/News/National/UCC-suspends-SIM-card-registration-refugee-cards-OPM-letters/688334-5302436-ftd3ejz/index.html

The Daily Star. (2017, November 7). 5 Rohingyas jailed for selling mobile, SIMs. https://www.thedailystar.net/rohingya-crisis/5-rohingyas-jailed-selling-mobile-sims-1487776

The Daily Star. (2019, January 23). One-third handsets imported illegally. https://www.thedailystar.net/business/telecom/bangladesh-telecom-regulator-mobile-phone-imei-database-launched-legal-import-mobile-handset-1691311

de Koker, L., & Jentzsch, N. (2013). Financial inclusion and financial integrity: Aligned incentives? *World Development*, *44*, 267–280. https://doi.org/10.1016/j.worlddev.2012.11.002

Dencik, L., Hintz, A., & Cable, J. (2016). Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data and Society*, *3*(2), 1–12. https://doi.org/10.1177/2053951716679678

Dhaka Tribune. (2016, April 13). Biometric SIM registration legal. https://www.dhakatribune.com/bangladesh/2016/04/13/biometric-sim-registration-legal

Diaz, M. (2017). Data retention and registration of mobile phones: Chile in the Latin American context. Derechos Digitales. https://www.derechosdigitales.org/wp-content/uploads/Data-Retention-and-Registration-of-Mobile-Phones-.pdf

Donovan, K. P., & Martin, A. K. (2014). The rise of African SIM registration: The emerging dynamics of regulatory change. *First Monday*, *19*(2). https://doi.org/10.5210/fm.v19i2.4351

Dunn, W. L. (2008). *Public policy analysis: An introduction* (4th ed.). Prentice Hall.

The Economist. (2019, September 4). Bangladesh bans mobile phones for 1 m Rohingya refugees. https://www.economist.com/news/2019/09/04/bangladesh-bans-mobile-phones-for-1m-rohingya-refugees

Farraj, A. (2010). Refugees and the biometric future: The impact of biometrics on refugees and asylum seekers. *Columbia Human Rights Law Review*, *42*, 891–942.

Foucault, M. (1976). The will to knowledge: The history of sexuality, volume 1 (trans. R. Hurley, 1998).

Fraser, N. (2008). Abnormal justice. *Critical Inquiry*, *34*(3), 393–422. https://doi.org/10.1086/589478

Gow, G., & Parisi, J. (2008). Pursuing the anonymous user: Privacy rights and mandatory registration of prepaid mobile phones. *Bulletin of Science, Technology and Society*, *28*(1), 60–68. https://doi.org/10.1177/0270467607311487

GSMA. (2016). Mandatory registration of prepaid SIM cards. GSM Association. https://www.gsma.com/publicpolicy/mandatory-registration-prepaid-sim-cards

GSMA. (2017). Landscape report: Mobile money, humanitarian cash transfers and displaced populations. GSM Association. https://www.gsma.com/mobilefordevelopment/resources/mobile-money-humanitarian-cash-transfers/

GSMA. (2018). Access to mobile services and proof-of-identity: Global policy trends, dependencies and risks. GSM Association. https://www.gsma.com/mobilefordevelopment/programme/digital-identity/access-mobile-services-proofidentity-global-policy-trends-dependencies-risks/

GSMA. (2019a). Access to mobile services and proof of identity 2019: Assessing the impact on digital and financial inclusion. GSM Association. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/ProofofIdentity2019_WebSpreads.pdf

GSMA. (2019b, September 10). The digital lives of refugees: Lessons from Uganda. GSM Association. https://www.gsma.com/mobilefordevelopment/country/uganda/the-digital-lives-of-refugees-lessons-from-uganda/

Heeks, R., & Renken, J. (2018). Data justice for development. *Information Development*, *34*(1), 90–102. https://doi.org/10.1177/0266666916678282

Human Rights Watch. (2019, September 7). Bangladesh: Clampdown on Rohingya Refugees. https://www.hrw.org/news/2019/09/07/bangladesh-clampdown-rohingya-refugees

Human Rights Watch. (2020, March 26). Bangladesh: Internet ban risks Rohingya lives. https://www.hrw.org/news/2020/03/26/bangladesh-internet-ban-risks-rohingya-lives

ICRC. (2020). *Handbook on data protection in humanitarian action* (2nd ed.). International Committee of the Red Cross.

