Baki Cakici, Alena Thiel & Ranjit Singh

Chapter 5
The politics of seamlessness: a rights claims perspective on digital identification technologies

1 Introduction

In the past decade, many countries have introduced digital identification systems to facilitate service provision and other state-citizen interactions such as distributing welfare benefits, tracking births, registering residents, and voting in elections. These systems are occasionally linked to physical identification cards in the traditional sense, but increasingly come with their own code cards, card readers, or mobile phone apps. These forms of digitized identification often aspire to function *seamlessly.* The stated goal is for citizens and residents to communicate with state institutions easily, for example to request services or access documentation about themselves. In this chapter, we explore the relationship between seamlessness and political participation as digital identification becomes the invisible background of state-citizen interactions.

We analyze empirical cases drawn from our work with national identification systems in Ghana, India, and Denmark. In each case, we identify the role of seamlessness and describe its political implications for people who use these systems. We agree that such systems make life easier and even increase the possibility of making rights claims for many, but contend that whether this ease represents a significant improvement in their everyday lives remains an open question. There is no straightforward yes/no answer to this question; thus, our efforts in this chapter are oriented toward exploring participation in debates over what kinds of digital identification systems are ultimately built, or even whether such systems should be built in the first place. In short, we seek to provide a political perspective on digital identification systems by arguing that rights claims, not seamless operation, must be a primary concern for designing any technological system that operates at the scale of a nation state.

Content warning: This chapter mentions sexual violence.

https://doi.org/10.1515/9783110787641-006

2 On seamless and seamful technologies

In our experience of and field research into digital identification systems, seamlessness is mostly aspirational on the part of system designers and developers, rather than a regularly realized outcome. This aligns with literature on ubiquitous computing, which points to a mythology of seamlessness[1] that drives the design of digital technologies and calls attention to 'seamfulness' (Dourish and Bell 2011). Although seamlessness is rarely achieved in system design, the *aspiration* to seamlessness occupies considerable labor, mainly by actors who understand the workings of these technologies (Vertesi 2014). In other words, we can never take seamlessness for granted, and when approaching the claims of seamlessness that we encounter in our material, we remain aware of its contingencies and aspirational rhetoric.

A related issue is how digital identification technologies tend to be bundled with infrastructural ambitions. In other words, they aspire to a seamless mode of functioning while also forming the foundation of other technological interventions. To emphasize this dimension, we draw on scholars of infrastructure working in Human-Computer Interaction (HCI), Computer Supported Collaborative Work (CSCW), and science and technology studies (STS), who have articulated the importance of attending to how infrastructures shape inclusion and exclusion. As Inman and Ribes (2019) explain, in scholarship dealing with the design, development and critique of technology, seamfulness and seamlessness have often operated as implicit values, since they highlight the tensions present in notions such as foreground versus background, or visibility versus invisibility (2019, 11).

To study infrastructures is to study the making and management of difference in everyday life (Anand, Gupta, and Appel 2018), and the ability to use infrastructure includes individuals in the group for whom the infrastructure functions seamlessly. As Brian Larkin puts it: "all visibility is situated and what is background for one person is a daily object of concern for another. The point is not to assert one or another status as an inherent condition of infrastructures but to examine how (in) visibility is mobilized and why" (Larkin 2013). The differentiation in visibility also has a disproportionate effect on already marginalized groups. This is because they are not able to access the infrastructure and the benefits that follow, and also because the invisibility of the seamlessly functioning infrastructure makes it difficult to challenge it politically.

[1] This aspirational stance is already visible in early definitions of seamlessness by one of the most influential computer scientists in the field of ubiquitous computing, Mark Weiser (Weiser 1993, cited in Vertesi 2014).

Seamlessness can close off opportunities for political intervention by those for whom the system works as intended; the invisibility of the system makes it an unlikely or elusive target for political action. However, a deeper and much more problematic consequence for rights-based claims is that the assumed seamlessness also forecloses the possibility of political participation for people who experience seamfulness. In other words, when the system works very well for most people, it is all the more challenging for the minority to make their voices heard. There are usually limited opportunities for due process because designers and implementers assume seamlessness. Furthermore, since seamlessness involves a lot of different new and existing components working together, it diffuses accountability because there is always a different component to blame when things do not work (Singh 2021).

In public debates, however, digital identification systems are often discussed in relation to either their technical shortcomings, or occasionally the extent to which they represent an expansion of the surveillance state into the private lives of citizens. While these are important concerns, focusing on them exclusively risks neglecting the political consequences of these systems once they start functioning, consequences that are only amplified if the systems in question do attain a state of seamlessness. Hence the political emphasis of this paper. To address this issue, we draw on literature from STS and critical citizenship studies, and propose foregrounding rights claims by residents and citizens as an essential part of understanding the implications of developing and using digital identification systems at the national level.

