ACE SOAS Consortium Anti-Corruption Evidence
Making Anti-Corruption Real

Working Paper 015

Digital identities: a political settlements analysis of asymmetric power and information

Mushtaq Khan,[1] Pallavi Roy[2]

October 2019

[1] Department of Economics, SOAS University of London, mk100@soas.ac.uk
[2] Centre for International Studies and Diplomacy, School of Interdisciplinary Studies, SOAS University of London, pr16@soas.ac.uk

Contents

Tables

Executive summary

Digital identity systems are being enthusiastically adopted in Africa and Asia as a response to corruption, inefficient service delivery, high costs of doing business, and security threats. The expectation is that by establishing the identities of citizens and their entitlements and responsibilities, these systems will reduce the information asymmetries that allow rules to be violated. However, this assumes that developing countries have a rule of law that ensures that evidence on violations will lead to enforcement regardless of the identity and power of the violator.

Debates in the United Kingdom and other advanced countries have centred around appropriate regulation and have been driven by the concern that identity data linked to multiple databases can lead to a loss of privacy that is not justified by improvements in security. But when the rule of law is weak – such is often the case in developing countries – there is the additional possibility of a *deliberate misuse of data* by the powerful, leading to rent extraction or political exclusion of different types. These are qualitatively different concerns and require a different analytical frame for assessing the likely impact of digital identity systems.

In many developing countries we observe variants of rule *by* law, where enforcement has a higher likelihood of success when it benefits the more powerful party. In such contexts, reductions in the asymmetry of information achieved by digital identity systems can have anomalous effects, depending on the type of violation and the relative power of the parties involved. For some types of violations digital identity systems can have significant positive social effects, for example by mobilising the powerful to change rules in order to improve compliance and reduce fraud. However, for an important subset of violations, better information can strengthen the asymmetric power of extractive groups and support their ability to exclude and repress others further. Such systems can also contribute to economic exclusion through what we describe as the 'premature formalisation' of informal, small and medium-sized enterprises.

We develop an analytical framework to explain the anomalous effects of digital identity systems, reviewing the available literature on relevant systems in Asia and Africa. We consider the need for asymmetric power analysis alongside asymmetric information analysis to understand the causes of, and possible policy responses to, rule violations, and introduce the political settlements framework as a lens for understanding the differences between digital governance and data concerns in developed countries compared to advanced countries. The theory and evidence suggest that a more robust analysis, which recognises the interdependence of asymmetric information and power, can assist in the design of country-specific, welfare-enhancing digital strategies.

List of Acronyms

BJP	Bharatiya Janata Party (India)
GST	Goods and services tax (India)
ID	Identification
IT	Information technology
MSEs	Micro and small enterprises
NRC	National Register of Citizens (India)
SMEs	Small and medium-sized enterprises
UIDAI	Unique Identification Authority of India
UID	Unique identity number

1. Introduction

Digital identity systems create unique identity numbers (UIDs) for each citizen linked to their unique biometric data. These numbers can then be linked to data on welfare rights, tax contributions, bank accounts and so on, creating a powerful tool to assist the enforcement of the formal rights, taxes, social entitlements and other responsibilities of citizens. Applications include tackling corruption and fraud in public delivery systems, creating new markets by reducing transaction costs and improving national security (World Bank 2014). Digital identities have been used to try to improve the delivery of public services, reduce election fraud, create and expand markets, improve security, accelerate formalisation, improve tax collection, and improve regulatory compliance. However, the evidence is mixed: in some areas digital identity systems have reduced corruption, improved service delivery and increased market activities by making it easier to establish identity, but they have also contributed to increasing economic and political exclusion in other areas. The potentially positive role of digital identity is based on the possibility of reducing the asymmetry of information, enabling some of the transaction costs of formal contracts to be reduced and contract violations to diminish. But these expectations are based on a number of critical assumptions.

The primary assumption is that the society has a *rule of law*, by which we mean that the detection of violations will lead to enforcement regardless of the relative power of the violator and the injured party. With a rule of law, information is indeed power. Unfortunately, most countries, particularly developing ones, do not have a rule of law and at best have some variant of a rule *by* law (Khan 2010, 2018; North, et al. 2007; North, et al. 2009). In the latter, laws and institutions are unequally enforced and the chances are that the powerful will enforce rules on the less powerful, but not necessarily, or always, the other way around. For instance, the prime minister may be able to get the anti-corruption commission to prosecute the leader of the opposition (who may indeed be corrupt), but the leader of the opposition is unlikely to be able to get the anti-corruption commission to prosecute the prime minister (who may also be corrupt). These power asymmetries can run right through society, with more powerful or better-connected individuals and organisations having a systematic enforcement advantage over less powerful ones. In these societies, the detection of contract violation does not necessarily lead to enforcement unless the aggrieved party is more powerful than the violating party.

In rule-by-law societies, the relationship between asymmetric information and asymmetric power can be complex. A reduction in information asymmetries, for instance due to digital technologies, may *reduce* power asymmetries in some areas, but it may also result in power asymmetries *increasing* in other areas. The distribution of power in a society or sector, which we describe as the political settlement, is likely to determine what happens to enforcement if information improves. As a result, the specific application of digital identities can determine the welfare impact. In some applications, the use of digital identities can shift the balance of power further against already excluded groups. For instance, it could result in premature formalisation that makes low-productivity activities go out of business and result

in greater economic exclusion or create new opportunities of rent extraction and political control for powerful groups that results in greater political exclusion. Adverse effects of these types may outweigh welfare-enhancing enforcement gains elsewhere. This makes it important to examine the interdependence of information and power, particularly in the context of societies where power is very unequally distributed to begin with, and the rule of law is weak. In these cases, contract violations based on asymmetries of power cannot be addressed by reducing asymmetries of information, and the latter may actually make matters worse for some types of violations. Other strategies have to be considered, including directly addressing structural power asymmetries.

International development partners including the World Bank have been promoting the advancement of digital identities in developing countries, particularly in Africa, without always understanding the complex relationships between asymmetric information and power in contexts of a weak rule of law. According to the World Bank, Africa accounts for around 15% of the world's population but around half of the world's population without legal national identification (NID), and is therefore particularly in need of developing these systems (World Bank 2017: 4, 2014). The experience of India with its well-developed Aadhaar identity system – which gives every citizen a unique identity number linked to multiple databases – is often used as an exemplar of the advantages that can follow. Aadhaar has multiple objectives, including improving the efficiency of transfers and service delivery (particularly to the poor), reducing resource leakages, and improving security, but it has also been used in other ways that are more questionable and has contributed to widening the asymmetries of power in important dimensions.

Based on their reading of experiences of countries like India, the World Bank's *Digital identity toolkit* encourages African states to invest in identity infrastructure as 'digital identity, or electronic identity (eID), offers developing nations a unique opportunity to accelerate the pace of their national progress. It changes the way services are delivered, helps grow a country's digital economy, and supports effective safety nets for disadvantaged and impoverished populations' (World Bank 2014: vii). It goes on to say: 'Today's modern society creates new demands on identity: identity has to be mobile, transactional, interoperable, portable, and social – in addition to being secure'. The report recognises that there are issues of privacy and trust but assumes that these can be addressed by legislation and regulatory frameworks. Similarly, it is optimistic about the commercial benefits of mobile and transactional identity data and ignores the challenges of regulating the concentrations of market power that are likely to follow. Most importantly, it ignores the limited efficacy of regulations as a way of protecting the misuse of data in countries where the rule of law is weak. This does not mean that we should be opposed to digital identity systems, but we need a more robust analytical framework to assess the opportunities and dangers.

Advocates of digital identity point out the evidence from Aadhaar and other early adopters which shows that leakages of cash transfers meant for the poor have indeed declined in some contexts and that digital identities have reduced transaction costs, for instance in setting up bank accounts for previously excluded groups (Gelb and Clark 2013; Department

of State 2011: 7; GSMA 2017; Muralidharan, et al. 2017). However, there is also evidence that the linking of identities to tax, welfare and other databases can make informal businesses unviable as a result of premature formalisation (Dibben, et al. 2015; La Porta and Shleifer 2014). More worryingly, access to identity data can allow the powerful to control opposition more easily or to expropriate from particular groups more effectively, with adverse impacts on political and economic inclusion (Bukari and Schareika 2015; Ragas 2017). In extreme cases, these systems make it technically possible to rapidly deprive targeted groups of the rights and services required for everyday life. In the context of ethnic and religious conflicts and contestations over citizenship, digital identities can be used to deprive targeted groups of access to banking, public-sector jobs, land transactions and the operation of sim cards, allowing coercive repression for political ends that, in extreme cases, can facilitate ethnic cleansing at the push of a button. A holistic analysis of the benefits and dangers of digital identity systems is therefore necessary, particularly in the context of the growing authoritarianism in many developing countries. It should be of particular concern that many authoritarian governments in developing countries are at the forefront of advancing and adopting digital identity systems.

