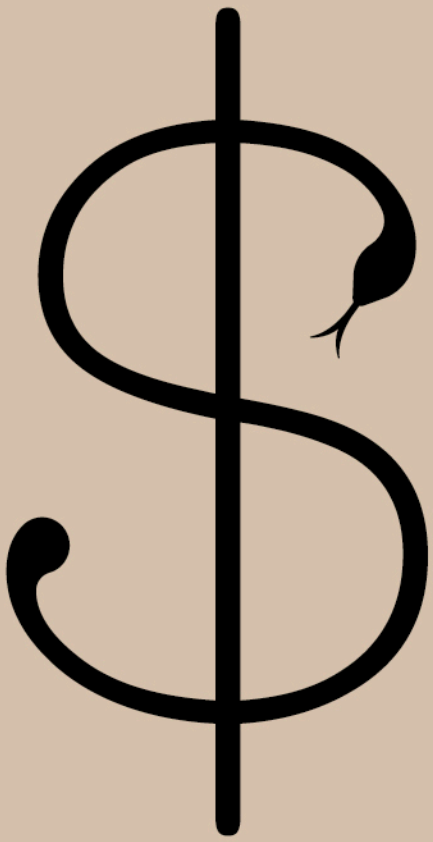


Aiding Surveillance

Aiding Surveillance

An exploration of how development and humanitarian aid initiatives are enabling surveillance in developing countries

Gus Hosein and Carly Nyst[01]
October 2013

PRIVACY INTERNATIONAL

www.privacyinternational.org

Contents

Executive Summary

Information technology transfer is increasingly a crucial element of development and humanitarian aid initiatives. Social protection programmes are incorporating digitised Management Information Systems and electronic transfers, registration and electoral systems are deploying biometric technologies, the proliferation of mobile phones is facilitating access to increased amounts of data, and technologies are being transferred to support security and rule of law efforts.

Many of these programmes and technologies involve the surveillance of individuals, groups, and entire populations. The collection and use of personal information in these development and aid initiatives is without precedent, and subject to few legal safeguards. In this report we show that as development and humanitarian donors and agencies rush to adopt new technologies that facilitate surveillance, they may be creating and supporting systems that pose serious threats to individuals' human rights, particularly their right to privacy.

Introduction

1.0

It is hard to imagine a current public policy arena that does not incorporate new technologies in some way, whether in the planning, development, deployment, or evaluation phases. New technologies are enabling the creation of new forms and high quantities of data that can inform policy-making processes, improving the effectiveness and efficiency of public policy and administration. Water management, for example, now employs measurement and metering techniques; tax administration increasingly involves outsourcing of contracts to the private sector, and the use of data mining techniques for analysis; healthcare now involves advanced diagnostic technologies and distributed computing.

Today, advanced data analysis technologies and techniques inform and underpin sustainable policy related to transport, health, infrastructure and other public services. Frequently, this data includes vast amounts of personal information of citizens, and, increasingly, non-citizens. Generating and analysing such data creates new and potentially malevolent opportunities for surveillance – the use of personal data to influence, manage,[02] direct or protect those whose data have been garnered[03] – by public and private entities. As a result, in Europe and North America, and increasingly globally, there is a trend towards the establishment of legal frameworks to govern how personal information is managed and to ensure that individuals' rights are protected.

It is possible to see surveillance as a necessity in modern societies. Over the years leading social thinkers have conceptualised surveillance in numerous beneficial ways:[04] as progress towards efficient administration, a benefit for the development of Western capitalism, essential to the modern nation-state, and even a power generator in itself.[05] Yet surveillance that is unconstrained

by legal frameworks, human rights protections and the rule of law has the potential to jeopardise individuals' rights to privacy, free expression, association, assembly and political participation. As such, in developed countries, the introduction of new technologies that have the potential to facilitate surveillance has traditionally been accompanied by public resistance, critique and oversight.

In developing countries, however, new technologies and techniques are being deployed with a considerably less critical eye. Analysis of the potential adverse implications of the use personal information is often completely neglected in public administration in developing countries, and governance measures to ensure protection of personal information are often non-existent.[06] Emerging economies and developing nations across Africa, Asia and Latin America are seeing the rapid deployment of technologies that many more developed countries are hesitant to use, such as national identity registries using biometric technologies,[07] and e-health systems[08] with national registries of sensitive personal information, in the absence of legal safeguards and, indeed, critical analysis. Security techniques, technologies, and programmes are also being transferred to developing countries prior to the establishment of the necessary democratic and legal safeguards.

The amount of attention devoted to privacy and personal information issues in developing countries is growing. This is in part due to the increased use of technologies by governments and other institutions, but it also reflects the greater use of technology by citizens. Modern technologies can facilitate the surveillance of nearly every interaction done by individuals in their homes, on the streets, as they travel, over telecommunications networks and the internet. Registration of populations creates a single store of identity that can be used for many purposes, including to track individuals' use of services and interactions with the state and private sector in ways previously unforeseen, and unimagined by the registration systems themselves. Interfering with privacy allows for control to be exerted on individuals, inhibiting their

autonomy. In the public sphere this could result in undue attention to specific individuals and groups, and this focus turns frequently to government critics, opposition groups and parties, journalists, and human rights defenders. Abuse could be less intentional, but equally destructive, where creating data stores allows accidental disclosures that place individuals at risk of fraud by malicious third parties. Data collected about individuals for one purpose can be used for other purposes, including monitoring individuals and groups, creating profiles of their activities, predicting their activities, and discriminating against them.

New technologies hold great potential for the developing world, and countless development scholars and practitioners have sung the praise of technology in accelerating development, reducing poverty, spurring innovation and improving accountability and transparency.[09] Indeed, the ICT4D (information and communications technologies for development) movement has come to dominate the discourse on technology and development, and is at the centre of discussions about the post-2015 development and humanitarian agendas. This is, of course, with some good cause – new technologies present countless opportunities for expression, connectivity and empowerment. Developing countries lack the legacy systems and infrastructure long present in the developed world, and proponents of the deployment of new technologies in development argue that this facilitates the positive 'leapfrogging' effect. Why should, after all, a developing country deploy paper ID cards when it can use biometrics to secure the process of issuing identity and delivering public services? Similarly, why manage borders by merely checking people and their possessions when we can search through travel histories and other profiles? After all, developing countries also often face a complex concoction of political instability, rapid population growth, and inequality that raises the stakes when it comes to public service delivery or border management.

The problem, as this report will identify, is that there is a systematic failure to critically contemplate the potential ill effects of deploying technologies in development and humanitarian

initiatives, and in turn, to consider the legal and technical safeguards required in order to uphold the rights of individuals living in the developing world.

As privacy rises on the policy agendas of countries across the world, the contrasting approaches to new technologies in the developed and developing worlds has become increasingly stark. Many of the technologies embraced as being key to effective and sustainable development by the development community[10] have been the subject of extensive debate in advanced Western democracies in recent years. Identity systems and databases that collect biometric information including fingerprints, facial scans, iris information and even DNA, and other expansive registration systems have been proposed, resisted, and sometimes rejected in various countries. In the United Kingdom significant political concern and scrutiny led to the reversal and destruction of the National Identity Register and ID card with the Minister in charge of its destruction calling it "intrusive and expensive" and articulating concerns about "fantastic claims about supposed benefits".[11] Israel saw significant debate around its proposed smart ID and biometric database, with the High Court calling a pilot program extreme and harmful.[12] The German parliament decided to deploy next generation passports using biometrics but explicitly excluded the storing of biometrics on a centralized database because of privacy concerns. South Korea's policy of requiring real-names to access communications was rejected by the Constitutional Court because it undermined democracy.[13] National health and genetic databases[14] and other national registers have been called into question,[15] data deleted,[16] and on occasion dismantled[17] because of privacy and human rights concerns.