While seamlessness is often aspirational, and never achieved without considerable labor in maintenance and repair, some technological systems do occasionally achieve it. Wadmann and Hoeyer (2018) define seamlessness as a state where a well-functioning technology is embedded in a wider infrastructure, enabling easy data collection and exchange. They also point out, however, that achieving seamlessness also comes with risks. Working with seamless systems can blur the sense of control or lead to systems that continue to grow and encompass activities that they were not originally designed for. Wadmann and Hoeyer (2018) describe a Danish case where a nationwide data infrastructure achieved seamlessness, but was not able to establish the means of due process by which its uses could be negotiated, which ultimately undermined its social sustainability. While the efforts to obtain seamlessness made the expansion of the data uses enabled by the infrastructure invisible, they did not erase conflicts of interest or provide means of negotiating the political values underlying the data collection. In this case, seamlessness engendered “an inability to ensure political legitimacy” (2018, 10)[2] rather than situations amenable to technical troubleshooting.

The problems of seamlessness go beyond the simple failure or success of a system. Wadmann and Hoeyer point out that if we consider seamlessness as not only “an ideal of technical operationability but also a source of social instability” (2018, 10), then we must focus our attention on the political mechanisms that mediate our relationship with these technologies. Simply bringing friction back into the system is not the solution; it will only serve to make everyday life difficult.

In the rest of the chapter we take up Wadmann and Hoeyer’s call to attend to the politics of engaging with seamless technologies. We introduce a rights claims perspective to assess the consequences of seamlessness within a political frame. Our point is not that systems should be designed to favor seams or vice versa, or even that one option is preferable to the other. There are always consequences for living with digital identification systems. Instead, our contribution is to describe how we can use the lens of rights claims to investigate the political consequences of technologies operating at a national scale, whether or not this operation is seamless or seamful. We begin with a brief overview of the notion of digital rights claims.

3 Rights-claiming digital subjects

In Being Digital Citizens (2015), Isin and Ruppert draw on critical citizenship studies to argue for the performative nature of citizenship: digital citizens are “those who make digital rights claims” (2015, 18), and the capacity to make such claims turns a digital subject into a citizen (2015, 52). In studies of citizenship, exploration of citizen rights is often organized into three traditional categories: civil rights, such as the right to free speech; political rights, such as voting; and social rights, such as health care (Isin and Turner 2002)

Taking the performative nature of citizenship rights as a point of departure, we offer a practice-oriented unpacking of seamlessness in organizing data infrastructures. Simply put, citizens lacking the ability to access, utilize, and challenge state infrastructures are *lesser* citizens (Singh and Jackson 2021). Political subjects become citizens when they engage and live with public infrastructures. Even if public data infrastructures are invisible and seamless, establishing an ecosystem of rights and obligations for citizens, and a corresponding set of responsibilities

[2] Also see Vezyridis and Timmons (2017) for analysis of a case in the United Kingdom dealing with legitimacy and data sharing.

and due process procedures on the part of state bureaucrats, is crucial in the lived experience of a person who is simultaneously a citizen and a data subject.

Isin and Ruppert, in their work on Being Digital Citizens, show that citizenship and data subjecthood shape each other in three kinds of power relations: obedience, submission, and subversion (2015, 29). 'Subjects *to* power' are dominated; they exist only insofar as they obey. 'Subjects *of* power' submit to power; they become a part of it. This becoming also produces the potential to subvert power. In other words, while being a subject of power requires submission, that very act of submission also provides the grounds for subversion. Thus, the integral paradox of digital citizens' subjectivity is that they are obedient, submissive, and subversive at the same time (2015, 31).

In relation to digital technologies, claiming a right is still an act of obedience and/or submission ("I have a right to this") (c.f. Isin and Ruppert 2015, 25). Rights claims of this type take place when citizens request the state to deliver access to a resource or to provide material support, for example, receiving healthcare or unemployment benefits. We acknowledge that digital systems can make such claims smoother, such as when using an online booking system for medical appointments or keeping in touch with an unemployment office online.