Digital identity cards have been rejected in a number of advanced countries because of their implications for privacy. There is also a pressing and related regulatory challenge in advanced countries as a result of the use of 'big data' by first-mover companies, which can create insurmountable entry barriers simply as a result of network economies of scale. The involvement of private-sector companies in designing digital identity systems in developing countries raises equivalent concerns. Although the appropriate regulatory response in advanced countries is not yet known because network economies raise new problems of defining the sources of monopoly power (as they are no longer based on directly preventing entry into markets), the expectation is that once the regulatory framework is agreed upon, it will be enforced. In developing countries, the challenge is more severe. If the rule of law is weak, regulatory solutions will not necessarily work because the regulations themselves will be difficult to enforce. The appropriate strategy may be to determine the *pace* of digitisation, and the *uses* to which digital identities should be restricted in different contexts.

In section 2 we look at some of the privacy and data concerns in advanced countries and the differences between the digital governance concerns in advanced and developing countries. In advanced countries the concern is primarily with appropriate forms of regulation but in developing countries this is insufficient to assure desirable outcomes. In section 3 we consider the need for asymmetric power analysis alongside asymmetric information analysis to understand the causes of, and possible policy responses to, rule violations. We introduce the political settlements framework as a lens for understanding the differences between digital governance and data concerns in developed countries compared with advanced countries. In section 4 we develop an analytical classification of various types of rule violations in developing countries and describe the expected outcomes of enforcement using digital identity systems in each case. We review the available evidence on the rule violation to show that the empirical evidence supports our analytical expectations. To conclude, section 5 outlines some of the implications of our analysis for the global discussion around digital identity systems and appropriate strategies for development partners.

2. Digital identity and data issues in advanced and developing countries

The potentially negative outcomes that can be triggered by digital identity systems have been of concern in advanced countries, but for different reasons than in developing countries. The United States, United Kingdom and Canada were at the forefront of developing digital identity systems in the aftermath of the Twin Towers attacks in New York in 2001. The aim was to improve the identification or exclusion of aliens and to track domestic suspects, however it was also hoped that there would be profitable opportunities for deploying identity data in service delivery. But very soon enthusiasm began to wane as privacy implications came to the fore. The UK Parliament's Select Committee on Home Affairs recommended in 2004 that the proposed national identity system should go through 'exhaustive testing' of biometric technology and vetting by experts to ensure there were no unexpected adverse effects (House of Commons Home Affairs Committee 2004: para 175 of Conclusions and Recommendations). After extensive technical discussions, including the evaluation of available evidence, the Conservative–Liberal Democrat coalition government terminated the UK's identification (ID) card plans in 2010, describing it as unnecessarily 'intrusive' (Guardian 2010).

The debates in the UK and other advanced countries have been driven by the concern that identity data linked to multiple databases can lead to a loss of privacy that is not justified by improvements in security or service-delivery outcomes. Privacy is a code-word for saying that perfectly legitimate individuals may have on their records innocent events that they do not wish to explain to public officials. Moreover, by linking records, individuals may be picked up and forced to account for 'red flags', activities or transactions that serve no public purpose. Once multiple databases are linked to identities, it is also hard to prevent 'function creep', for instance sharing data with new agencies in areas like surveillance and security. If information is acted upon that is inaccurate, inadequately checked, or based on inappropriate red flags, this information may not be easy to correct, even when there is a rule of law, because individuals may not be aware that they are being tracked or why they have been prevented from engaging in some activities or transactions.

Services based on digital identities are also prone to the concentration of market power even in advanced countries. First-mover companies are likely to enjoy huge network economies of scale because the more information a network can process or provide, the more attractive that network becomes for new customers. This can result in enormous market power emerging in entirely lawful ways, as in the case of the FAANGs (Facebook, Apple, Amazon, Netflix and Google/Alphabet) (Economist 2019a). Regulators in advanced countries are still grappling with the challenge of constraining these concentrations of market power in the public interest. The challenge is that this market power is not based on preventing entry into markets, on the contrary, the network economies allow first movers to provide better and cheaper services but also gives them huge power that may be socially undesirable. Banking is emerging as the next frontier for digital disruption, and new sources

of market power are likely to emerge in advanced countries over the next decade (Economist 2019b). Emerging asymmetries in market power are, however, second-order problems in developing countries compared to the illegitimate misuse of data by the politically powerful. Nevertheless, market-power issues can also affect developing countries. In particular, the growth of the digital economy in these countries can depend on identity data since other forms of identity-checking may be weak. This is already resulting in partnerships between private companies and states in developing digital identity systems, which can give first-mover companies significant market power. This can be doubly problematic if the rule of law is also weak.

The concern in advanced countries is not that the politically powerful will illegitimately or illegally misuse information, because rules on how information can be collected and used are likely to be enforced. Rather, the concern may be that the data analysis may intrude on privacy or result in concentrations of market power when commercialised. Even with a rule of law, this can place many legitimate citizens in the difficult position of being tracked for the wrong reasons, often without their knowledge, and without clear mechanisms of exiting from wrongful scrutiny. Regulators also face challenges in defining restrictive market practices when there is ostensibly free entry into these markets. When the rule of law is weak there is the additional possibility of a *deliberate misuse of data* by the powerful, leading to rent extraction or political exclusion of different types, beyond the exercise of market power (Ramanathan 2017; Thakar 2018). These are qualitatively different concerns and require a different analytical frame for assessing the likely impact of digital identity systems in developing countries.

3. Asymmetric information and power

The *asymmetric information* approach is widely used to analyse the causes of, and possible policy responses to, rule violations. The approach offers useful insights, but in developing-country contexts it has to be complemented with an *asymmetric power* analysis. Asymmetric information problems arise whenever a 'principal' contracts with an 'agent' to provide a good or a service, but the principal has insufficient information to assess whether a poor outcome was because of fraud by the agent or some other reason. If the agent also knows that the principal does not have full information, the agent is likely to cheat the principal and get away with it. A wide range of policy failures have been attributed to simple or nested asymmetric information problems. These include citizens failing to observe what politicians are doing, which may allow politicians to deviate from manifesto promises, or politicians in turn failing to observe what bureaucrats are doing, allowing bureaucrats to divert resources or respond to offers of bribes.

If contract violations are primarily due to asymmetric information problems, better information about the identities of principals and agents – linked to other data that allows their formal responsibilities and entitlements to be tracked – could help reduce information asymmetries, and therefore reduce corruption and improve accountability. From this perspective, digital identities linked to information on the services citizens are entitled to, their tax liabilities, regulatory reporting requirements and so on, would help to track the fulfilment of a variety of contracts. This is why supporters of digital identity systems believe they help to strengthen citizen rights, reduce corruption, improve the formalisation of the economy and help to implement development programmes.

However, two critical assumptions are required to ensure that more symmetric information will actually improve welfare through a better enforcement of laws and contracts. The first assumption is that the country has a *rule of law*, which means that contracts are enforced once violations are revealed, irrespective of the power of the parties involved. In contrast, if the rule of law is weak, the effects of better information may depend on the power of the violator relative to those affected by the violation. A second assumption necessary for symmetric information to improve enforcement is that the laws and contracts in question are *feasible*, meaning that violators could in principle have complied with the rules. This may sound like a reasonable assumption, except that it is often not the case in developing countries. If compliance is not feasible for some or all individuals or organisations, better information about violations does not make it so. Instead, better information could either result in changes in laws if non-compliance affects the powerful, or it could further disadvantage the less powerful if the information is used to extract from them, to control them politically, or to shut them out.

The weakness of the rule of law in developing countries is structural, and not deliberate or accidental. A rule of law means that laws can be enforced on everyone, including the

powerful. The powerful in advanced countries may have a greater say in making laws in line with their interests, but they have to follow the laws once they are there. Developing countries typically have variants of what we describe as rule *by* law, where enforcement depends on the relative power of the affected parties. In these contexts, if a less powerful individual or organisation violates a contract with a more powerful one, detection is much more likely to lead to contract enforcement than the other way around (Khan 2010, 2018). The degree of enforcement in these contexts can therefore depend not just on information but also on the relative power of the individuals or organisations affected. *Asymmetric power* is therefore another independent variable affecting the persistence of contract violation in addition to asymmetric information, but also interacting with it in ways that we will discuss.

Of course, a rule of law on its own does not ensure inclusion or fair outcomes. Even with a rule of law, asymmetric power can prevent the drawing up of inclusive laws. Nevertheless, if there is a rule of law, once a law is made, its *enforcement* is not a significant concern. Greater inclusion can therefore be pursued through the legislation of fairer laws and contracts, for instance, by mobilising collective action by the excluded to demand legislation for greater inclusion. The powerful are also likely to use their influence to get laws and contracts *interpreted* in favourable ways. But with a rule of law, the disadvantaged or those adversely affected can mobilise to tighten legislation to make it more difficult to interpret laws in particular ways. This is currently playing out in Europe over issues like the right to be forgotten on the internet or face recognition being used by police forces without consent. The main difference between contexts with and without a rule of law is therefore that, in the latter, in addition to laws being *formulated* and *interpreted* in biased ways, they may also be *enforced* in biased ways. This is a very significant difference and allows for qualitatively different outcomes in terms of the scale and severity of exclusion.