ID4D. (2019). About us. World Bank. https://id4d.worldbank.org/about-us

Internews. (2016). Strategic plan. https://internews.org/sites/default/files/Internews_strategic-framework.pdf

Jentzsch, N. (2012). Implications of mandatory registration of mobile phone users in Africa. *Telecommunications Policy*, *36*(8), 608–620. https://doi.org/10.1016/j.telpol.2012.04.002

Kaurin, D. (2019, July 8). Why libra needs a humanitarian fig leaf. Berkman Klein Center. https://medium.com/berkman-klein-center/why-libra-needs-a-humanitarian-fig-leaf-79ae6a463c8

Kazeem, Y. (2019, May 16). MTN is finally listed on the Nigerian Stock Exchange—but its shares will likely be out of reach. Quartz Africa. https://qz.com/africa/1620856/mtn-shares-up-as-finally-listed-on-nigeria-stock-exchange/

Latonero, M., Poole, D., & Berens, J. (2018). Refugee connectivity: A survey of mobile phones, mental health and privacy at a Syrian refugee camp in Greece. *Harvard Humanitarian Initiative and Data and Society*. https://datasociety.net/library/refugee-connectivity/

Libra Association. (2019). Libra white paper. www.libra.org/en-US/white-paper

Lyon, D. (2010). Surveillance, power and everyday life. In P. Kalantzis-Cope & K. Gherab-Martín (Eds.), *Emerging digital spaces in contemporary society* (pp. 107–120). Palgrave Macmillan.

Malakata, M. (2018, May 10). Uganda's comms regulator lifts SIM card ban. IT Web Africa. http://www.itwebafrica.com/security/813-uganda/244198-ugandas-comms-regulator-lifts-sim-card-ban

Martin, A. (2019). Mobile money platform surveillance. *Surveillance and Society*, *17*(1/2), 213–222. https://doi.org/10.24908/ss.v17i1/2.12924

Martin, A., Van Brakel, R., & Bernhard, D. (2009). Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. *Surveillance and Society*, *6*(3), 213–232. https://doi.org/10.24908/ss.v6i3.3282

Milko, V. (2019, September 3). 'Genocide card': Myanmar Rohingya verification scheme condemned. Al Jazeera. https://www.aljazeera.com/news/2019/09/genocide-card-myanmar-rohingya-verification-scheme-condemned-190903012922259.html

Muller, B. J. (2011, June 13). Governmentality and Biopolitics. *Oxford Research Encyclopedia of International Studies*. https://doi.org/10.1093/acrefore/9780190846626.013.50

Murakami Wood, D., & Firmino, R. (2009). Empowerment or repression? Opening up questions of identification and surveillance in Brazil through a case of 'identity fraud'. *Identity in the Information Society*, *2*(3), 297–317. https://doi.org/10.1007/s12394-010-0038-y

Privacy International. (2019, August 5). Africa: SIM card registration only increases monitoring and exclusion. https://privacyinternational.org/long-read/3109/africa-sim-card-registration-only-increases-monitoring-and-exclusion

Rahman, Z. (2019, September 3). Bangladesh cuts access to mobile phone services for the Rohingya. Global Voices. https://globalvoices.org/2019/09/03/bangladesh-cuts-access-to-mobile-phone-services-for-the-rohingya/

Ratcliffe, R., & Ahmed, R. (2020, June 11). Bangladesh urged to lift Rohingya internet ban as Covid-19 rumours swirl. *The Guardian*. https://www.theguardian.com/world/2020/jun/11/internet-ban-sparks-covid-19-rumours-in-rohingya-camp

Richards, D. (1996). Elite interviewing: approaches and pitfalls. *Politics*, *16*(3), 199–204. https://doi.org/10.1111/j.1467-9256.1996.tb00039.x

Rottenburg, R. (2009). Social and public experiments and new figurations of science and politics in postcolonial Africa. *Postcolonial Studies*, *12*(4), 423–440. https://doi.org/10.1080/13688790903350666

Sandvik, K. B., Jacobsen, K. L., & McDonald, S. M. (2017). Do no harm: A taxonomy of the challenges of humanitarian experimentation. *International Review of the Red Cross*, *99*(904), 319–344. https://doi.org/10.1017/S181638311700042X

Scott, J. C. (1998). *Seeing like a state: How certain schemes to improve the human condition have failed*. Yale University Press.