However, following Isin and Ruppert, we pose a different set of questions in relation to digital identification technologies: what actions become possible, what actions can be imagined, and what is encouraged/discouraged? In the cases we investigate, a well-functioning system is equivalent to an invisibly functioning system in the eyes of the designers and developers. The ideal scenario for such a system is one in which the subjects of the technology either never notice that they are using an identification system, or that they only spend minimal effort to get the infrastructure to work for them. For example, fingerprint readers, retinal scanners, or facial recognition are often described in connection to this version of seamless functionality, even when the implementation is far from the aspiration. Regardless, if systems become invisible for most subjects, they also become elusive sites in political struggles to claim rights except when they break down. The space of political negotiation is lost, and many debates quickly turn to technical issues which require a different mode of participation. In such debates, the citizen or resident subjects do not argue on the same grounds as systems designers or developers; the opinions of the latter are often seen as carrying more weight, and sometimes technical competence itself becomes a prerequisite for participating in the debate.

We seek to intervene in this process which makes seamless technologies inaccessible as sites of political negotiation by formulating rights claims as an avenue for access to and visibility of such technologies. Even if the system itself is seamless, there are moments in its operation when its seams become visible and topics of negotiation on an everyday basis. In the following sections, we present three empirical cases to explore these moments and analyze how the notion of seamlessness, either in its aspirational mode or in its practical achievement intersects with the formulation of a particular infrastructural right. To foreground the concern, then, we pose the questions above to our empirical material, and we describe the consequences of bringing politics back into the discussions of these systems. In this way we open these technologies to political intervention by foregrounding the possibilities of rights claims by state subjects.

4 Seamless transition

In 2021, the Danish government started phasing out the old digital identification system *NemID* [EasyID] for the newer *MitID* [MyID]. NemID had been released in 2010 and had evolved to include features such as a mobile phone app. At the time of writing, the transition to MitID is not yet complete and both systems are in use simultaneously. While the identification system is used for a variety of state-provisioned services, the most common use of the app is for daily banking operations and for accessing digital inboxes to receive messages from state institutions as well as other public and private entities.

A major concern in upgrading, changing, or repurposing a national digital identification system is making sure that everyone who moves from the old system to the new system is who they claim to be. In Denmark, the proposed solution for moving users from NemID to MitID was for Danish passport holders to scan their passport using an RFID scanner on their phones. This upgrade path relied on four major assumptions: the person in question is a Danish citizen; they hold a currently valid passport that includes an RFID tag; they own a smartphone equipped with an RFID reader; and that they have sufficient technical expertise to complete the process.

These assumptions divided the population into two groups: those who can upgrade on their own (Danish citizens holding valid issued passports who own relatively new smartphones) and those who must upgrade by visiting the citizen service office in person. This second group contained three further subgroups: Danish citizens who cannot complete the self-service process on their own due to not meeting one of the criteria listed above, non-Danish citizens about whom there is sufficient available data in the population register for the civil servant to perform an identity confirmation, and non-Danish citizens about whom the population register does not hold sufficient data.

This final “migration of users” from NemID to MitID is the culmination of a long process of upgrading NemID that was originally initiated in 2014. From

2017 onwards, the Agency of Digital Government [*Digitaliseringsstyrelsen*] organized annual stakeholder forums where they communicated the progress of the project and asked for input. While the project itself was visible to the public only in the migration from NemID to MitID, in the background it involved the upgrading and integration of other authentication and digital signature systems. In this sense, it was a major infrastructural undertaking that involved many state institutions (DIGST 2017).

As early as 2017, the organizers of the stakeholder forum envisioned the "migration of end users" as a highly important part of the process, and in 2018 provided four migration principles [*Migreringsprincipper*] for the process (DIGST 2018):

1) End-users should use existing NemID to create and sign up for MitID.
2) Ease of use and a "seamless" [*sømløs*] migration is required, with the minimum possible inconvenience to users.
3) The migration flow should help the users as much as possible and there should be "handholding" [*holdes i hånden*] until the migration is complete.
4) The migration must be carried out as one coherent flow where end users are guided and required to make as few decisions as possible.

The notion of seamlessness as expressed in the second principle is an example of the aspirational mode of seamlessness that appears in a wide variety of IT infrastructure projects. However, as with so many other cases of IT projects, the aspiration to seamlessness was not met, and resulting problems led to questions about the process, especially in connection with its planning and efficiency. What we have argued for, however, is a rights-based understanding of this gap. The issue is not that the migration works as planned or not, but that the further we move into this infrastructural process, the more it takes on an air of inevitability. In such a process, technical arguments about the security, efficiency, or some other technical property of the system supersede right-based arguments, and they undermine the citizens' legitimate right to voice their opposition regardless of their technical competence.

Taking a performative perspective on rights, we can see two types of rights claims by state subjects involved in the switch from NemID to MitID. The first type includes the different varieties of upgrade procedures, whether through the mobile phone app using an RFID-equipped Danish passport, or by visiting the citizen service in person, alone or accompanied. The second type is the exact opposite: claimants in this category retain the right to communicate with the state, but are not involved in upgrades and systems changes that appear arbitrary from the perspective of the state subjects. It is this second type of claim that encounters resistance in digitalisation initiatives, because both the platforms on which these systems run and the means for accessing them, for example via mobile phones, are constantly changing.