For a rule of law to emerge, a society must have a broad distribution of powerful organisations in different activities and with different interests. This ensures that any particular individual or organisation breaking rules is likely to be resisted by other powerful organisations acting in their own interest. For the powerful to want rules to be enforced on each other, it must also be the case that they *require* rule enforcement to sustain their high-productivity activities. This happens when powerful organisations require complex contracts with many parties on an ongoing basis to carry out their high-value activities. These conditions are only likely to be found in advanced countries with diversified and competitive productive sectors. Powerful organisations in these societies will have an effective demand for generalised contract enforcement because they have the power to put pressure on politicians and bureaucrats to deliver and to pay for the delivery. Even though individuals will always have an incentive to free ride and violate rules, once any violations are detected, enforcement agencies can rely on the support of other powerful organisations to ensure enforcement, and the violator is likely to admit the error and take corrective action. Unfortunately, this configuration of power is rare, and few countries fulfil these characteristics, as both North et al.'s classification of Open Access Orders and Khan's political settlements analysis point out (Khan 2018; North, et al. 2007; North, et al. 2009).

A 'political settlement' describes a reproducible distribution of organisational power in a society or sector. For a structure of organisational power to be reproducible, powerful organisations must have interacted to work out formal and informal institutions that give them access to the resources that reproduce this distribution of power. The distribution of power in developing countries can vary significantly, but the configuration shares some common characteristics. Unlike their counterparts in advanced economies, powerful organisations in developing countries often do not need, and therefore do not support, the enforcement of a rule of law; nor, given their capabilities, do they rely solely on formal institutions to generate their revenues. The variations in the distribution of power, rather than simply differences in custom and norms, plays an important role in explaining the varying levels of violations of rules by the powerful in developing countries, with high levels of corruption and informality (Khan 2019). While some enforcement problems may indeed be due to asymmetric information, many violations persist despite full information because the powerful are able to break rules and contracts with a low probability of punishment. Transparency does not always lead to accountability. These types of rule violations cannot be addressed with more information.

In developing countries power is likely to be concentrated across a much smaller number of organisations, creating opportunities for rule violations that are unlikely to be effectively checked. Many powerful organisations may not be particularly productive or competitive and may not need a rule of law to sustain their activities. They are then more likely to rely on political and bureaucratic connections to access rents in informal ways, often violating formal rules. Even if they are relatively high-capability organisations in their context, they are often not competitive in global markets and are likely to be involved in relatively simple transactions with small numbers of other domestic organisations. For these they can rely on trust-based contract enforcement, or informal enforcement involving mafias, patron–client networks often within political parties, or informal arrangements with enforcement agencies. Without an effective demand from the powerful for impersonal rule enforcement, the emergence of a rule of law is unlikely.

Under these conditions, information about violations may not lead to enforcement. Some violations may happen openly, others may be hidden for the sake of political form or to hide violations from competing groups who may use this information for their political advantage. Information about rule-violations may occasionally result in punishment if powerful groups use this information to mobilise support to displace competitors. However, these occasional instances of enforcement may have no systemic effects if the overall distribution of organisational power continues to allow rule violations by the powerful (Khan, et al. 2019). Occasional punishments of violators may simply result in the replacement of one powerful group with another, for instance when political incumbents use anti-corruption cases to get rid of competitors in opposition parties. These are instances of rule *by* law, where the enforcement of rules, including anti-corruption rules, happens when some powerful actors find it in their interest to selectively apply the law.

While powerful and relatively high-capability organisations violate rules as part of accumulation strategies, a much larger number of lower-capability firms violate rules

because they find it difficult to adhere to formal rules. They are often collectively described as the 'informal economy'. In Asia and Africa the informal economy accounts for 50%–80% of gross domestic product (GDP) and 70%–90% of employment (Schneider, et al. 2010; Chen, et al. 1999; Benjamin and Mbaye 2012). Informal-sector small and medium-sized enterprises (SMEs) and micro-organisations lack the capacity to comply with most formal rules such as those governing taxation, social and environmental regulations, labour laws, building codes, land and other registration requirements, and other regulatory requirements. They do not generate the income or profit to be able to make the investments required for compliance and record-keeping. This type of informality declines with economic development as organisations become more productive. However, the reverse does not follow; the rapid enforcement of rules on low-capability firms will not necessarily accelerate their productivity growth or their transition to formality. It is more likely to slow down their development or even close them down (La Porta and Shleifer 2014; Demenet, et al. 2016).

4. Classification and evidence of rule violations in developing countries

In contexts with a weak rule of law, the impact of better information on enforcement is likely to depend on the type violation and the relative power of the violator. Table 1 identifies four types of violations, distinguished by the *relative power* of the violator and whether the violator could have *feasibly complied* with the rule being violated. Violators can be more or less powerful than those affected by the violation or the agencies attempting to enforce the rule. Violations are also different depending on whether the violator is *deliberately violating a rule* that they may have complied with or is violating a rule they are *unable to comply with*.

For violations of the types identified in cells 1 and 4 in Table 1, more symmetric information is likely to result in improved enforcement and lower corruption. But for the types of violations described in cells 2 and 3, the result is likely to be increased asymmetry of power and potentially more serious violations and exclusionary outcomes. In the next four sub-sections, we explain our theoretical expectation for each cell, and review the literature on digital identity systems to show that the available evidence supports our analysis.

Table 1: Effects of improved information on different types of violations

		FEASIBILITY OF COMPLYING WITH VIOLATED RULE	
		Difficult *(violator cannot comply)*	Feasible *(but violator will not comply)*
RELATIVE POWER OF VIOLATOR	High	**1. The powerful violate difficult rules** ***Evasion aided by corruption*** Information may have **positive** effects by mobilising the powerful to change rules to improve compliance	**3. The powerful capture illicit rents** ***Illicit rents, clientelist/populist politics*** Information likely to have **negative** effect by strengthening capacity to repress, control and extract from the less powerful
	Low	**2. The less powerful violate rules** ***Particularly violations in informal economy*** Information likely to have **negative** effect if enforcement leads to economic exclusion or is used by the powerful to control and extract	**4. Fraud based on asymmetric information** ***Opportunistic contract violations*** Information likely to have **positive** effects by reducing fraud as violators are not powerful and enforcement is likely to follow

Source: The authors.

The feasibility of compliance in Table 1 refers to how seriously compliance affects the bottom line. If compliance reduces profitability to below the normal or acceptable level, the rule is difficult to comply with. If profitability becomes zero or negative, the rule may be impossible to comply with. Feasibility therefore varies along a continuum. Some violations happen because the violator *cannot* comply with a difficult rule. But other violations happen because even though the rule is feasible, the violator *will not* comply in order to gain additional illicit benefits or rents.

The relative power of the violator is relevant because we are interested in the probability of enforcement in contexts where the rule of law is weak. Individuals or organisations are powerful if they have greater holding power relative to others in contests over enforcement. This, in turn, depends on the economic and organisational resources they can mobilise. The location of individuals or organisations within the important pyramidal patron–client networks in developing countries is an important determinant of their ability to mobilise support, and therefore their holding power (Joseph 1987; Khan 2000). The greater the holding power of the violator relative to other affected parties and enforcement agencies, the more difficult it is to enforce rules on them regardless of information.

The emerging evidence on the impact of digital identity systems in developing countries demonstrates the importance of distinguishing between these different types of violations. India is a useful case to examine because its Aadhaar system is often held up as an exemplar of an identity system based on a UID linked to the biometric data of each citizen. It has been described as 'the largest biometric laboratory in the history of the modern world' with the Unique Identification Authority of India (UIDAI) enrolling 1.2 billion out of 1.31 billion citizens between 2010 and 2019 (Sen 2019; Ragas 2017). It was sold as a system that would reduce the corruption and fraud in public delivery systems.

Other states in Africa and Asia have introduced digital identity systems with similar goals of reducing identity fraud, improving the targeting of welfare schemes, improving tax collection, and promoting cashless transactions. Digital identity projects often begin with voter registration, but a few began as national identity initiatives. Some African countries including Botswana, Kenya, Morocco and Rwanda are at advanced stages of coverage; others like Nigeria, Chad, Zambia, Cameroon, Tanzania, and Ethiopia are at intermediate or early stages. Most use a combination of biometrics and other data to create electronic databases to store identity information as a precursor to linking with other databases. Countries like Chad and Côte d'Ivoire already see their digital identity systems as a way of documenting stateless people and refugees (Clark 2017). We look at the evidence from Asia and Africa to evaluate the usefulness of the distinctions we have drawn between different types of violations in Table 1, and the likely effects of digital identity data on enforcement in each case.

4.1. Violations when the powerful cannot comply with rules

Cell 1 in Table 1 describes violations where the violators are powerful and are breaking rules that are difficult to comply with. We know from many sources, including the *Doing business* surveys of the World Bank,[1] that many rules affecting even powerful or high-capability organisations in developing countries are dysfunctional in this sense. Rules may be complex

[1] See https://www.doingbusiness.org/

or even contradictory, in some cases deliberately so. Many rules may have been introduced without consultation with anyone and earlier contrary rules are never removed. Or the rules may have been copied from more advanced countries where the productivity and competitiveness of organisations is higher. Evasion sustained by bribes and speed money are likely to be widespread in these contexts. Heightened information requirements to stop these violations is unlikely to directly improve enforcement if the rules are actually unworkable. But pressure for compliance generated by better information available as a result of digital identity systems or otherwise is likely to drive changes in rules since the powerful are involved. Greater transparency about violations is likely to be inconvenient for powerful organisations, particularly if they are engaging in corruption to work around dysfunctional or excessively difficult-to-comply-with regulations. They are likely to override resistance (for instance from bribe-collectors) and force changes in rules that make compliance possible once detection becomes easier.