Systems that track individuals at borders and profile movements have been called into question in Canada,[18] the US[19] and Europe,[20] resulting in systems being abandoned,[21] and safeguards being applied. Recent revelations by US National Security Agency whistleblower Edward Snowden of extensive and indiscriminate communications surveillance systems in the US and abroad have

resulted considerable public outcry in the United States, Europe and elsewhere, resulting in action by the European Union,[22] United Nation bodies[23] and civil society groups.[24]

When surveillance technologies are proposed by policy makers in Western democratic states, at least two debates emerge. The first focuses on human rights, civil liberties and the rule of law. The second interrogates the value of a system, its impact, and the calculable costs against perceived benefits. Social institutions, civil society, regulators, interest groups, government auditors, opposition parliamentarians, scientists and technologists are able to interrogate each other's claimed understanding of the problem, statements regarding the effectiveness of the technological choices, and whether other solutions are possible with lesser costs. Increasingly, these debates are intertwined. Discussions around the US initiative to enhance security of driving licenses, under the REAL ID Act, led to debates over civil liberties and constitutionality as much as to debates over the size of the costs and the management of the costs.[25] Similarly, when the Nigerian House of Representatives recently stalled the procurement of an internet surveillance system, they did so both for reasons that it violated constitutional rights and that it breached the Fiscal Responsibility Act.[26]

Contrast these debates with the emergence of new technologies as a key element for delivering development and humanitarian aid in the developing world. The deployment of surveillance technologies by development actors, foreign aid donors and humanitarian organisations is conducted in the complete absence of any public debate or deliberation. The development discourse rarely considers public opinion of the target populations when approving aid programmes. Even the availability of countervailing perspectives is surprisingly low. Seminal strategy documents like the UN Office for Humanitarian Affairs' 'Humanitarianism in a Networked Age'[27] or the UN High-Level Panel on the Post-2015 Development Agenda's 'A New Global Partnership: Eradicate Poverty and Transfer Economies through Sustainable Development,'[28] pay scant attention to the potential impact of

the adoption of new technologies or data analysis techniques on individuals' privacy.

In sum, there are four major problems arising from the increased use of development aid to advance surveillance in developing countries. First, technologies are being deployed that raise significant concerns with regards to privacy and other human rights. Second, such technologies may not necessarily be appropriate for achieving development goals or may have undesirable side effects. Third, these technologies are already seen as legally and technologically problematic in more developed countries. Fourth, these technologies are deployed in the absence of relevant and adequate legal frameworks, in contravention of international human rights and national constitutional requirements. Too often these are the missing dynamics in modern development discourse around the deployment of technological solutions.

1.1 Human rights and development

Development is not just, or even mostly, about accelerating economic growth. The core of development is building capacity and infrastructure, bridging historical divisions, ending conflict, addressing social vulnerabilities, and supporting democratic societies that protect, respect and fulfill human rights.

Traditionally, a chasm existed between the human rights and development communities, in which "the latter group proved generally reluctant to engage in debates about international legal obligations and how to reflect the relevant norms in policies at the domestic and international level."[29] This has begun to change in recent years, spurred by the call of Kofi Annan to mainstream human rights in all UN agencies in 1997, the expansion of UN human rights mechanisms, and by difficulties experienced in development and humanitarian interventions. In a 2005 report, Annan, then Secretary-General, emphasized that the challenges

of human rights, development and security are so closely entwined that none can be tackled effectively in isolation.[30]

Nevertheless, development and humanitarian aid organisations have been slow to adopt a rights-based approach to development. It was not until June 2012 that the European Union released a new strategic framework for the administration of foreign aid that married rights and development. In July 2013 USAID for the first time elevated human rights to a key objective in its development approach.[31] The World Bank is under ongoing pressure to mainstream human rights protections in its programmes.[32]

In a 2012 speech in Senegal on 'building sustainable partnerships in Africa', then-US Secretary of State Hillary Clinton spoke to the important role foreign aid donors plays in promoting rights in development. In comments that were seen as veiled criticism of other development funding sources,[33] she contended that funding must be carefully deployed:

> "the United States will stand up for democracy and universal human rights, even when it might be easier or more profitable to look the other way, to keep the resources flowing. Not every partner makes that choice, but we do and we will."[34]

Yet there continues to be a gap between theory and practice, particularly in the application of new technologies in development contexts. The EU Development Fund has supported the issuance of voter cards and ID cards in Somaliland;[35] in 2013 USAID put US$53 million towards a programme that, amongst other things, facilitated the production of national identification cards in Kenya;[36] the UK Department for International Development played a key role in setting up the M-PESA mobile money system in Kenya in collaboration with Vodafone.[37] While each of these initiatives has contributed to development in the respective countries, they have also raised a number of concerns from a human rights perspective that have been all but ignored.

1.2 Development and technologies

New technologies are now seen as a crucial element of development and humanitarian aid initiatives. Indeed, the aid community has often heralded technology as the key to effectively and efficiently achieving sustainable development and overcoming obstacles to delivering humanitarian aid. Technologies have been embraced as a key component of "humanitarianism in the networked age"[38] and will be a priority for the post-2015 agenda discussions, constituting one of four thematic focal points at the World Humanitarian Summit in 2015. Technologies are being incorporated into every development initiative from education to health to elections, and in humanitarian initiatives related to crisis response, food delivery and refugee management.

This fervour surrounding ICT4D discourse has been so cacophonous as to drown out – or, arguably, forestall – any critical analysis of the potential adverse effects of the adoption of new technologies on human rights and civil liberties. This discussion paper seeks to fill the gap in of critical research and thinking on this issue.

The paper will focus on critically evaluating four types of technologies or technical modalities applied in the development and humanitarian sectors: management information systems and electronic transfers; biometric identification and voter registration systems; the use of mobile phones and the data collected and generated by them; and border surveillance and security technologies. Each of these interventions seeks to create new information infrastructures that become national utilities in ways that require great care and significant scrutiny.