As with other digitalisation initiatives, the NemID-MitID upgrade has its own politics: any state intervention that requires identification at the individual level is made easier by the existence of an online system that responds to requests immediately. In Denmark, digitalisation narratives are also accompanied by the reduction of opportunities for in-person interactions, with two effects: many rights claims are made by people with access to mobile phones or personal computers, and they take place on platforms designed by the state. If rights claims are the performance of citizenship, in this case citizenship is performed digitally. The second effect is that those who cannot use the devices are left even more isolated than before: since the device makes everyone responsible for their own conduct, those without the means to participate are locked out even from the means to protest at their own exclusion.

A rights claims perspective on identification infrastructure can therefore foreground the political issues surrounding digitalisation. In the Danish MitID case, the initial aspiration to seamlessness gave way to an undesired but not entirely unexpected seamful transition process that was featured on the national news in the form of growing queues at citizen service centers and various technological problems within the system. In the following section, we turn to another national digital identification system and explore our second case where citizens make rights claims by challenging the repurposing of data infrastructures.

5 Seamless repurposing

Bureaucracies use specific eligibility criteria to identify a particular group of citizens (say, individuals ‘below the poverty line’) for delivery of services (say, distribution of social welfare, employment, health insurance and so on). Once eligibility is confirmed, citizens are issued an identity document that allows them to claim identity and eligibility together with respect to a government service. At the same time, this process of confirming eligibility has its own requirements for some form of identification. Thus, identity and eligibility are often tightly coupled in government services. The appropriation of digital identification systems has slowly decoupled this relationship. Such decoupling is exemplified in the design of Aadhaar, India’s biometrics-based national identity database, where identification is imagined as a government service in and of itself, rather than a mechanism to facilitate last-mile delivery of other government services (Nilekani and Shah 2016). While identity documents are generally connected with a particular bureaucratic function of the state, Aadhaar's design unbundles this connection and makes it secondary to unique identification of an Indian resident.

Unique identification is not an end; it is a means to several ends. It creates the conditions of possibility for repurposing digital identification systems for any bureaucratic function. Such repurposing raises its own set of challenges. To begin with, as the scope of using a digital identification system expands, so does the scale of the challenges faced by people who struggle to claim their identity through such systems. Furthermore, repurposing raises questions around the *appropriate* circulation of digital identity, which is often contingent on "context-relative informational norms" (Nissenbaum 2009, 127). Controversies over determining what is appropriate during repurposing are deeply consequential for the seamless operation of digital identification systems. They not only make the inner workings of such systems an object of debate and intense scrutiny, but also bring out the differences in normative assumptions around their operation, use, and future(s). The controversy over whether or not investigative agencies can use the Aadhaar database (Venkatanarayanan 2018; Reddy 2018) is a stark example of this tension.

Aadhaar is a unique number assigned to every enrolled individual based on their biometric (ten fingerprints, two irises, and facial photograph) and demographic (name, age, gender, and residential address) data in India (UIDAI 2010). The rationale for using Aadhaar in criminal investigations draws on the extensive use of fingerprinting in criminal forensics, which has historically gained gradual acceptance and credibility in criminal courts across the world (Lynch et al. 2008; Cole 2001). Aadhaar, however, was never geared towards criminal forensics; the Unique Identification Authority of India (UIDAI, the government body in charge of implementing Aadhaar) has consistently claimed that Aadhaar is designed only for the purposes of civil identification and denied the possibility of using the database for criminal investigations (TNN 2018).

In January 2013, to investigate the rape of a seven-year-old girl in the toilet of a school in Goa, the Central Bureau of Investigation (CBI), India's foremost investigating agency, requested the biometric information of every Aadhaar-enrolled person in the state. It later modified its request to access the biometric information of three suspects. Finally, upon recovery of some chance fingerprints from the crime scene, it changed its request again to ask UIDAI to run the fingerprints against the whole database to find a match (UIDAI 2014). A local court in Goa also ordered the UIDAI to comply with the CBI's request. UIDAI first appealed against this order in the Mumbai High Court. It cited two reasons for its refusal to share biometric information: "One, that such a move would violate privacy of the number-holders. And two, that its biometric database and deduplication systems are not designed for forensic inquiries" (Rajshekhar 2014). It also claimed that following these orders "will open the floodgates of such directives by other courts as well other authorities" (Anand 2014). After the Mumbai High Court rejected its appeal, the UIDAI petitioned the Supreme Court on the grounds of: (1) the distinct possibility of false identification: "Any such random search [...] would put lakhs [100 thousands] of innocent people under the scanner" (UIDAI 2014, 27); and (2) "Building a system that can search using latent fingerprints, quite like criminal database searches, is not within the constitutional and legal mandate and scope of UIDAI and fundamentally against the core reason residents have provided their data voluntarily to UIDAI" (UIDAI 2014, 33). On 24 March 2014 the Supreme Court issued a stay order on the Mumbai High Court judgement that prohibited the UIDAI from divulging biometric information to any agency without the resident's written consent. This controversy emerged before the 2016 passage of the Aadhaar Act (Ministry of Finance 2016), which restricted the use and sharing of biometric information stored in the Aadhaar database. In the absence of this law restricting the scope of repurposing Aadhaar, the controversy over using it for criminal forensics was inevitable.