We would therefore expect to see improvements in compliance, together with reductions in associated types of corruption. Moreover, digital platforms may suggest possible solutions to compliance problems by providing new and cheaper ways of speeding up registrations, simplifying and improving access to forms, or revealing exactly where the compliance requirements or procedures are dysfunctional or contradictory. Digital information may therefore create both strong incentives for reform as well as providing tools for making feasible improvements. Even before the digital identity process began, repeated rounds of the World Bank's *Doing business* surveys identified specific areas where regulatory requirements had excessively high transaction costs in particular countries, and this allowed countries to focus on and simplify specific areas of concern. Digitisation may simply make further simplification along these lines feasible and make compliance easier in specific areas.

India's relatively more developed digital identity system provides useful insights into the types of improvements that can be achieved. Digitisation around Aadhaar helped India improve its *Doing business* rankings in several ways. The Aadhaar identity allowed the development of a set of software interfaces called the 'India Stack' that developers and service providers could access to build and provide value-adding services that required identity data. The first layer of the stack, called 'know-your-customer', electronically verifies the identity of customers applying for various services and maintains verified paperless records. The 'cashless' layer came into being in 2016 with the Unified Payments Interface (UPI), which allows an effective real-time mobile payments system for peer-to-peer and inter-bank transfers. This established a single identifier using Aadhaar that could be used to conduct transactions on a recurring basis without the use of credit/debit cards or bank details. The introduction of paperless and digital identification and payments systems made it faster to process a range of paperwork, for instance to get construction permits, or to set up or liquidate companies. These simplifications contributed to India improving its *Doing business* ranking between 2015 and 2019 from 142 to 77 (Gupta and Auerswald 2019). Digitisation is very likely to continue to help high-capability organisations reduce their transaction costs. Moreover, some of the corruption that these organisations had previously engaged in to evade these high-cost compliance requirements would also have declined as a result (Khan 2006).

The Indian experience shows the kinds of areas where digital systems have been most useful in simplifying procedures, improving enforcement and reducing some types of corruption. These have typically involved violations by high-capability individuals and organisations and regulations that were poorly put together or had excessively high costs of compliance. The digitisation of regulatory compliance systems and linking these with identity data creates strong compulsions for changing procedures that affect powerful and potentially compliant organisations, as well as suggesting technological fixes. An important requirement, however, as the Indian experience also demonstrates, is that implementing agencies have to be technically competent, with close and trusted relationships with the state to push through these changes. India benefited from having a domestic information technology (IT) sector that was at the global technological frontier in many areas, and it had IT entrepreneurs like Nandan Nilekani who were close to and trusted by governments to drive through these technical innovations linked to state systems. Thus, even in these relatively straightforward areas where digital technologies can provide solutions, most developing countries are likely to make slower progress than India given differences in indigenous IT capabilities and trust and coordination between IT delivery agencies and states. In Nigeria, for instance, poor coordination resulted in 12 ongoing ID card projects in 2006, most of which were abandoned, and none achieved close to full coverage. The country is estimated to have spent around $2 billion on these schemes in ten years, double that spent on Aadhaar in India with a population roughly six times bigger (Gelb and Diofasi 2016).

4.2. Less-powerful organisations violating rules including in the ‘informal economy’

Cell 2 in Table 1 describes violations by less-powerful individuals or organisations of rules that they find difficult to comply with. The less powerful can be high-capability firms and individuals who are not connected to the ruling coalition, but the largest segment of these violators are relatively low-capability firms in the informal economy. Micro and small enterprises (MSEs) often find it impossible to comply with the registration requirements, tax codes, building, environmental, labour and other regulations appropriate for higher-capability firms. As a result, a long tail of low-capability firms constitutes the ‘informal economy’ in these countries characterised by non-compliance or partial compliance with rules. These violators typically have to pay informal ‘taxes’ in the form of bribes and protection money to officials or mafias, but in this case the violators are more vulnerable and have little power to trigger changes in rules. If their violations become easier to observe and link with data on their identities, the outcomes may be higher extractions and greater political vulnerability for some groups. In this cell, better information should *not* be expected to result in improvements in enforcement and reductions in corruption.

If there was a rule of law, improved information would have the same effect in both cells 1 and 2 because the identity or power of violators would not matter. If rules were not feasible, there would be pressure to change the rules. But in the absence of a rule of law, better information about violations in cell 2 may lead to greater economic and political exclusion. First, better information is likely to lead to enforcement or demands for bigger bribes, and both can drive many informal businesses to close down, contributing to economic exclusion.

Secondly, information about violations can increase power asymmetries and contribute to increased rent-capture by the powerful by allowing them to differentially target groups and communities in populist or patron–client mobilisations. This can make it easier to mobilise target groups in the context of sectarian or populist politics as well as making it cheaper to recruit individuals in patron–client organisations to assist the rent-capture strategies of powerful organisers. Thus, better information about what is happening in this cell can further empower the powerful and give them greater access to illicit rents, while making some of the less powerful more dependent on protection and patronage. The potentially adverse outcomes in cell 2 are therefore linked to the greater extraction possibilities of the powerful described in cell 3, discussed next. The two cells are therefore linked as shown by the arrow, and in both, a reduction in information asymmetries is likely to result in greater power asymmetries, more serious violations by the powerful, and less-inclusive outcomes.

We find limited evidence of information leading to changes in rules for these types of firms. Two factors may help to explain this difference. First, the productivity of a vast number of firms and organisations in developing countries is so low that regulatory tweaking is insufficient and any improvement in compliance is likely to require significant reductions in regulatory requirements or substantial improvements in firm capabilities. But secondly, the limited power of these organisations means there are no political compulsions for making regulatory requirements lighter. Moreover, the powerful usually want to maintain control over what they see as the disorderly activities of the informal sector, and to keep social order by enforcing the rules on some while providing clientelist exemptions for others. Better information can therefore strengthen the drive for enforcement and the emergence of clientelist politics of different types. Finally, many of the powerful are also engaged in rent extraction from the vast informal economy and better information can also facilitate these processes. The outcomes here are therefore mixed, but the evidence shows no systematic tendency towards regulatory simplification or the reduction of compliance costs for the informal sector. On the contrary, some forms of digitisation and digital identity systems have enhanced the capabilities of the powerful to control, exclude and extract.

Consider the use of digital identity data to support financial inclusion in Nigeria. The Nigerian digital identity card, the National Identity Management Commission (NIMC) card, provided identity data that in theory could facilitate financial inclusion in an economy where 65% of the economically active population borrow from informal lenders, rising to 98% in rural areas. The partial rollout of NIMC cards made identity checking less expensive and this enabled some individuals who had been previously excluded to open bank accounts. These accounts did make it easier to transfer money to relatives in rural areas, but did not result in more substantive financial inclusion because the new account-holders still found it difficult or impossible to borrow money with their limited collateral, low productivity and low profitability businesses (McGrath 2016). A long tail of informal businesses therefore remained excluded from critical financial services because their limited collateral and capabilities persisted, and they had to continue accessing informal credit markets. In Kenya, linking digital identities to credit histories resulted in benefits for banks by significantly reducing non-performing loans, but this was simply because it enabled formal banks to exclude borrowers with poor credit records (Gelb and Diofasi 2016).

The current distribution of capabilities in the informal sector is therefore critical for understanding the likely impact of digital solutions on compliance. Some high-capability firms (particularly those already partially in the formal sector) may become more compliant and their transactions may benefit from better information. But low-capability firms may not benefit. Firms with capabilities are likely to benefit if they had the capabilities to comply but had not been able to because of high costs of compliance. If the latter can be reduced using digital technologies, compliance and transaction efficiency can both be expected to improve. But low-capability firms may have failed to comply for different reasons; they may simply not have had the productivity or cash flow required for specific types of compliance regardless of the costs of filling in forms or establishing identity. Nor may they have the capabilities to benefit from high-value market transactions like borrowing from banks even if they could establish identity. This is why the evidence shows that high-capability SMEs tend to benefit from the enforcement of regulations, and low-capability SMEs are actually held back by enforcement (Mallett, et al. 2018).

Tougher enforcement hurts low-capability SMEs, but some have argued that this is not necessarily a bad thing. The argument is that low-capability firms *should* be squeezed out because their violations give them a competitive advantage over high-capability firms and this keeps overall productivity low (Farrell 2004). But, in reality, the huge differences in productivity and quality between a high-capability formal-sector firm and an informal-sector one means that it is very unlikely that any non-compliance by the latter is going to give it an unfair advantage that would prevent the growth of the former. The more likely effect of enforcing rules on low-capability informal-sector firms may simply be to close them down, destroying jobs and incomes without compensating growth in the formal sector. When formalisation results in such an outcome we describe the process as one of *premature formalisation*.