This assessment also provides an opportunity to reflect critically upon and reassess policy choices concerning technology. For instance, one form of development policy that has been receiving a significant amount of international development funding has been electoral reform and modernisation, often involving the

registration of an entire population's biometrics. This has caused numerous problems and challenges, as viewed most recently in Kenya. Applying technology in such contexts is challenging, as the UN Secretary General contended in 2009:

> "[S]ome of the poorest countries in the world have chosen some of the most expensive electoral processes and technology. […] I am concerned about techniques and systems that might cause a State, in the conduct of its own elections, to be financially dependent on donors, or technologically dependent on specific vendors for extended periods… [E]xperience throughout the world has shown that it is not the case that the more complex or expensive a system, the more successful the elections will be."[39]

The UN Development Programme, which is funding much of the activity in this domain, responded that they have begun to argue for technology and electoral processes that are "cost-effective, transparent, sustainable, inclusive, accurate, flexible, and supported by appropriate infrastructure and computer literacy."[40] Similarly, the independent body that oversees UK aid programmes, the Independent Commission for Aid Impact, also recognised the UN Secretary General's concerns, and presented some case studies:

> "In countries such as Sierra Leone and DRC, the UK has helped to fund an investment in biometric technology for voter registration, requiring equipment such as laptops, webcams, fingerprint scanners, colour printers and mobile generators. In Malawi, delicate computer equipment used to collect photo identification of voters was damaged because it was transported in the back of uncovered vehicles. In Sierra Leone, Commissioners saw an ambitious voter registration programme being rolled out, using biometric data collection technology. Donor and civil society stakeholders noted the risk to the political process of this technologically advanced approach. While we acknowledge

> the potential of new information technologies to strengthen electoral processes, deploying such sophisticated technologies in difficult environments has a high failure rate and does not usually represent good value for money."[41]

While technologies and new programmes may help target, support, and secure development, their adoption must be subjected to rights-based questions about whether they are the necessary, proportionate, and effective methods for development, and whether legal frameworks exist to protect against human rights abuses. Only after answering these questions can a judgement be made about whether the right technologies are being deployed in the most appropriate ways. Importantly, a rights-based evaluation must come before the critical assessment of the technology; the alternative would allow for an enquiry about the ideal methods for deploying problematic technologies.

Methodology

2.0

This paper draws from the authors' expertise and scholarship in privacy, technology, human rights and development. The authors have been engaged with analysis of technology in development and humanitarian initiatives since at least 2008, and have conducted field research on the issue of biometric identification technology in refugee management situations. In 2011 we undertook research on medical information protection in development and humanitarian initiatives.[42] The research for this study builds upon this prior research and other desk research undertaken over the past year, including research undertaken by Privacy International into privacy in the developing world.

A number of research challenges were encountered when conducting this review. Surveillance is a domain that is difficult to observe because it is, by its very nature, secret. Furthermore, researching development programmes is quite challenging due to the absence of transparency requirements in the design, implementation and evaluation of development programmes. Initiatives such as the International Aid Transparency Initiative and the Humanitarian Accountability Partnership have gone some way to alleviate this challenge.

Development initiatives that involve the transfer of technology or capabilities are also often particularly obfuscated because of the involvement of the private sector in providing technologies or infrastructure essential to the project. While such interventions often generate significant interest at the outset, unfortunately this does not translate into a level of transparency across the life-cycle of the programme. Rarely are funding proposals made public. Procurement information is infrequently published. In turn, the specific types of technologies being sought and delivered cannot be monitored.

This report thus focuses on only a few international organisations, foreign aid donors, and international funding agencies that articulate clearly what it is they are funding at a project-level basis. Monitoring and evaluation programmes have proven to be quite helpful in elucidating what the programmes and projects tried to accomplish and some of the obstacles to success, but even the most critical evaluations have not necessarily critically analysed the technology in detail, and none identified human rights as a consideration.

A few key evaluations and studies have been relied upon, along with reports from foundations and other agencies, when available, but these are often high-level statements, or selectively detailed press releases and narratives of the successful achievements from development interventions. One positive trend is the growing number of insightful local media organisations and civil society institutions in developing countries that have begun to question the merits of technology choices, procurement processes, and the sustainability of development interventions. This paper therefore makes use of these media reports and perspectives, and although they do represent secondary sources of information, the same can be said of the published statements from foundations and international organisations.

When the significant 'e-government' movement in the developed world expanded in the 1990s and 2000s without critical analysis and at great cost, it took significant critical analysis by academics, media, and civil society to catalyse questioning of the merits of programmes, technological efficacy, and human rights implications.[43] The same emergence of a policy discourse is beginning to appear in the developing world. This discourse certainly needs informing, but many key issues are being raised already. For instance, there is an emerging sensitivity to procurement policy, as evidenced by a recent public uproar over tender processes in Kenya,[44] the Maldives,[45] and Nigeria.[46] This paper seizes on, and seeks to further, such discourses.

Management Information Systems and electronic transfers

3.1 The promise

In recent years, donors, development agencies and poverty-reduction initiatives have increasingly turned towards social protection, cash transfer or social safety net programmes as an effective tool for addressing extreme poverty and accelerating development in the world's poorest countries. The term refers to the provision of benefits in cash or in kind to secure protection in case of social risks and needs, and takes the form of cash transfer schemes, public work programmes, social pensions, school stipends and food vouchers or transfers.[47]

Although social security systems have played an integral role in many developed countries for decades, the idea that a minimum level of non-contributory social protection could be affordable and easily adopted by low-income countries has really gained momentum only in the last ten years. Programmes such as Bolsa Familia in Brazil and Oportunidades in Mexico have achieved impressive advancements in decreasing poverty and improving health and education outcomes. Widespread political support for the idea of non-contributory minimum social protection crystallised in 2009, when the heads of the UN agencies launched the Social Protection Floor Initiative as one of the nine UN joint initiatives to cope with the global economic and financial crises. Importantly, the G20 States declared their support for social protection in the 2011 Cannes Summit Final Declaration, emphasising the importance of investing in nationally determined social protection floors which "will foster growth resilience, social justice and cohesion."[48]

Social protection is now a priority initiative both for bilateral aid donors, such as the UK's Department for International

Development,[49] the US Agency for International Development,[50] and the European Commission[51] and for development agencies, such as the World Bank[52] and UNICEF.[53]

Research suggests that social protection initiatives can significantly reduce the prevalence and severity of poverty,[54] contribute to improved nutrition levels, help families absorb the costs associated with schooling[55] and have a positive impact on higher school attendance levels,[56] reduce child labour,[57] and improve maternal health, and the lives of people living with HIV/AIDs. Nevertheless, a number of significant challenges exist when delivering social protection initiatives in developing countries which often impede the effectiveness of such programmes. Obstacles include the absence of legal and institutional frameworks, long-term strategies, and adequate and sustainable financing; programme fragmentation and a lack of capacity of programme stakeholders; and institutionalised discrimination and the absence of a gender approach in programme design and implementation. Programmes are also hampered by practical challenges associated with, for example, the geographical remoteness of target communities; difficulties in identifying potential beneficiaries; requirements for the production of identification; transportation, accommodation and opportunity costs associated with collecting payments in remote or dangerous areas;[58] and complex application processes which require literacy.

In this context, new technologies are seen to hold enormous potential and promise for improving the reach and effectiveness of social protection programmes. In recent years, a variety of ICTs have been piloted to increase the reach and effectiveness of social protection programmes, particularly in remote and rural areas, and include smart cards, cell phones, mobile ATMs, GPS devices, and biometrics.[59] In addition, the migration of social protection systems from paper-based to fully electronic systems is gradually being undertaken in many countries, in combination with the consolidation of information derived from multiple and separate social protection initiatives into a Single Registry of social protection beneficiaries. Proponents of the integration of

ICTs into social protection programmes cite the following benefits: efficiency and cost-effectiveness; flexibility; access to financial infrastructure; leapfrogging the digital divide; multi-functionality; scalability; and minimising fiduciary risk and fraudulent access.[60]

Acknowledging the considerable benefits that can be derived from integrating ICTs into the delivery of social protection, the use of information and communication technologies nevertheless pose a number of risks to beneficiaries' right to privacy, as extensive and sensitive information is collected, analysed and disseminated about them. In particular, the use of electronic Management Information Systems (MISs) to collate and generate information about social protection beneficiaries and inform targeting, management, reporting and analysis raise serious concerns. MISs facilitate the gathering and storing of extensive amounts of personal data in what are often insecure or high-risk environments. Where donors or development agencies administer the scheme, and where private-public partnerships are integrated into the scheme, the potential for abuse of beneficiaries' personal information is high. There is some confusion around the ownership and use of sensitive personal information collected by social protection programmes; these concerns are particularly serious in low-income countries where data protection laws are weak, or non-existent.