The passage of the Aadhaar Act, however, did not end the controversy over the use of Aadhaar in criminal investigations. The Supreme Court, in its final judgement on the public interest litigations against Aadhaar in 2018, read down a provision in the Aadhaar Act prohibiting disclosure of biometric information except in cases of a court order from District Judge level or above. It clarified that, "an individual, whose information is sought to be released, shall be afforded an opportunity of hearing. If such an order is passed, in that eventuality, he shall also have right to challenge such an order passed by approaching the higher court [...] on accepted grounds in law" (Justice K.S. Puttaswamy and Anr. vs. Union of India and Ors. 2018, SC India, 558–559). Effectively, the Court ruled that, "it is constitutional to use the Aadhaar database for criminal investigation [creating ...] more pressure on the UIDAI to co-operate with investigative agencies" (Reddy 2018). The controversy emerged again in New Delhi when police filed a request with the High Court in February 2018 to access the Aadhaar database to compare chance fingerprints and CCTV footage obtained from a murder scene with its entire biometric dataset. The UIDAI has persisted in its position that Aadhaar cannot be used for criminal investigations (Ahsan 2022).

While the investigative agencies in India have sought to run chance fingerprints obtained at the scene of crime against the entire Aadhaar database, the Supreme Court has only allowed the ability to compare chance fingerprints with Aadhaar data of a particular suspect after they have been granted an opportunity to meaningfully participate in the investigation. The Court did not explicitly prohibit the use of Aadhaar for criminal investigations; it articulated the right of any person to challenge the decision of a court to allow the repurposing for their Aadhaar data for criminal investigations.

This case introduces a number of instances in which citizens can make rights claims to challenge the implementation of Aadhaar (in general) and its repurposing (in particular). To begin with, the right to file a public interest litigation in the Supreme Court of India or the High Courts of respective Indian states to challenge government policies also affords, by extension, Indian citizens the right to question and debate in the court what kind of digital identification systems are built and whether they should be built in the first place. Furthermore, this broadening of any citizen's standing in the courts as an affected party further provides citizens with the ability to challenge any repurposing of Aadhaar in India. The court's judgement on the use of Aadhaar in criminal investigation also serves to provide a citizen with the right to challenge the use of their Aadhaar data for criminal investigations without their consent. This right is intended to make repurposing seamful and add friction in its functioning to ensure that it is made possible only after due process. Claiming this right is not only an act of submitting to the authority of the courts as a constitutive part of the Indian state, but also an act of subverting the seamlessness of its data infrastructures. In our third case, we explore such frictions extensively in the implementation of a novel ID system in Ghana.

6 Seamless redress

Of the three cases presented in this chapter, the Ghanaian national ID infrastructure is the most seamful – as a consequence of the *longue durée* of colonial disinvestments in civil registration architecture (Szreter and Breckenridge 2012, 27), the collapse of earlier attempts at building paper-based registration systems, and the ongoing political contestation around ownership and direction in the country's emerging digitalization agenda (Thiel 2020). Seamlessness therefore first and foremost features as an aspiration and operational principle: Ghana's identification agenda has historically been fragmented, with various biometric registers being developed side by side in the 2010s. Since 2017, the high-priority political project of re-integrating the national ID ecosystem has sought to subsume these predominantly incomplete registers under a single personal ID number and biometric ID card, the "Ghanacard" (see all mandatory documents for the national biometric ID as laid out in the National Identity Register Amendment Act, Act 950, 2017). Besides replacing competing ID cards in the health and social security systems, as well as the tax administration, the Ghanacard and associated ID number have since forcefully been linked to all mobile payment systems (paving the way to their subsequent taxation under the e-levy scheme), the highly contested re-registration of SIM cards, GPS-based digital addressing data, as well as the maternal and child health records used to assign national ID numbers at birth to every institutionally attended newborn.