The decision of the Modi government in India to begin to enforce formal rules on a largely informal economy demonstrated many aspects of premature formalisation. The demonetisation of most banknotes in 2016 was justified as an attempt to crack down on corruption, crime and tax avoidance (as those with cash hoards had to explain the source of their cash to convert it into new money). However, by 2018 more than 99% of hoarded cash had been converted, showing that the powerful had found ways of persuading banks to accept almost all of their money. As almost no ‘black money’ had been identified, demonetisation began to be justified by the claim that it would move society towards a cashless economy where transactions would be on record and potentially taxable (Safi 2018). This was followed by the imposition of the goods and services tax (GST) which was difficult to evade because of the range of instruments that were now available to ensure enforcement as a result of digital identity systems. The GST reforms did accelerate formalisation, though even its supporters agreed that its implementation imposed much hardship (Chowdhury 2019). Growth slowed for thousands of MSEs and SMEs as the time taken to refund claims of GST credit and complying with increased paperwork affected their cash flow, with potentially long-lasting effects on poverty (Mukherjea 2019). It is difficult for struggling entrepreneurs in the sector to remain competitive without significant improvements in their capabilities. A more inclusive policy would have focused on

simplifying regulations so that lower-capability SMEs could begin to comply and to assist capability development in the informal economy (Rajagopalan 2018).

Consistent with the Indian findings, a study of informal firms in the capitals of Benin, Burkina Faso and Senegal found significant differences in the productivity of formal and informal firms, with the differences being greatest between smaller informal firms and others. The argument that informal-sector firms *choose* not to formalise is therefore only likely to be true for the largest informal firms, which already have many characteristics of formality (Benjamin and Mbaye 2012). Similar research in Kampala showed that 69% of the informal enterprises in the city were well below the threshold for company taxation and therefore unlikely to be choosing to remain informal to avoid paying tax (Kathage 2018). Yet smaller informal firms are not necessarily the ones that are less productive. In contrast to Benjamin and Mbaye's findings, , a study of over 500 informal firms in seven African countries found that firms that employed fewer than three workers (the median number employed) achieved higher labour productivity than those employing more (Amin and Islam 2015). What is significant is that all studies show a wide range in the productivity of informal firms. For the long tail of low-productivity informal firms (whether large or small), digital tools for assisting formalisation may only raise their operating costs without creating the capabilities that would enable them to participate in high-value transactions in credit, insurance or capital markets. This is why studies also show that access to better information have had little effect in ensuring compliance or raising taxes, as enforcement often leads to low-productivity informal firms going out of business (Benjamin and Mbaye 2012; Gelb, et al. 2009).

4.3. Extractive violations by the powerful

Cell 3 in Table 1 describes violations where the powerful *will not* comply with feasible rules so as to extract from others. These violations may be underpinned by both asymmetric power and information. However, when the violators are powerful, better information usually does not lead to better enforcement. In a small number of cases there may occasionally be effective punishments, but these are usually cases where the individuals punished have lost power as a result of conflicts within or between networks. Enforcement is only likely to be systematic when the conditions supporting a rule of law have emerged. The arrow from cell 3 to cell 2 describes the invidious link between power, information and enforcement. The powerful are not only likely to violate rules, they are also likely to exploit information about rule violations by others to deepen their control and extraction. That is why greater information flows can paradoxically *increase* the asymmetry of power if the powerful can use this information to their advantage.

In the political settlements of developing countries, the distribution of power is not broad-based enough across powerful and productive organisations to ensure a rule of law. As a result, rules are often violated with limited recourse for correction. When the rule of law is weak, information will lead to enforcement if a powerful group takes an interest in using the information to prosecute and punish particular violators when it is in their interest to do so. For instance, anti-corruption agencies may be effective when directed by the ruling party to

lock up opposition leaders, who may indeed be corrupt, but corrupt individuals linked to the ruling party may be almost impossible to prosecute or punish. If information is commonly used in discretionary ways, it is likely that new sources of information linked to identities can lead to heightened extraction and new forms of political control by contributing to this asymmetry. This evidence is most developed in India as it has led the introduction of digital identity systems, but there is similar evidence emerging in Africa.

Linking the delivery of welfare transfers and public services to Aadhaar in India has enabled the targeting of resources for political purposes and new forms of control or extraction. In the state of Andhra Pradesh, which has led the digital transparency movement, land acquisition for the new state capital was organised using Aadhaar identities, with records registered using blockchain technology. Blockchain makes it very difficult to change records once they have been entered, but the entry has to happen through human agency. Demands for bribes and coercion of poor farmers to give up their land did not stop. Indeed, powerful bureaucrats were able to use their own access to data to identify individuals who were soft targets and offer or threaten to manipulate the recording of transactions with them *before* entering this information into the distributed ledger system (Bhattacharya 2018). As the powerful could continue to use information in discretionary ways, the availability of more detailed information actually increased the asymmetry of power for some of the most vulnerable groups.

In the 2019 Indian elections, the ruling Bharatiya Janata Party (BJP) began to systematically use public digital data for its own electoral purposes. It was returned to power with a bigger majority. Jarvis, a consulting firm, was given access to 150 million data points of beneficiaries of a public welfare scheme from every state. It then used identity data to map these individuals to their nearest polling station and developed applications for party workers disaggregating voters into castes, voting patterns, occupations and so on (Mehrotra 2019). The *Financial Times* reported that BJP call centres contacted more than 200 million beneficiaries of various central programmes (Kazmin 2019). The misuse of social media data for electoral purposes has happened in more developed countries too, but in India identity data and data from *public* programmes were directly mined by the ruling party. India is currently considering a Personal Data Protection Bill, but this was already circulating in draft form in 2018 and had no effect on the activities of the ruling party.

Even more worrying applications of digital identity systems are emerging in contexts of populist-nationalist disputes over citizenship and identity. The position of the Muslim minority in India has been vulnerable ever since the partition of British India in 1947 into India and Pakistan. The Indian state of Assam, bordering Bangladesh, has had a long-standing movement against ‘outsiders’ directed at non-Assamese Indians as well as individuals identified as illegal Bangladeshis. In the context of growing violence, the Indian government signed the ‘Assam Accords’ of 1985 to organise a National Register of Citizens (NRC) to identify illegal migrants from Bangladesh, thereby also diverting attention from internal Indian migration to Assam. A cut-off date was established, and residents had to prove citizenship prior to that date for their citizenship to be confirmed. A massive process of checking documents began, but in developing countries vast numbers of individuals do

not have proper documentation of their birth or residence. Such a process was therefore always going to be fraught and open to local-level political manipulation. Evidence also had to be provided by community governments (*panchayats*) and local officials, and they were often alleged to have been biased given the growing anti-Muslim political mobilisation in India. In 2018, four million people out of a population of 30 million were identified as suspect, and in the phase concluded in 2019, 1.9 million were left out of the NRC, thereby becoming stateless.

Unsurprisingly, the excluded included many from the targeted Muslim minority but unhelpfully for the BJP also included many poor Hindu households. The Hindu agenda of the BJP became transparent when they sought to reassure their Hindu constituency by saying they would reintroduce the Citizenship Amendment Bill that had not passed in the last parliament, this time possibly linked even more dangerously to an NRC exercise across the country. This Bill would ensure that Hindus who could not prove their citizenship would be deemed to have fled Bangladesh to escape religious persecution (even if they had not claimed this themselves) and would be granted Indian citizenship. But Muslims would be treated as economic migrants (even if they claimed to be Indian) and would not be granted citizenship. This deft tactic could potentially exclude around one million Muslims from Indian citizenship under the current NRC, and many more were it to be extended. The even more worrying precedent was to link the identities of excluded people to their Aadhaar numbers during the re-enumeration process. In 2018, the Assam government decided to record the reapplication of citizens who had been left out of the NRC on their Aadhaar records, making it easy at a future date to 'switch off' the access of these individuals to public services, passports and so on, effectively making it impossible for them to live in the country (Chakravarty 2019). The effectiveness of such a tool for further identity-based exclusion, bordering on ethnic cleansing, at some future date does not need to be spelled out.

African countries with tribal, ethnic and religious cleavages that rival India's should also be wary of the types of exclusionary strategies that could be facilitated by digital technologies. Less than 45% of sub-Saharan African children under the age of five have birth certificates, raising the possibility of significant manipulation of evidence when digital identity numbers are issued. The formal rules for determining citizenship are in any case deficient in many African countries. Many allow naturalised citizenship to be withdrawn on arbitrary grounds and half of Africa's states allow revocation of a person's birth nationality (Gelb and Diofasi 2016). The ethnic and tribal contestation over numbers is already intense. From its first census in 1962, census data in Nigeria have been manipulated by competing ethnic networks to increase or maintain the political representation of their groups (Fawehinmi 2018). The recording of digital identities is likely to result in more intensified manipulation, and as the Indian experience shows, the forms of exclusion may become more severe and permanent. An African example is that of Fulani herdsmen in Ghana, many of whom were excluded from the National Identification Exercise (Kaderi and Schareika 2015).