Similar concerns exist with the move away from cash or in kind transfers and towards electronic transfers by aid agencies. The card – or mobile – enabled conversion of cash into electronic money has been a hugely successful advancement in the provision of social protection transfers in developing countries. However, numerous risks arise due to the sharing and transfer of personal information with third parties.

Cash transfer programmes mapped by the Cash Learning Partnership (CALP)

Projects
330

Beneficiaries
10,262,050

ACF International
2,540,878 (25%)

IRFC/National Societies
2,222,303 (22%)

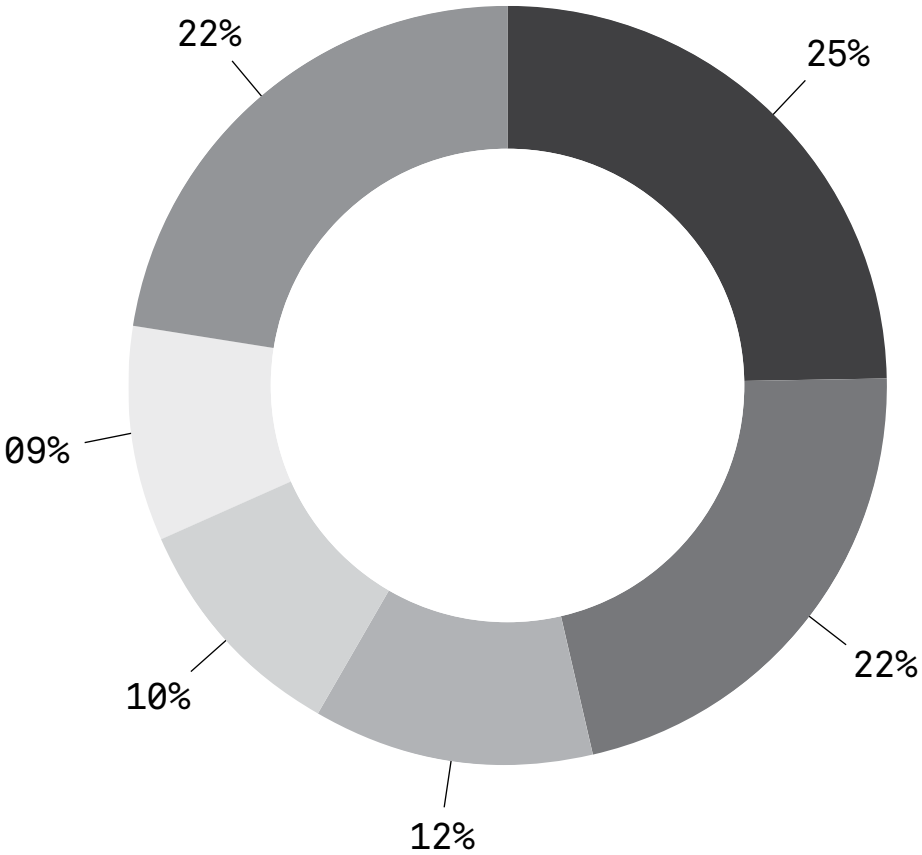
OXFAM
1,228,872 (12%)

World Food Program (WFP)
1,043,174 (10%)

Concern Worldwide
923,311 (09%)

Others
2,303,512 (22%)

Number of beneficiaries per organisations:



Source: CALP Cash Atlas.

3.2 The potential

Increasingly, social protection programmes in developing countries are making the transition from paper to electronic systems. Complete transition to fully-integrated electronic systems remains elusive in many low-income countries, particularly those hampered by difficulties in access to electricity, internet and mobile phone networks. Generally, however, donors and development agencies are encouraging the adoption of electronic systems in social protection pilots and supporting the migration of social protection information to centralised single registries.

Within the literature on social protection, MISs are identified as an integral part of the administration of social protection programmes, enabling the collation and application of information related to the various components of the scheme, including those related to registration, conditions, targeting, payments, grievance systems, and graduation. MISs collect and collate an extensive amount of data, particularly in those social protection systems which require compliance with programme conditionalities (which often relate to attendance at health or education services) as a prerequisite for receipt of benefits.[61] The following table is illustrative of the types and amount of personal information collected about a social protection beneficiary.

HelpAge International notes that additional information on recipients degrades in accuracy as soon as it collected, as people leave the household, children are born and assets are sold or purchased. Much of the information, in addition to being inaccurate, is of little use, and is extraneous to the determination about beneficiary eligibility, according to HelpAge.

Data to populate the MISs is collected through a variety of forms, mostly electronic (using laptops and mobile devices).[62] Once digitised, MISs allow for increased flows of data to other institutions. Research shows that the adoption of MISs to administer social protection information increases the ability of

programmes to send data directly from communities or districts to databases held in the capital cities.

Linked to the adoption of MISs is the move towards a Single Registry of social protection programmes in each country. The drive towards a Single Registry is inspired by Brazil's Cadastro Unico which aims to build a database of the entire poor population of Brazil; it now holds data on the declared incomes of 16 million households and uses an unverified means test for targeting. The main user of the Cadastro Unico is the Bolsa Familia scheme, but it has also been adopted by nine other schemes.[63]

The availability and persistence of this information means that if effective, it could provide a single source of information on large populations, available to numerous stakeholders with differentiated levels of access, as has been the case in Chile.[64] It is therefore open to re-use for other purposes and by other State and potentially non-State entities. In Kenya, for example, the government is rolling out an Integrated Financial MIS that integrates social protection payments with all other electronic payments made through the Central Bank electronic payment system.[65]

Electronic transfers also have huge beneficial implications for humanitarian assistance. By providing a secure and simple method of potentially life-saving transfers to vulnerable groups, electronic transfers could make social protection programmes more efficient and effective, while at the same time creating a new resource of information about how money is spent. Organisations such as Concern Worldwide have been quick to take up electronic transfers, working with Safaricom's M-PESA system, and the Cash Learning Partnership, a consortium of non-governmental organisations such as Oxfam and the Norwegian Refugee Council, are currently investing considerable research into piloting guidelines and a Code of Conduct related to the use of e-transfers.