Both the general population and civil society groups have responded with growing frustration to the perpetual expansion of what are officially presented as identification "services". On 25 November 2022, one user posted on the Ghanaweb online forum: "Ghana Card for bank accounts, for mobile phone SIM registration, for vaccination, for Social Security, for police database, for bit by bit, for on and on…you become a blockchain digital person with no legal rights." Others criticized the accumulating social and economic cost of repeated registrations and, crucially, their cascading exclusive effects on basic rights, particularly since registration for the Ghanacard is experienced unevenly across the population. In the words of one urban trader: "I rely on the medical system due to my health. But before I can go to the hospital I have to renew my card, stand in line a whole day whilst I am sick." Another urban professional recounted his family's experience. Contrary to the official claim, "the ID cards are not instantly issued. My son turned eighteen so together with his brother we went to register in [the local registration center]; six months later I was called to pick up my card all the way across town, near Dome [a suburb north-east of Accra]; my youngest son received his card in Achimota while the eldest has not received it at all." Beyond such immediate frustrations, interviews with digital rights groups in Ghana revealed further concerns about the potential abuses of the automation of identification in state-citizen interactions. Liberal policy think tank IMANI, for example, anticipated a fundamental redistribution of social wealth through the creation of new types of taxpayers as a consequence of linking IDs and addresses (IMANI 2016). Referring to the newly introduced biometric driver's license, another activist group worried that biometric matching with the national ID and address register would encourage traffic police to further extort bribes. "Imagine if they can just threaten to follow you home,".

We have argued above that seamlessness excludes certain knowledges from public purview. As Horn (2011, 106) has cautioned with reference to Carl Schmitt, such invisibility and the secrecy it entails "serves to protect and stabilize the state, and as such it is the precondition for the functioning of the law; but at the same time secrecy opens a space of exception from the rule of law, an exception that can breed violence, corruption and oppression." For this reason, we argue, every public data infrastructure must have a robust bug reporting policy and mechanisms to contest harm and adjudicate liability. Ghana's National Identity Register Act (Act 750, 2008) and Data Protection Act (Act 843, 2012) have made provisions for reporting grievances through the Data Protection Commission and the courts. However, the provisions made for such rights claims have effectively been rendered dysfunctional because of several factors. During her keynote at the 2017 Africa Open Data

Conference in Accra in the function of the (then) Data Protection Commissioner and lead author of Ghana's communication legislation, Teki Akuetteh Falconer expressed her conviction that data protection should serve an enabling function rather than restricting government reach into personal information. Similarly, court cases contesting the ID agenda have regularly been decided in favor of the government and failed to acknowledge fundamental concerns around digital rights. For example, legal contestation of the 2017 amendment of the National Identity Register Act suggested that the additional requirement for the new mobile app- and GPS-based digital residential address in the ongoing national ID registration had severe exclusionary effects. However, concerns around low smartphone and internet penetration, but also the de facto denationalization of nomadic and homeless populations did not factor into the court's decision (Ghana News Agency 2019), which rejected the claim purely on procedural grounds and was hence widely considered a political decision. Equally, the – suspiciously – unanimous 2020 Supreme Court ruling on the legitimacy of the Electoral Commission's decision to limit voter registration to those issued the biometric Ghanacard has been described as politically motivated (Rickard 2020), and awarded the Supreme Court the mocking designation of "FC Unanimous" among the Ghanaian public.

At this moment, the pursuit of seamlessness itself constitutes the object of Ghanaians' legal claims, largely mobilizing the technical registers flagged in our literature discussion. It is not difficult, however, to anticipate how seamless population registers, once attained, might impact the possibility of redress. As access to the legal justice system is costly and time-intensive, we observed Ghana's digital citizens resorting to subversive tactics such as double registration (e.g., in the birth register) in order to navigate system-inherent frictions under a new identity, knowing very well that this creates further bureaucratic tensions along the lines. With the envisioned seamless integration of population registers, this problem is almost certain to grow as the potential for exclusion multiplies. At the same time, citizens do opt for the courts as a strategy to produce visibility through the legal contestation of grievances as a political act in and for itself.

The case of Ghana shows how rights claims associated with the pursuit of seamless infrastructuring are distributed beyond formal juridico-political mechanisms and include various legal and political vernaculars. Yet, while grievance reporting in Ghana has suffered at the hands of the politicization of institutions and the public's frustration over the emerging ID infrastructure, this analysis is not prescriptive. Different institutional and techno-political conjunctures, such as the high level of trust in Danish state institutions, ultimately generate different opportunities for grievance reporting and redressal. Our comparative effort reveals how such infrastructural and cultural conjunctures expand purely institutionalist perspectives.