As digitisation allows identities to be linked to public services, bank accounts, mobile phones and so on, there are more rapid and more severe consequences for the excluded (GSMA 2017: 12). The Carter Center (2013) reports that tribal and traditional leaders already

provide evidence on applications for national identity in Sudan and Zanzibar. In Cameroon, Côte d'Ivoire, Kenya and South Africa, opposition supporters have found it difficult to get identity cards. The consequences of discretionary powers will be greatly amplified as digital identities become more important. The weak rule of law in developing countries means that these problems are unlikely to be addressed by passing laws on citizenship, making the national identity authority autonomous, or establishing regulatory limits on the use of digital identities, as many such laws already exist.

Our assessment of the likely adverse effects of digital identity systems on power asymmetries radically modifies the earlier expectation that new technologies like Facebook may make it easier for the less powerful to organise and put pressure on states for reform. Around the time of the Arab Spring that was a plausible expectation. However, the evidence of how the technological arms race has proceeded suggests that the powerful now have tools that make collective action and mobilisation more, not less, difficult than before. New surveillance technologies linked to digital identities that are in turn linked to many other vital aspects of a citizen's life – including their welfare entitlements, bank accounts, sim cards, and even nationality and residence status – have made it easy to identify Facebook and other platform users and use more or less subtle methods to encourage them to desist. The use of social media for organising significant social protests has consequently declined in developing countries and is likely to decline further as surveillance technologies that are being rapidly developed in countries like China, Israel and India are likely to be rapidly adopted by other developing countries.

There is an optimistic but entirely hypothetical scenario where the interaction between cells 2 and 3 can result in a positive dynamic. Better information about the types of violations by the less powerful could in principle be used to revise rules in line with capabilities, restricting enforcement to rules that are feasible for low-capability organisations. Low-capability organisations could be simultaneously supported to raise their productivity and capabilities, allowing more rules to be enforced over time. Such a benign strategy could accelerate both growth and the pace of formalisation. More critically, it could accelerate the broadening of power in society as competitive rule-following firms begin to multiply. In time these firms may effectively demand a rule of law. Unfortunately, this optimistic scenario requires many unrealistic assumptions. It requires a benign coalition of the powerful to calibrate enforcement in this way over a long period, a coalition that altruistically foregoes easy rent opportunities to use information to extract and to demobilise opposition. It is much more likely that the powerful will be rationally selfish.

The dynamic path that actually emerges when digital identity systems are introduced will depend not only on the calibration and sequencing of digital strategies, but also on the initial asymmetries of power described by the political settlement. A ruling coalition that can effectively calibrate and implement enforcement along an inclusive path (or is forced to do so in response to pressure from society) is likely to be one that relies on the support of all major ethnic, religious and other identities in a country, and is able to discipline its own supporters who may want to misuse information lower down the power pyramid. If, as is more likely, support for the ruling coalition comes from a few communities or regions, or the

coalition finds it difficult to discipline its own supporters, digital data is likely to be used in discriminatory ways to exclude some groups and reward others to capture rents, votes or to otherwise strengthen the ruling coalition. The inclusive path also requires a ruling coalition that is able to benefit from longer-term growth since the benefits of this path take longer to appear. If the ruling coalition is vulnerable and has a short time horizon, it will find it easier to reward its supporters with extractive strategies. An evaluation of the likely outcome of a digital identity strategy therefore also needs to assess the characteristics of the ruling coalition and the political settlement in the country to determine the dynamic path that is most likely to emerge.

4.4. Opportunistic violations based on asymmetric information

Finally, cell 4 in Table 1 describes opportunistic violations that are most consistent with asymmetric information problems. Here, less powerful agents skim rents by exploiting their asymmetric information advantage to violate contracts. Better information about identities and violations is likely to result in better enforcement and reduced corruption and fraud for these types of violations. The violators are less powerful by assumption, and information is likely to lead to enforcement. However, there is an important exception even to this. Many agents who appear not to be powerful may often turn out to be clients of powerful patrons who protect them. In this case, the ultimate rule-violator is not the ostensible lower-level agent but a powerful coalition in which the agent is simply a lower-level functionary. These violations should, of course, be correctly located in cell 3, where the violator is powerful because of network connections, and where enforcement is likely to be difficult. Finally, even if the violator is not so networked, the powerful may sometimes still drag their feet on enforcement to ensure that similar cases where they or their clients are involved are not pursued. Nevertheless, better information flows are most likely to have a positive effect on contract enforcement, particularly for service-delivery outcomes, if the violations are located in cell 4.

Opportunistic contract-violations due to asymmetric information are most likely to be effectively addressed by digital technologies. Linking service delivery or other entitlement records to digital identities makes it easier for principals to detect violations by their agents. And, if the public officials involved in the violations are lower-level functionaries who are less powerful than (some of) their principals, the probability of enforcement may be high, even with a weak rule of law.

An important justification for Aadhaar was that it would help to reduce corruption in welfare programmes and service delivery. Several types of fraud can affect welfare programmes. Identity fraud occurs when the wrong individual is targeted for a benefit, eligibility fraud when the individual is correctly identified but is not eligible for the benefit, and quantity fraud when the wrong quantity of a benefit is transferred. Through a process called ‘seeding’, a person’s Aadhaar UID number can be linked to their name on another database, for instance the database for entitlements to the public distribution of subsidised staples. Names on the entitlement list without UID numbers are then automatically deleted. This

ensures that resources do not go to made-up individuals and there is no duplication. The evidence suggests that biometric identification systems have played a role in reducing identity fraud, but have had a limited effect on curbing eligibility fraud, and an even more limited effect on quantity fraud (Dreze, et al. 2017; Khera 2017). The latter two still require human intervention to judge, and remain open to manipulation at the local level.

In some states in India, quantity fraud still allows very significant diversions of stocks meant for distribution to beneficiaries. Eligibility for various schemes is based on criterion like the quality of dwellings or caste status, and these are subject to interpretation and manipulation. This is because technology cannot determine the poverty level or caste of individuals and therefore their eligibility. In theory the system could have been set up to allow individuals who are short-changed in terms of quantity received to record this in the system. But when the recipients are poor and powerless, the system is not set up to enforce their rights, even though formally they are the 'principals'. The 'ration mafia', the politically powerful agents who are dealers in the public distribution system, remain powerful and any attempt to dislodge them continues to meet with fierce resistance (Mooij 2001). However, where the problem is mainly one of identity fraud, there have been significant achievements. The biggest fraud reduction has been in India where using digital identities to provide subsidies directly to bank accounts has eliminated 40 million ghost beneficiaries of liquified petroleum gas cylinder subsidies. In Nigeria, the government was successful in 2011 in weeding out 43,000 'ghost workers' from its payroll system as well as 17,000 fake workers from the Power Holding Company of Nigeria (Gelb and Diofasi 2016).

However, even for establishing identity, digital and biometric systems are themselves open to fraud and technical errors can be quite serious. It has been possible for fraudsters to construct Aadhaar numbers based on cloned documents and biometric data. Moreover, for technical reasons, mandatory biometric authentication for welfare benefits can result in increased transaction costs and serious exclusion problems for the poor. According to a recent submission to the Indian Supreme Court by the head of the authority managing Aadhaar, the UIDAI, technical authentication failures in welfare programmes are as high as 6% when using fingerprints and 8.5% using iris checks. In a related presentation to the Supreme Court, the Chief Executive Officer also revealed that failures were even higher, around 12%, when accessing government services in general (Somanchi 2018).

4.5 Commercialisation and new power asymmetries

Our focus so far has been on how the technology of digital identity systems is likely to affect different types of violations when the rule of law is weak. An important additional dimension that we can only refer to briefly is that the commercialisation of digital data with private companies can further deepen power asymmetries. The generation of identity data has significant commercial applications, but first-movers can achieve network economies that make it virtually impossible for competitors to enter later. Adam Smith's 'invisible hand' works very differently when it becomes a 'digital hand' with network economies, and profit-seeking private behaviour may no longer be in the public interest (Economist 2017).

Network economies give first-movers a huge advantage because customers benefit by being on service platforms that already have many users. This allows a few companies to exploit huge amounts of data and offer cheaper and more attractive services than competitors, but they then enjoy historically unprecedented profits and influence. Even in advanced countries with a rule of law, regulators are struggling with this challenge. The involvement of the private sector in the implementation of identity systems in developing countries may help to finance infrastructure and provide financial and telecommunications services using this data. Initially this can improve service choices and enhance consumer welfare, but network economies can then drive the system in the same direction as more advanced countries.

India's Aadhaar Act of 2016 allows 'any corporate or person' to use the public database called 'know your customer' if they are 'requesting entities'. A number of telecommunication and IT companies have already started accessing this database raising questions about data security and ownership (Ramanathan 2017). Mobile companies have been able to access the Aadhaar platform to identify citizens eligible to be offered digital financial services (GSMA 2017). South Africa's biometric enrolment strategy has a robust legal architecture protecting privacy, but the profusion of databases shared by the public and private sector makes effective enforcement a 'mammoth task' (McKinley 2016). Nigeria has perhaps been the most enthusiastic in enrolling the private sector in the implementation of its national identity card system. At one point the Nigerian government even allowed the MasterCard logo to appear on its national identity card launched in 2014. The card could also be used as a standard MasterCard to make payments. This was later reversed because of intense criticisms on the grounds of national dignity (Nwakanma 2014).