PRIMARY MONITORING INFORMATION	SECONDARY MONITORING INFORMATION
ADDITIONAL INFORMATION ON APPLICANT/RECIPIENT	
Marital status	Occupational status
Educational attainment	Disability
Additional address details (e.g. family name, name known by)	
INFORMATION ON HOUSEHOLD MEMBERS	
Number of members	Disability status
Date of birth	Occupational status
Sex	Grade enrolled at school
ID number	Health status
Marital status	
Single/double orphan	
Relationship to beneficiary and/or household head	
Educational attainment	
INFORMATION ON DWELLING AND ASSETS	
Water source	Description of dwelling
Sanitation	Type and number of animals
Landholding size	Car
Land tenure	Bicycle
	Agricultural implements
	Etc.
ACCESSIBILITY OF SERVICES	
Distance to health clinic	
Distance to primary school	
Distance to secondary school	
Distance to pay-point	

Source: HelpAge International, 2011

3.3 The problems

The collation of extensive and sensitive personal information in an MIS lends itself to a number of challenges in respect of privacy and data protection. These include:

— Accuracy of data: Multiple obstacles exist to collecting accurate and comprehensive data in situations in which social protection programmes are administered, including the geographical remoteness of target communities, social exclusion and discrimination, lack of literacy, and the absence of formal registration records. By enabling the digitisation and indefinite preservation of potentially inaccurate data, MISs risk reinforcing and institutionalising such inaccuracies, which may be impossible for beneficiaries to correct.

— Security of data: Ongoing technical support and maintenance of a system is key to ensuring security, and yet requires a level of expertise and capacity that may not be present in donor-run or pilot social protection schemes. Systems that involve the transfer of data via telecommunications networks face additional threats in the absence of encryption or where State authorities are conducting communications surveillance.

— Misuse of data: Any personal information contained in MISs is vulnerable to fraud or theft, as well as transfer to third parties. The higher the sensitivity of the data – data, for example, that reveals or could be paired with other data to reveal ethnicity, religion or political affiliation – the more vulnerable it is.

A further challenge of adapting MISs to social protection programmes is ensuring that the technologies deployed are appropriate to the relevant culture and context. A study of the development of an MIS for the distribution of social protection benefits in St.Kitts revealed that it is "necessary to understand the contexts in which data is collected and used to ensure that the [MIS] will fit within the users' work environment and be useful to them".[66] Simple assumptions inherent in the design of

technology such as the requirement to enter addresses that follow a predefined format may undermine the utility and effectiveness of MISs in developing countries. It is estimated that in developed countries approximately 25 per cent of MIS projects are failures, and up to 60 per cent have significant undesirable outcomes; in developing countries, this number is likely to be significantly higher.[67] A failure to take into account cultural contexts may be a contributing to such failures, which also stem from factors such as cost overruns, insufficiently trained staff, and inadequate processes. Early studies in this field showed that almost all World Bank-funded MIS projects in Africa were reported as partial failure.[68]

In order to ensure that an MIS takes into account the particular context of the country, it will most likely require a custom-made solution. However, most social protection programmes have neither the resources nor capacity to do so cost-effectively, and as such rely on generic MIS solutions. Kenya's Urban Food Subsidy relies on Microsoft Access, for example, while Mauritius uses Oracle, South Africa uses Adabas and the Hunger Safety Net Programme and OVC-CT in Kenya use Microsoft's SQL Server database.[69] Research shows that a generic approach "has serious drawbacks and is unlikely to be successful."[70]

When social protection programmes use generic MISs this raises additional questions about who might ultimately have access to the data. The role of private corporate entities in social protection programmes more broadly is also an issue. The situation in Swaziland is apposite – the government is in negotiations about contracting Standard Bank and the SwaziPost to administer the country's Old Age Grant. Should the scheme come to fruition, Standard Bank will hold a separate database with information on all 45,000 beneficiaries.[71] Similarly, the Dowa Emergency Cash Transfers project in Malawi was administered by Concern Worldwide contracting the Opportunity International Bank Malawi and the Malawi Police Service.[72] Issues around information governance will arise: who owns the information, who is responsible for problems and who is mitigating any risks of abuse?

The administration of electronic transfers lies at the heart of this challenge. E-transfers rely on the private sector to provide the telecommunications and financial infrastructure, and to design and maintain the banking and mobile systems upon which e-transfers rely. Electronic cash transfer systems are often run by small NGOs on a pilot basis without concrete structures, extensive legal expertise or sufficient resources to ensure that third party contracts are rigorously analysed and complied with. The likelihood that beneficiary data is being shared and analysed by third parties is thus increased.

The beneficiary data collected for e-transfer programmes is often more extensive than that gathered in conventional aid distributions and is necessarily shared with commercial partners who assist in the distribution of cash via new technological means. The development of sophisticated databases, the sharing of those databases with third parties, and the lack of technical and operational security around the collection, use and sharing of data all create a heightened risk framework, at the heart of which are the very people agencies seek to support.

The risks of deploying MISs and e-transfers in social protection programmes are heightened by the absence of legal frameworks and safeguards to regulate the use of data collected under the auspices of such programmes. In most developing countries, data protection legislation is weak or non-existent. Many social protection programmes are established ad hoc, as pilot programmes by development and humanitarian agencies, or under the ambit of bilateral aid agreements, without accompanying legislative or regulatory frameworks. This means that the rights of the beneficiaries in the programme are unprotected, and the administrators of the programme have wide discretion when dealing with beneficiaries' personal information. In any event, given that many programmes are the result of a collaborative effort by multiple stakeholders – including donors, government actors and international NGOs – there are serious questions about accountability, transparency and avenues for recourse for beneficiaries.

Digital identity registration and biometrics

4.1 The promise

Ensuring that development and humanitarian aid reaches those for whom it is intended is a perennial challenge for foreign aid donors and international funding organisations. Obstacles to delivering aid include not only security risks[73] and lack of infrastructure (airports, roads and other facilities),[74] but also the difficulty of identifying and targeting intended beneficiaries.

Increased pressure to focus aid where it is needed most, and to monitor aid programmes has resulted in a strong push for greater information on recipients. The benefits to development policy of targeted approaches are clear: properly identify the individuals and the groups that need assistance, and programmes will become more effective and efficient. As the US Government Accountability Office (GAO) framed it in a September 2012 report on targeting of food aid, "effective targeting is important to maximize the impact of limited resources", with a particular emphasis on the "quality of data used to identify and reach recipients".[75]

A significant challenge in targeting is ensuring that there are sufficient amounts of information on the target populations to ensure that the determinations made are necessary, proportionate, and critically assessed, and that aid delivery can be tracked and monitored to assess its effectiveness. In order to begin to address these issues, some donors have begun to use technology to support identification and registration. Development and humanitarian initiatives related to providing refugee assistance, delivering social protection or food subsidies, and improving democratic institutions, particularly electoral reform, have all begun to integrate digital identity registration.

Case study: UNHCR biometric identity registration in Dijbouti, Ethiopia, Kenya and Malaysia

UNHCR biometric identity registration in Djibouti, Ethiopia, Kenya and Malaysia

The UN Refugee Agency (UNHCR) has long used databases to collect and manage information on refugees, and has issued refugees with a form of certification of their status. In recent years, UNHCR has begun to deploy biometric identification systems to register refugees, and check their identity and status for aid disbursement. Pilot schemes were initiated in Eastern Africa and Asia in the mid-2000s, and in October 2012 UNHCR announced that it was to begin using biometrics in Senegal and South Sudan.

A field study conducted by the authors in 2008 witnessed the considerable problems being experienced with respect to UNHCR's deployment of a biometric system. The primary concern was the system's reliability: UNHCR had procured a fingerprinting system that was not designed for large populations, and particularly not for large populations that did not have well-defined fingerprints.