7 Tracing the politics of seamlessness

In this chapter, the invisibility of seamless technologies was one of our points of departure. We argued that a focus on seamlessness tends to produce systems that are difficult to challenge by digital citizens. To foreground this elusiveness, we adopted a rights claims perspective and analyzed three cases from our research into digital identification systems in India, Denmark, and Ghana. Our analysis points to two interesting sites for unpacking the politics of seamlessness: the negotiations of seamlessness, whether at design meetings or in public debates; and the experiences of those who encounter the seams of the system through other categories of exclusion or due to changes in the system.

Our position can be read broadly as a challenge to seamlessness insofar as this forecloses the possibility of political participation. We acknowledge that seamless systems can allow for rights claims by a wider group of state subjects, or where a previously difficult-to-exercise right becomes easier through a system that seems to work seamlessly. Yet, especially when seamlessness allows for rights claims to take place invisibly, we must still ask: what are the consequences of such invisibility for political subjectivities?

To answer this question, we proposed a practice-oriented focus on rights claims that moves our attention to mundane and often creative tactics of subversion and multiple forms of creating visibility, e. g., the Danish news reports, Indian and Ghanaian courts, and the Ghanaian public mocking the state. Adopting a practice-oriented approach allowed us to explore how technologies encourage or discourage new political imaginaries and actions, regardless of whether they work seamlessly. Across our highly diverse cases, digital citizens skillfully subvert initiatives of seamlessness. In all these cases (in)visibility is mobilized in unexpected sites, and hence is far from a monopoly of public authorities. Danish "analogist" initiatives performatively opt out of digital communication (Balslev and Kjærulff 2023), while Ghanaian digital citizens who navigate seamful systems through adopting multiple identities effectively, though likely without intention, evade the Ghanaian state's vision across registers. And in contrast to the Ghanaians' distrust of supreme court rulings on matters of national ID, the Indian SC limiting disclosure of personal information represents an internationally recognized example of a formal type of subversion. While subversion in this judicial form tends to be captured as obedience in that it still reproduces the categories of state vision, these forms of participation sometimes do open the black box of seamless systems and provide novel grounds for citizen engagement as they bring to the fore otherwise elusive implications of digital identification systems. What remains challenging in such contestations, however, is to bring designers/developers and citizens/data subjects into the same arena.

References

Ahsan, S. (2022). ‘Explained: why, according to UIDAI, Aadhaar data can’t be used in police investigations’. *The Indian Express*, 10 May 2022. https://indianexpress.com/article/explained/explained-why-according-to-uidai-aadhaar-data-cant--be-used-in-police-investigations-7908345/.

Anand, N., Gupta, A. and Appel, H. (2018). *The promise of infrastructure.* Durham: Duke University Press.

Anand, U. (2014). ‘Stop Aadhaar data use to probe crime: UIDAI to SC’, *The Indian Express*, 19 March 2014.

Balslev, J. and Kjærulff, A. (2023). ‘Analogiseringsstyrelsen’. https://analogist.dk/om/.

Cole, S. A., (2001). *Suspect identities: a history of fingerprinting and criminal identification.* Cambridge, MA: Harvard University Press.

DIGST. (2017). ‘Interessentforum for næste generation NemID – 20. januar 2017’. Presented at the Interessentforum for næste generation NemID, 20 January.

DIGST. (2018). ‘Interessentforum for næste generation NemID – 21. marts 2018’. Presented at the Interessentforum for næste generation NemID, 21 March.

Dourish, P. and Bell, G. (2011). *Divining a digital future: mess and mythology in ubiquitous computing.* MIT Press.

Ghana News Agency (2019). ‘Court endorses NIA’s demand for digital address code’. GhanaWeb. 24 April. https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Court-endorses-NIA-s-demand-for-digital-address-code-740836.

Horn, E. (2011). ‘Logics of political secrecy’, *Theory, Culture & Society* 28 (7–8), 103–22. https://doi.org/10.1177/0263276411424583.

IMANI. (2016). ‘IMANI report: don’t mess up the national ID system’. 2 August. https://imaniafrica.org/2016/02/08/imani-report-dont-mess-up-the-national-id-system/.

Inman, S. and Ribes, D. (2019). ‘” Beautiful seams,” strategic revelations and concealments’, in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1–14).

Isin, E. F. and Turner, B. S. (2002). ‘Citizenship studies: an introduction’, in E. F. Isin and B. S. Turner (eds.), *Handbook of citizenship studies* (pp. 1–10). SAGE.

Isin, E. F. and Ruppert, E. (2015). *Being digital citizens.* Rowman & Littlefield.