In contexts where the rule of law is weak, private firms cannot only acquire market power in the future, their collusive partnerships with powerful politicians can give the latter tools that can *increase* existing asymmetries of power. For instance, we have earlier referred to the role of Jarvis in India's 2019 elections. The potential collusion that can emerge between private companies hungry for privileged access to data and politicians who can benefit from the advantage they gain by using identity data for populist targeting or electoral processes can seriously exacerbate and entrench asymmetries of power in contexts of a weak rule of law.

5. Conclusion

Our distinction between the role of asymmetric information and asymmetric power in contexts of a weak rule of law can help to explain a range of different outcomes that may emerge with the introduction of digital identity systems in developing-country contexts. The theory and evidence suggest that a more nuanced analysis can assist in designing welfare-enhancing digital strategies by considering country-specific political settlements, the characteristics of asymmetric power in different sectors, and the characteristics of particular ruling coalitions.

Digital identity systems can have different types of effects on the enforcement of rules depending on whether the violators could have feasibly complied with the rules and the relative power of the violators. They can help to improve service delivery and reduce corruption in service-delivery violations where the entitlements and delivery requirements are feasible, and the violating bureaucrats and politicians are not very powerful. Such systems can also help to reduce violations by higher-capability and relatively powerful firms when rules are being broken because they are difficult to comply with.

Better digital systems can create strong compulsions to simplify rules by making violations by the powerful transparent, and also by providing technical solutions to speed up and simplify procedures. For two other types of violations, we need to be much more cautious. The extensive informal operations of low-capability firms are in most cases not likely to be sustainably reduced by digital systems. Attempts at enforcing premature formalisation may be welfare-reducing if low-capability firms are forced out of business or if they have to pay bigger bribes to survive. The most problematic violations are the extractive strategies of powerful organisations. Here, digital identities are least likely to make a systematic dent and may actually increase asymmetries of power in society. It is therefore not at all an accident that authoritarian and populist regimes have been at the forefront of developing digital identity systems. Enhanced asymmetries of power can adversely affect almost anyone but are most likely to affect low-capability organisations and poor people who are more likely to be the victims of populist and exclusionary politics.

The likely impact of a digital identity system will therefore depend on how it is applied to different types of enforcement problems. The enforcement problems in turn depend on the distribution of capabilities and organisational power in society, which determines the rent-extraction strategies of powerful groups, and the feasibility of rule-following behaviour by different types of organisations.

Developing countries dominated by high-capability productive organisations and a distribution of political power that precludes extractive, populist or exclusionary strategies by political organisations are already close to being rule-of-law societies. In these societies digital identity systems can accelerate the simplification of rules and reduce compliance costs to further improve rule-following behaviour and reduce corruption. These systems can also improve the efficiency of service delivery and reduce corruption associated with the

exploitation of asymmetric information by public officials. But in societies with a long tail of low-productivity firms in the informal sector, the distribution of power in politics is also likely to be asymmetric, with political organisations frequently using clientelist, populist and exclusionary strategies to stay in power. In these societies, digital identities will have more complex effects. There may still be positive effects for high-capability firms and for aspects of service delivery subject to asymmetric information. But there are significant possibilities of adverse effects on the informal sector and an intensification of asymmetric power which allows greater extraction from and control over targeted groups. Corruption of some types may increase as a result; political inclusion may deteriorate.

In these more typical cases, the calibration of the rollout of the digital identity system is likely to be critical. Simply saying that better regulatory structures and laws are required for data protection and citizen rights will not do in the political settlements of most developing countries. To mitigate some of these risks, linking citizenship information with service-delivery data is something that needs to be carefully considered given the emerging experience of the risks of exclusion for populist and exclusionary political reasons. Similarly, the possibility of increased transaction costs for the poor if they are forced to manage bank transfers or prove identity using digital systems can be mitigated by allowing dual delivery systems for an extended transition period. For instance, citizens could be allowed to choose whether they would prefer cash transfers or in-kind access to public distribution systems. The increased costs may be justified by welfare gains (Muralidharan, et al. 2017).

More generally, our argument suggests that in the presence of asymmetric power and the partial enforcement of rules, a *reduction* in the asymmetry of information can sometimes *enhance* asymmetries of power. This paradoxical outcome can emerge because an initial asymmetry of power can skew who can use subsequent improvements in information to their own advantage. This is an important dynamic to keep in mind, and is why using digital identity systems to improve information flows can also improve welfare outcomes in some cases while worsening them in others. This interdependence of asymmetric information and asymmetric power makes it particularly important for both lenses to be simultaneously used in evaluating policy and institutional design in developing countries.

References

Amin, M. and A. Islam (2015) 'Are Large informal firms more productive than the small informal firms? evidence from farm-level surveys in Africa', *World Development* 74: 374-85.

Benjamin, N.C. and A.A. Mbaye (2012) 'The informal sector, productivity and enforcement in West Africa: a firm-level analysis', *Review of Development Economics* 16 (4): 664–80.

Bhattacharya, A. (2018) 'Blockchain is helping a new indian city, but it's no cure for corruption', *Quartz India,* 18 July (https://qz.com/india/1325423/indias-andhra-state-is-using-blockchain-to-build-capital-amaravati/).

Bukari, K.N. and N. Schareika (2015) 'Stereotypes, prejudices and exclusion of Fulani pastoralists in Ghana', *Pastoralism: Research, Policy and Practice* 5 (20): 1-12.

Carter Center (2013) *Voter identification requirements and public international law: an examination of Africa and Latin America*. Atlanta, GA: The Carter Center (https://www.cartercenter.org/resources/pdfs/peace/democracy/des/voter-identification-requirements.pdf)

Chakravarty, I. (2019) 'In Assam, merging NRC updation with Aadhaar enrolment leads to fresh questions', Scroll.in, 13 July (https://scroll.in/article/902731/grey-area-assam-seeks-to-merge-nrc-claims-process-with-the-collection-of-biometric-data-for-aadhaar).

Chen, M., J. Sebstad and L. O'Connell (1999) 'Counting the invisible workforce: the case of homebased workers', *World Development* 27 (3): 603–10.

Choudhry, S.R. (2019) 'Voters in a crucial Indian state give mixed reviews for Modi's big economic policies', CNBC.com, 15 May (https://www.cnbc.com/2019/05/15/india-effects-of-demonetization-and-gst-in-west-bengal.html).

Clark, J. (2017) *The state of identification systems in Africa: a synthesis of country assessments*. Washington, DC: World Bank.

Demenet, A., M. Razafindrakoto and F. Roubaud (2016) 'Do informal businesses gain from registration and how? panel data evidence from Vietnam', *World Development* 84: 326–41.

Department of State (2011) *Country reports on human rights practices*. Washington, DC: Government of the United States Bureau of Democracy, Human Rights and Labor.

Dibben, P., G. Wood and C.C. Williams (2015) 'Pressures towards and against formalization: regulation and informal employment in Mozambique', *International Labour Review* 154 (3): 373-92.

Dreze, J., K. Nazar, R. Khera and A. Somanchi (2017) 'Aadhar and food security in Jharkhand: pain without gain?', *Economic and Political Weekly* 52 (50): 50–59.

Economist, The (2017) 'Data is giving rise to a new economy', 6 May (https://www.economist.com/briefing/2017/05/06/data-is-giving-rise-to-a-new-economy).

Economist, The (2019a) 'Big tech faces competition and privacy concerns in Brussels', 23 March (https://www.economist.com/briefing/2019/03/23/big-tech-faces-competition-and-privacy-concerns-in-brussels).

Economist, The (2019b) 'Young people and their phones are shaking up banking', 2 May (https://www.economist.com/special-report/2019/05/02/young-people-and-their-phones-are-shaking-up-banking).

Farrell, D. (2004) 'The hidden dangers of the informal economy', *McKinsey Quarterly,* July (https://www.mckinsey.com/featured-insights/employment-and-growth/the-hidden-dangers-of-the-informal-economy).

Fawehinmi, F. (2018) 'The story of how Nigeria's census figures became weaponized', Quartz Africa, 6 March (https://qz.com/africa/1221472/the-story-of-how-nigerias-census-figures-became-weaponized/).

Gelb, A. and J. Clark (2013) *Identification for development: the biometrics revolution*. CGD Working Paper No. 315. Washington, DC: Center for Global Development (http://www.cgdev.org/content/publications/detail/1426862).

Gelb, A. and A. Diofasi (2016) 'Identity for development: opportunities and challenges for Africa', *IT and Telecom Digest* 179: 23-25 (http://africapolicyreview.com/id-for-development-opportunities-and-challenges-for-africa/).

Gelb, A., T. Mengistae, V. Ramachandran and M.K. Shah (2009) *To formalize or not to formalize? Comparisons of microenterprise data from Southern and East Africa*. Center for Global Development Working Paper. Washington, DC: Center for Global Development (https://www.cgdev.org/publication/formalize-or-not-formalize-comparisons-microenterprise-data-southern-and-east-africa).