UNHCR staff members were unaware of this problem and lacked guidance on how to use the system in the field: various field operations were using the system differently, some fingerprinting adults of all ages, young people, and even babies, presuming that the system would work. The system was erratic; it worked sometimes on someone, and sometimes on that same person it would not work even moments later. But for UNHCR, it was a perceived success: staff had high confidence in the system, and it was a useful tool for communicating with host governments that UNHCR was taking fraud seriously.

The recording of identity into registers is not new; identity registries exist in many forms in many countries. Indeed, the maintenance of an effective system of identification is arguably essential for the development of individual's legal identity, to the distribution of social services,[76] and to the realisation of the right to identity registration at birth, enshrined in the United Nations Convention on the Rights of the Child.[77] However technologies are changing the impact and importance of identity registration in two ways. First, they are enabling the digitisation and centralisation of these registries, their use across government services, and the continual checking of identity. Second, technological advancements have facilitated the capture, processing and retention of biometrics, physical traits of individuals including fingerprints, facial scans, iris scans, or even DNA. These relatively unique characteristics can provide identifiers across systems, and even across borders, tracking individuals across contexts, allowing for the reuse of information. They also make sharing, linking and cross-checking information faster.

Proponents of digital identity registration and the tying of identity to biometric information maintain that such systems can help to empower individuals by giving them legal identity and connecting them to services. Biometric identification, it is argued, is more accurate and thus its employment more likely to forestall identity fraud and improve the transparency and accuracy of electoral processes and access to public services. According to the director of India's universal biometric identification scheme, such a scheme can be "transformational", and "solve the most basic of developmental challenges".[78] By offering a solution to the absence of traditions of birth registration and accompanying infrastructure, biometric identification systems provide for the opportunity to uniquely register a large population of people, and in turn, administer entitlements. By connecting data to a unique personal identifier such as a fingerprint or iris scan, biometrics avoid the opportunities for forgery associated with other forms of identification.

4.2 The potential

Biometric identification systems are used to record and identify social protection beneficiaries in at least 15 cash-transfer programmes: Pakistan, Afghanistan, the Democratic Republic of the Congo, Malawi, South Africa, India, Ghana, Namibia, Botswana, Kenya, Nigeria, Iraq, Philippines, Bolivia, and Indonesia.[79] Such systems tie the biometric information of the beneficiary to the information held about them by the social protection programme. Benefits are disbursed via shopkeeper-operated point-of-sale devices, which verify the fingerprint scan, connect with the central database, and transfer funds into the shop account that are immediately passed along in cash to the recipient.

Biometric technologies are particularly prevalent in Africa, and are spreading; estimates put biometrics technology in at least 34 countries in Africa. This primarily takes the form of biometric national identity cards or biometric voter registration systems that incorporate Automatic Fingerprint Recognition Systems (AFIS), fingerprints being the dominant form of biometric data collected.

Prominent instances of biometric identification systems include:

— Democratic Republic of the Congo: Biometric information is a key element of the Disarmament, Demobilisation and Reintegration Programme (PNDDR) in the DRC, established in 2004 and co-funded by the World Bank. The programme disburses 13 cash payments over the course of a year to ex-combatants. Biometrics – in the form of iris scans, as fingerprints were unreliable for ex-combatants with calluses on trigger fingers – were introduced in 2006 to enrol 110,000 individuals.[80] Beneficiaries visit one of ten mobile payment teams in rural areas, have their irises scanned and receive their payments.

— India: The state of Andhra Pradesh was one of the first to use biometrics to deliver government payments, partnering with FINO, an Indian technology company which designed a

platform based on biometric identification to link rural citizens with the formal banking system.[81]

— Pakistan: The Watan card – an identification card containing biometric data that can be credited with social protection transfers – was introduced after the 2010 floods by the National Database and Registration Authority, and used as a means of transferring National Flood Relief Grants to over 1.5 million victims, in a programme jointly administered by the government and UNHCR.[82]

— South Africa: One of the oldest systems of biometric registration in the world exists in South Africa; the government began collecting the fingerprints of non-white citizens in 1925 for the purpose of racial registration. In 1992, the province of Kwa-Zulu Natal worked with Net1, a South African company, to set up biometric technology to enable the payment of social protection grants to pensioners. The system continues to be extended, and now distributes grants to over 15 million beneficiaries. In 2012–2013, a new system provided by Net1/Cash Paymaster Systems captured the biometric information of more than 20 million South Africans as part of a new national social protection payment system which was aimed at reducing fraud and corruption.

In many cases, the technology is procured from foreign companies, many of them European. Unlike in other development sectors where there is now a drive towards local sourcing, biometric programmes often involve spending money designated for developing countries on Western high-tech firms.

Development agencies and bilateral donors have played a large role in supporting biometric initiatives. In 2011 the UN Development Programme (UNDP) provided 26 per cent of its funding towards fostering democratic governance in the developing world.[83] In Africa alone, through the United Nations Democracy Fund, the UNDP has funded biometric voter registration in Benin,[84] Cape Verde,[85] the Comoros Islands,[86]

Democratic Republic of Congo,[87] Sierra Leone,[88] Togo,[89] and Zambia.[90] Other examples of development funding for biometric systems include World Bank funding for registration of the urban poor in Benin[91] and Kenya.[92] USAID has funded biometric systems in Malawi[93] and Guinea,[94] and played a large role in supporting the registration of 14.3 million voters using biometric voter registration technology in the lead up to the 2013 Kenyan elections.[95]

The costs of deploying and operating these systems are significant. In Mozambique the cost of the national identity cards, contracted to Face Technologies, was US$15 million.[96] UNDP funding to biometric registration and machines in Sierra Leone was US$18 million for the 2012 elections.[97] The contract between Uganda and Muhlbauer group was €64 million.[98] In Ghana the costs were estimated at US$100 million.[99]

4.3 The problems

Biometrics, whether based on face, finger, iris, DNA, or some other physical or genetic characteristic, are in many ways just another form of personal information, and their registration and connection with identification thus give rise to questions of privacy and data protection.

Yet we cannot ignore the ethical dimensions. Identification registration systems have problematic legacies. In Rwanda, the colonial racialisation of the identities of Hutu and Tutsi contributed to the increasing polarisation of the two groups in the postcolonial period, leading to the 1994 genocide.[100] The use of identification cards was a key administrative component of this as they allowed differential access to the two groups – entitling Tutsis to far more extensive political and social freedoms than Hutus.[101] The Belgians' colonial approach was to institute an ethnic classification, involving such 'modern scientific' methods as a measurement of nose and skull sizes, and required this information on mandatory identity papers.[102]

Since 2007 Rwanda's National Identification Department has created a permanent civil and voter registry, and citizens' data is held in a central and permanent database.[103] While there is no ethnicity information on the new cards, they do contain biometric data – the fingerprints of approximately 9.2 million Rwandan citizens have been collected and stored.[104] Although the use of biometric registration has since been greeted positively in Rwanda,[105] the serious nature of the problem of political abuse of biometrics becomes apparent in this context.

The artificially constructed identities of 'Tutsi' and 'Hutu' were used to secure political, social and economic benefits. It is possible to imagine categories of identities relating to fingerprints being similarly constructed and being used to the advantage of political or criminal groupings.

The use of biometrics in South Africa also raises questions concerning the human dimensions of the use of biometric identification systems. Although a key mechanism for the functioning of citizenship in the country, the national population register was also the administrative and ideological cornerstone of apartheid. The 1950 Population Registration Act required people's identity numbers to refer to ethnicity. Although ethnicity is no longer incorporated as part of identity documentation in South Africa, this history raises important questions about identification systems that have the potential to be used for discriminatory purposes and social sorting.