Justice K.S. Puttaswamy and Anr. vs. Union of India and Ors. (2018). Writ Petition (Civil) No. 494 of 2012, SC India.

Larkin, B. (2013). ‘The politics and poetics of infrastructure’, *Annual Review of Anthropology*, 42, 327–343.

Lynch, M., Cole, S, McNally, R. and Jordan, K. (2008). *Truth machine: the contentious history of DNA fingerprinting.* Chicago: University of Chicago Press.

Ministry of Finance. (2016). *The Aadhaar (targeted delivery of financial and other subsidies, benefits and services) Bill.* http://www.prsindia.org/billtrack/the-aadhaar-targeted-delivery-of-financial-and-other-subsidies--benefits-and-services-bill-2016-4202/.

Nilekani, N. and Shah, V. (2016). *Rebooting India: realizing a billion aspirations.* UK edition. London: Allen Lane.

Nissenbaum, H. (2009). *Privacy in context: technology, policy, and the integrity of social life* (1st edition). Stanford, CA: Stanford Law Books.

Rajshekhar, M. (2014). 'SC Aadhaar verdict highlights data protection weaknesses'. *The Economic Times*, 25 March. https://economictimes.indiatimes.com/news/politics-and-nation/sc-aadhaar-verdict-highlights-data-protection-weaknesses/articleshow/32644798.cms.

Prashant Reddy, T. (2018). 'Did SC re-affirm that Aadhaar database could be used for criminal investigations?'. *The Wire*, 16 October. https://thewire.in/law/supreme-court-aadhaar-database-criminal-investigations.

Rickard, C. (2020). 'Allowing birth certificates for voter ID would be a "retrograde step" – Ghana's Supreme Court. African Legal Information Institute'. *African LII.* 22 July. https://africanlii.org/article/20200722/allowing-birth-certificates-voter-id-would-be-%E2%80%98retrograde-step%E2%80%99-%E2%80%93-ghana%E2%80%99s-supreme.

Singh, R. (2021). 'A new AI lexicon: imbrication'. *A New AI Lexicon* (blog). 13 July 2021. https://medium.com/a-new-ai-lexicon/a-new-ai-lexicon-imbrication-40b380dafa35.

Singh, R. and Jackson, S. (2021). 'Seeing like an infrastructure: low-resolution citizens and the Aadhaar identification project', *Proceedings of the ACM on Human-Computer Interaction* (5) (CSCW2), 315: 1–26. https://doi.org/10.1145/3476056.

Szreter, S. and Breckenridge, K. (2012). *Registration and recognition.* British Academy.

Thiel, A. (2020). 'Biometric identification technologies and the Ghanaian "data revolution"', *The Journal of Modern African Studies* 58(1), 115–136. https://doi.org/10.1017/S0022278X19000600.

TNN. 2018. 'UIDAI rejects NCRB plea for database access'. *The Times of India*, 23 June. https://timesofindia.indiatimes.com/india/uidai-rejects-ncrb-plea-for-database-access/articleshow/64705340.cms.

UIDAI. 2010. 'UIDAI strategy overview: creating a unique identity number for every resident in India'. New Delhi: Unique Identification Authority of India (UIDAI). https://www.dropbox.com/s/eg9p5uzucsd9t5r/UIDAI_Strategy_Overview_2010.pdf?dl=0.

UIDAI. (2014). 'Petition by UIDAI in the matter of UIDAI and Anr. vs. CBI and Anr. (Special Leave Petition (Criminal) No. 2524 of 2014)'. New Delhi: Supreme Court of India. https://www.dropbox.com/s/27gtzub8hk7ko8r/UIDAI and Another Vol 1.pdf?dl=0.

Venkatanarayanan, A. (2018). 'Fingerprints, Aadhaar and law enforcement – a deadly cocktail is in the making'. *The Wire*, 16 August. https://thewire.in/tech/aadhaar-fingerprints-ncrb-police-investigations.

Vertesi, J. (2014). 'Seamful spaces: heterogeneous infrastructures in interaction', *Science, Technology, & Human Values* 39(2), 264–284. https://doi.org/10.1177/0162243913516012.

Vezyridis, P. and Timmons, S. (2017). 'Understanding the Care.Data conundrum: new information flows for economic growth', *Big Data & Society* 4(1) 2053951716688490. https://doi.org/10.1177/2053951716688490.

Wadmann, S. and Hoeyer, K. (2018). 'Dangers of the digital fit: rethinking seamlessness and social sustainability in data-intensive healthcare', *Big Data & Society* 5(1) 2053951717752964. https://doi.org/10.1177/2053951717752964.