GSMA (Global System for Mobile Communications Association) (2017) *Aadhaar: inclusive by design: a look at India's national identity programme and its role in the JAM trinity*. London: GSMA.

Gupta, A. and P. Auerswald (2019) 'The ups and downs of India's digital transformation', *Harvard Business Review,* 6 May (https://hbr.org/2019/05/the-ups-and-downs-of-indias-digital-transformation).

House of Commons Home Affairs Committee (2004) *Identity cards: fourth report of session 2003-04*. London: House of Commons.

Joseph, R. (1987) *Democracy and prebendal politics in Nigeria: the rise and fall of the second republic*. Cambridge: Cambridge University Press.

Kaderi, N.B. and N. Schareika (2015) 'Stereotypes, prejudices and exclusion of Fulani pastoralists in Ghana', *Pastoralism: Research, Policy and Practice* 5 (20): 1-12.

Kathage, A.M. (2018) 'Understanding the informal economy in African cities: recent evidence from Greater Kampala', World Bank blogs: Can Africa End Poverty? (https://blogs.worldbank.org/africacan/understanding-the-informal-economy-in-african-cities-recent-evidence-from-greater-kampala).

Kazmin, A. (2019) 'Modi's publicity machine cannot hide india's patchy progress', *Financial Times*, 1 June (https://www.ft.com/content/52013cbe-959f-11e9-8cfb-30c211dcd229).

Khan, M.H. (2000) 'Rent-seeking as process', in Khan, M.H. and K.S. Jomo (eds) *Rents, rent-seeking and economic development: theory and evidence in Asia.* Cambridge: Cambridge University Press, pp. 70-144.

Khan, M.H. (2006) 'Determinants of corruption in developing countries: the limits of conventional economic analysis', in Rose-Ackerman, S. (ed.) *International handbook on the economics of corruption.* Cheltenham: Edward Elgar, pp. 216-44.

Khan, M.H. (2010) *Political settlements and the governance of growth-enhancing institutions*. Research Paper Series on Governance for Growth. London: SOAS, University of London (http://eprints.soas.ac.uk/9968).

Khan, M.H. (2018) 'Political settlements and the analysis of institutions', *African Affairs* 117 (469): 636–55 (https://academic.oup.com/afraf/article/117/469/636/4690667).

Khan, M.H. (2019) 'Institutions and development', in Nayyar, D. (ed.) *Asian transformations: an inquiry into the development of nations.* Oxford: Oxford University Press, pp. 321-46 (http://fdslive.oup.com/www.oup.com/academic/pdf/openaccess/9780198844938.pdf).

Khan, M.H., A. Andreoni and P. Roy (2019) *Anti-corruption in adverse contexts: strategies for improving implementation*. SOAS-ACE Working Paper No. 13. London: SOAS, University of London (https://ace.soas.ac.uk/wp-content/uploads/2019/09/ACE-WorkingPaper013-AntiCorruptionAdverseContexts-Text-190909.pdf).

Khera, R. (2017) 'Impact of Aadhaar on welfare programmes', *Economic and Political Weekly* 52 (50): 61–70.

La Porta, R. and A. Shleifer (2014) 'Informality and development', *Journal of Economic Perspectives* 28 (3): 109–26.

Mallett, O., R. Wapshott and T. Vorley (2018) *Understanding the Firm-level effects of regulation on the growth of small and medium-sized enterprises*. Research Paper. London: Department of Business, Energy and Industrial Strategy.

McGrath, K. (2016) 'Identity verification and societal challenges: explaining the gap between service provision and development outcomes', *MIS Quarterly* 40 (2): 485-500.

McKinley, D.T. (2016) *New terrains of privacy in South Africa: biometrics/smart identification systems, CCTV/ALPR, drones, mandatory sim card registration and FICA*. Pretoria: Media Policy and Democracy Project and Right2Know (https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/r2kmpdp_new_terrains_of_privacy_in_south__africa_masterset_small.pdf).

Mehrotra, K. (2019) 'Its team drawn from Modi's 2014 campaign, Mumbai firm works on BJP's 2019 run', *The Indian Express,* 2 May (https://indianexpress.com/elections/its-team-drawn-from-modis-2014-campaign-mumbai-firm-works-on-bjps-2019-run-5705599/).

Mooij, J. (2001) 'Food and power in Bihar and Jharkhand', *Economic and Political Weekly* 36 (34): 3289–3299.

Mukherjea, S. (2019) 'Dissecting the economic slowdown in India', moneycontrol.com, 19 September (https://www.moneycontrol.com/news/economy/policy/policy-dissecting-the-economic-slowdown-in-india-4448441.html).

Muralidharan, K., P. Niehaus and S. Sukhtankar (2017) *Direct benefits transfer in food: results from one year of process monitoring in union territories*. San Diego: UC San Diego.

North, D.C., J.J. Wallis, S.B. Webb and B.R. Weingast (2007) *Limited access orders in the developing world: a new approach to the problem of development*. World Bank Policy Research Paper No. 4359. Washington, DC: World Bank.

North, D.C., J.J. Wallis and B.R. Weingast (2009) *Violence and social orders: a conceptual framework for interpreting recorded human history*. Cambridge: Cambridge University Press.

Nwakanma,O. (2014) 'National identification and MasterCard', Vanguard, 31 August (https://www.vanguardngr.com/2014/08/national-identification-master-card/).

Rajagopalan, S. (2018) 'Formalization of the economy is a form of coercion', Mint, 9 July (https://www.livemint.com/Opinion/4O2zG2XPgcnm2AD16I9hjJ/Formalization-of-the-economy-is-a-form-of-coercion.html).

Ragas, J. (2017) 'The silent revolution: how ID cards are changing the world, *Harvard International Review* 38 (2): 24–7 (http://hir.harvard.edu/article/?a=14537).

Ramanathan, U. (2017) 'Without supreme court interference the Aadhaar project is a ticking time bomb', The Wire, 4 April (https://thewire.in/government/aadhaar-supreme-court-uid).

Safi, M. (2018) 'Demonetisation drive that cost India 1.5m jobs fails to uncover "black money"', *The Guardian***,** 30 August (https://www.theguardian.com/world/2018/aug/30/india-demonetisation-drive-fails-uncover-black-money).

Schneider, F., A. Buehn and C.E. Montenegro (2010) 'New estimates for the shadow economies all over the world', *International Economics Journal* 24 (4): 443–61.

Sen, S. (2019) 'A decade of Aadhaar: lessons in implementing a foundational ID system', Observer Research Foundation Issue Brief 202. New Delhi: Observer Research Foundation.

Somanchi, A. (2018) 'Aadhaar fraud is not only real, but is worth more closely examining', The Wire, 3 May (https://thewire.in/economy/aadhaar-fraud-uidai).

Thaker, A. (2018) 'The new oil: Aadhaar's mixing of public risk and private profit', *The Caravan***,** 1 May (https://caravanmagazine.in/reportage/aadhaar-mixing-public-risk-private-profit).

Travis, A. (2010) 'ID cards scheme to be scrapped within 100 days', 27 May, *The Guardian* (https://www.theguardian.com/politics/2010/may/27/theresa-may-scrapping-id-cards).

World Bank (2014) *Digital identity toolkit: a guide for stakeholders in Africa*. Washington, DC: World Bank.

World Bank (2017) *Identification for development: Africa business plan IDA 18 (FY18–20)*. Washington, DC: World Bank (http://pubdocs.worldbank.org/en/484791507732929415/ID4D-Africa-Business-Plan-FINAL.pdf).

ACE SOAS Consortium

Anti-Corruption Evidence

Making Anti-Corruption Real

About the Anti-Corruption Evidence (ACE) Research Consortium:

ACE takes an innovative approach to anti-corruption policy and practice. Funded by UK aid, ACE is responding to the serious challenges facing people and economies affected by corruption by generating evidence that makes anti-corruption real, and using those findings to help policymakers, business and civil society adopt new, feasible, high-impact strategies to tackle corruption.

ACE is a partnership of highly experienced research and policy institutes based in Bangladesh, Nigeria, Tanzania, the United Kingdom and the USA. The lead institution is SOAS, University of London. Other consortium partners are:

- BRAC Institute of Governance and Development (BIGD)
- BRAC James P. Grant School of Public Health (JPGSPH)
- Centre for Democracy and Development (CDD)
- Danish Institute for International Studies (DIIS)
- Economic and Social Research Foundation (ESRF)
- Health Policy Research Group (HPRG), University of Nigeria Nsukka (UNN)
- Ifakara Health Institute (IHI)
- London School of Hygiene and Tropical Medicine (LSHTM)
- Palladium
- REPOA
- Transparency International Bangladesh (TIB)
- University of Birmingham
- University of Columbia

ACE also has a well established network of leading research collaborators and policy/uptake experts.

Anti-Corruption Evidence (ACE) Research Consortium

SOAS University of London, Thornhaugh Street, Russell Square, London WC1H OXG

T +44 (0)20 7898 4447 • **E** ace@soas.ac.uk • **W** www.ace.soas.ac.uk

SOAS University of London