Few registration systems are now considering including ethnicity information because of these lessons. But the inclusion of biometrics and additional biographic information raises new concerns. The linkability of biometrics increases the likelihood of their expansion and re-purposing in other environments (in the criminal justice or immigration systems, for example) or for other purposes unimagined at the time of their collection. One of the predominant reasons why digital identification systems, particularly those containing biometrics, have faced resistance in developed countries is the potential for scope creep: once

Case study: Aadhaar Unique ID project (UID) in India

Recent experiences with the UID project in India demonstrate the complications that can be faced in deploying biometric identification systems. In 2009, the UID Authority of India was established to carry out the UID scheme with the objective of issuing every resident in India with a unique identification number based on their biometrics, designed to eliminate duplicate identities and authenticate individuals in a cost-effective way. Implementation of the project has been conducted since 2010 in the absence of legislation.

The UID was initially designed to be an identification tool to authenticate and provide services, adoptable by any platform in a consolidated manner. But without clear limitations on its use, the number has been adopted by various services and platforms for their unique purposes – including identification, linking, and tracking individuals in various systems. In this way the UID number has expanded from being just an authenticator, to being an identity and a tool for service delivery, and increasingly mandatory for access to many services. For example:

— the Indian government has required that citizens have a UID number to purchase cooking gas, issue an open-government request for information, and register vehicles.

— the High Court has directed all police stations in Maharashtra to record the UIDs of accused individuals and witnesses filing an incident report.

— railways are proposing to use the UID database for bookings and validation of passengers;

— the city of New Delhi is implementing a scheme called Saral Money that allows individuals to open bank accounts once they have stated their UID number.

— the Rajasthan Government has made it mandatory for employees to have a UID number and has linked the number to employee salaries. Yet, infrastructure issues including a lack of available machines has prevented individuals from enrolling for the number.

The system faces numerous serious challenges, including:

— many rural workers, elderly, and poor individuals do not have readable fingerprints. It has been reported that often agencies are simply refusing to enrol such individuals, thereby excluding them from the service and all the subsequent uses (and benefits) of the UID.

— enrolment centres are overcrowded without proper facilities.

— duplicate numbers have been issued and some enrolment agencies have been blacklisted for fraudulent practices.

Malu. B. The Aadhaar Card – What are the real intentions of the UPA Government? DNA. February 18th 2013. Available at: http://www.dnaindia.com/blogs/post_the-aadhar-card-what-are-the-real-intentions-of-the-upa-_1801080-all. Last accessed: February 28th 2013.

Misra. U. Inside the Direct Cash Transfer Debate. Forbes India. January 2013. Available at: http://forbesindia.com/article/briefing/inside-the-direct-cash-transfer-debate/34510/1

Plumber, M. Make UID numbers must in FIRs: Bombay HC. DNA. October 2011. Available at: http://www.dnaindia.com/mumbai/report_make-uid-numbers-must-in-firs-bombay-hc_1603127. Last accessed: February 28th 2013.

Times of India. Govt tries to ramp up Aadhaar enrollments, but centres ill-equipped. March 3rd 2013. Available at: http://articles.timesofindia.indiatimes.com/2013-03-03/jaipur/37409682_1_uid-registration-uid-card-aadhaar

UIDAI Strategy Overview. Creating a Unique Identity Number for Every Resident in India. April 2012. Pg.2. Available at: http://uidai.gov.in/UID_PDF/Front_Page_Articles/Documents/Strategy_Overveiw-001.pdf

collected, biometrics can be re-used for a variety of other purposes. Therefore, a system that is designed for the purpose of disbursing aid and entitlement services will soon be used for verifying citizenship and age, and biometrics may be checked and compared with those for policing purposes.

From a privacy perspective, some biometric applications are more sensitive than others: for example, photographs enabling facial recognition and DNA records facilitating genetic profiling can assist the creation of racial and ethnic profiles. The invasiveness of collection also has a bearing on the privacy impact of the technology. DNA requires intimate contact with the individual, and even submitting to facial recognition technology may require the removal of clothing. Studies have indicated that there is some concern from users about the requirement to physically touch a fingerprint scanner, or even cast one's eyes into a biometric scanner for retina or iris recognition. In some circumstances, facial images can be collected without the consent or knowledge of the individual; fingerprints and DNA can be collected from latent prints or samples left behind on objects and linked with other databases and activities.

The predominant form of biometric recognition used in developing countries is fingerprinting. However, fingers are vulnerable and prints are not always easy to read.[106] For example, fingerprint scanners tend to fail more frequently on women in developing countries, as their fingerprints have been degraded due to manual labour. Some fingerprint recognition systems may also have difficulty in registering the fingerprints of the elderly, those with small or fine fingerprints, and fingerprints that may have worn down such as those of manual and rural workers. This can result in high 'failure to enrol' rates meaning that a number of individuals cannot be 'read' by the technology and therefore cannot participate in the registration that is taking place.

Digital identification registration systems increase the likelihood that processes become data dependent, and in turn, that determinations are driven by such data. The adoption of biometric

technologies means that sensitive personal information on entire populations can be collected and processed rapidly, and decisions can be made with reference to digital profiles and aggregated data, the integrity and veracity of which is difficult to establish or safeguard. Information and data is not value-free, and discriminatory judgments can become accepted and institutionalised through the use of automated systems. Individuals quickly become reduced to a set of knowable and measurable facts that may not necessarily represent them or their circumstances accurately. With the advent and proliferation of the EURODAC biometric database system for identifying asylum-seekers and irregular migrants, submitting to biometric registration has become a de facto pre-requisite to claiming asylum. Asylum seekers and refugees are reduced to someone with a file, whose biometrics need to be verified in order to gain access to, or be prevented from wrongly accessing services. When the biometrics systems do not accurately function, the refugee's status is thereby called into question sooner than the technology. This may lead to the further marginalisation of vulnerable individuals, other human rights violations, and exclusion from vital aid. In September 2013, for example, 6,500 refugees in the Mbera camp in Mauritania were denied access to refugee assistance because of problems with the biometric registration system.[107]

Case study: Biometric voter registration in the DRC

The DRC's first democratic elections in four decades were held on 30 July 2006. In support of the 2006 election process the international community donated US$460 million to the DRC. La Commission Électorale Indépendante (CEI) of the DRC decided to biometrically register voters for the elections. The UNDP oversaw the procurement process and two contracts were awarded to European companies to institute biometric registration. Zetes was awarded the contract for 10,000 biometric registration kits, at a cost of US$40.16 million and Sagem, a French company, was charged with removing

duplicates in the system. An additional US$58 million was spent on the operation costs.

The biometric system was implemented in a context in which there was:

— no reliable electoral list or any demographic data from 1984 onwards.

— a lack of basic infrastructure; in the DRC there are only 42,000 fixed phone lines for a population of over 73 million, and only 9 per cent of the country has access to electricity.

— no centralised fingerprint matching system within the system itself, meaning that checking for duplicates within the registration system could not be carried out within the DRC itself, but instead by the European company that designed the system.

— a high degree of machine malfunction, and systematic flaws in the system that required its redesign.