Sen, A. (2007). *Identity and violence: The illusion of destiny*. Penguin Books India.

Sengoopta, C. (2003). *Imprint of the Raj: How fingerprinting was born in colonial India*. Macmillan.

Singh, R., & Jackson, S. J. (2017). From margins to seams: Imbrication, inclusion, and torque in the Aadhaar identification project. In *Proceedings of the 2017 CHI Conference on Human factors in Computing systems (CHI '17)* (pp. 4776–4824). Association for Computing Machinery. https://doi.org/10.1145/3025453.3025910

Songwe, N. (2019). A digital Africa. *Finance and Development*, *56*(2), 27–29. https://www.imf.org/external/pubs/ft/fandd/2019/06/digital-africa-songwe.htm

Sumbwanyambe, M., & Nel, A. (2013, May 29-31). Assessing the implications of SIM card registration policy in the SADC region. *IEEE IST-Africa conference and exhibition (IST-Africa)* (pp. 1–9), Nairobi, Kenya, IEEE.

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

Telecompaper. (2018, March 1). Ugandan govt warns operators of penalties or licence withdrawal for unregistered SIMs. https://www.telecompaper.com/news/ugandan-govt-warns-operators-of-penalties-or-licence-withdrawal-for-unregistered-sims–1234262

UNCDF. (2018). Uganda country assessment on affordable and accessible remittances for forcibly displaced persons and host communities. United Nations Capital Development Fund. https://www.uncdf.org/download/file/127/6633/uganda-refugee-remittances-assessment-report0620v3pdf

UNHCR. (2016). Connecting refugees. United Nations High Commissioner for Refugees. https://www.unhcr.org/5770d43c4.pdf

UNHCR. (2019a). Displaced and disconnected. United Nations High Commissioner for Refugees. https://www.unhcr.org/innovation/displaced-and-disconnected/

UNHCR. (2019b). Displaced and disconnected: Country reports. United Nations High Commissioner for Refugees. https://www.unhcr.org/innovation/displaced-and-disconnected/

UNHCR. (2019c). Uganda. United Nations High Commissioner for Refugees. http://reporting.unhcr.org/node/5129?y=2019#year

UNHCR. (2019d). Bangladesh. United Nations High Commissioner for Refugees. http://reporting.unhcr.org/node/2539?y=2019#year

UNHCR. (2019e, August 20). UNHCR welcomes Uganda Communications Commission directive to improve refugees' access to SIM cards. United Nations High Commissioner for Refugees. https://www.unhcr.org/afr/news/press/2019/8/5d5ba4274/unhcr-welcomes-uganda-communications-commission-directive-to-improve-refugees.html

UNHCR. (2020, January). Uganda: Operational update. http://reporting.unhcr.org/sites/default/files/UNHCR%20Uganda%20Operational%20Update%20-%20January%202020_0.pdf

UNSG. (2014). A world that counts: Mobilising the data revolution for sustainable development. United Nations secretary general. https://www.undatarevolution.org/wp-content/uploads/2014/12/A-World-That-Counts2.pdf

Vassas, Q., & Laïda, N. (2018). Addressing customer due diligence obligation to promote rohingya financial inclusion. Cash Working Group. https://www.humanitarianresponse.info/sites/www.humanitarianresponse.info/files/documents/files/addressing_customer_due_diligence_obligations_to_promote_rohingya_financial_inclusion.pdf

Walby, K. (2013). Institutional ethnography and data analysis: Making sense of data dialogues. *International Journal of Social Research Methodology*, *16*(2), 141–154. https://doi.org/10.1080/13645579.2012.661207

World Bank. (2018, June 5). Cote d'Ivoire and Guinea to Kick-Start West Africa regional identification program. https://www.worldbank.org/en/news/press-release/2018/06/05/cote-divoire-and-guinea-to-kick-start-west-africa-regional-identification-program

Yin, R. K. (2003). *Case study research: Design and methods* (3rd ed.). Sage.