Despite these problems, biometric registration went ahead and was used in the 2006, 2009 and 2011 elections. Yet the country has remained plagued by undemocratic institutions and claims of electoral fraud; in 2011 violence broke out when doctored ballot papers were found. A leaked report from Zetes recorded that there had been more than 700,000 double registrations on the biometric system.

EISA, (2010), "Voter Registration in Africa: A Comparative Analysis', Case study on DRC by Akumiah, H., p.57-102, available at: http://www.eisa.org.za/PDF/vrafrica.pdf

McElroy, D., (2011), 'UK pays £22.5 million for 'questionable' Democratic Republic of Congo election' from The Telegraph [online] 16 October 2011, available at: http://www.telegraph.co.uk/news/worldnews/africaandindianocean/democraticrepublicofcongo/8830144/UK-pays-22.5-million-for-questionable-Democratic-Republic-of-Congo-election.html

While biometric identification systems may offer significant opportunities for development, equally they may not be suitable for countries where there is very little communications or transport infrastructure. Biometric identification systems require a constant electricity supply, and registration kits include a computer and printer at a minimum. They may require reliable transportation, highly trained personnel to operate the systems, a network connection, an accessible and accurate civil or voter registry, webcams, extensive data storage facilities or any number of additional components in order to operate effectively. Just as with those development projects that provide infrastructure to a community without the tools, expertise and capacity to maintain and integrate such infrastructure, so too are biometric projects which do not take into account the local context doomed to fail.

Although many biometric identification systems have been adapted for use in difficult conditions (primarily by encasing the kits in hardy coverings, and budgeting for back-up electricity generators) the nature of this technology means that it can be fragile and susceptible to damage, or attractive to thieves. Any investment into a biometric identification system simultaneously requires investment into the infrastructure required to support and protect these systems. However, research suggests that despite claims by proponents, biometric systems are not infallible, and systems and processes around biometric registration are susceptible to fraud, forgery and corruption. Research into medical record registries, for example, reveals that leaked or stolen medical information has not only been sold for profit, but has been used by government agencies and to publicly shame political figures.[108]

The possibility for misuse of biometric identification information is high, and the potential for harm to follow is very real. The ability for digital identification systems to be used as a means of surveillance has been recognised by producers of biometric technologies and even emphasised as a selling point to make the technology attractive to repressive regimes. The director of one firm involved with the deployment of Egypt's ID system under Mubarak, and

funded by the Danish Aid Agency DANIDA, recognised that "[the technology] could be used for surveillance… We can easily design a program for the ID card which enables surveillance of user's internet activities or conversations on Skype… This is business, we sell to those who are interested. If I was approached by Iran I would sell to them."[109]

Biometrics is a growth market for technology companies, particularly in developing countries. Zetes, the supplier of biometric technology to Cape Verde, Ivory Coast, DRC and Togo states on its corporate website that "the interest of governments and international institutions in biometrics is growing". They note "in the Western world, the use of biometrics has been raising some privacy concerns. That doesn't seem to be the case on the African continent, where biometrics are regularly used".[110]

As the role of the private sector in providing biometrics systems to the governments of developing countries continues to expand, the problematic nature of such relationships becomes increasingly clear. Procurement contracts have been questioned in the case of the Muhlbauer group in Uganda,[111] Semlex in Mozambique,[112] Net1 in South Africa,[113] and Giesiecke & Devrient in Cameroon.[114] In Mozambique, several stakeholders accused the National Electoral Commission of a lack of transparency.[115] Much of the equipment provided by Mühlbauer to Uganda has been lost or broken, and only 400 ID cards had been produced since the contract began in 2010 up until late 2011.[116] Recently, Mastercard and Nigeria announced a shared initiative to deploy a shared national ID that would combine biometric functionality with electronic payments. There is little information on how information will be managed between the company and the government.[117]

Mobile phones and data

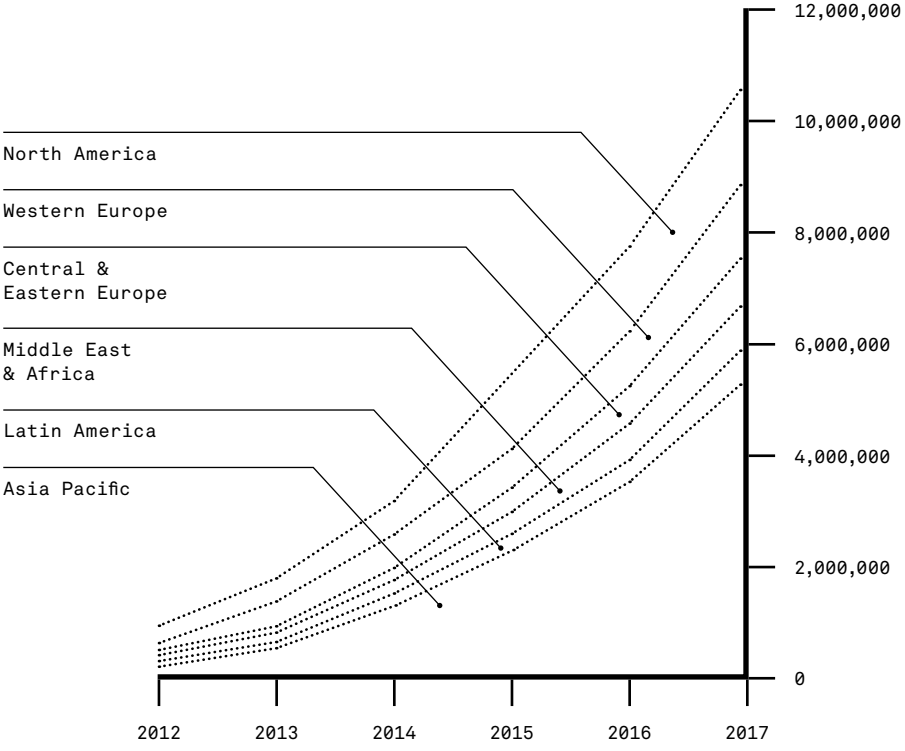
5.1 The promise

The arrival of mobile telephony in developing countries has played a crucial role in the success of many development interventions over the past ten years. Mobile phones have not only greatly improved opportunities for communication and expression, they have enabled financial empowerment, provided access to information and services, and revolutionised the collection and recording of information in humanitarian disasters. Systems such as Kenya's M-PESA mobile money system, which allows individuals to bypass traditional financial infrastructure and access and transfer money by SMS, has greatly reduced the financial exclusion of vulnerable groups, improving their ability to save money and accumulate assets. In the first three months of M-PESA's operation, 11,000 people registered for the service, and nearly US $6million was transferred; today it is used by a quarter of the population, some of whom had not previously used mobile phones or owned bank accounts.[118]

Linked to the proliferation of mobile phones in developing countries are initiatives designed to use the data generated or collected by mobile phones to conduct analysis about trends and events that might inform future development and humanitarian initiatives. 'Big data' – the amassing and analysis of high volumes of digitial data to uncover new correlations – is taking the development world by storm, facilitated by the rapid reproduction of the quantity and diversity of data generated by digital activities conducted on mobile phones, particularly smart phones – call logs, mobile-banking transactions, online user-generated content, online searches, satellite images, etc. Algorithms are applied to develop intelligence on people, groups, and events and places. With enough data, the theory goes, we even can try to predict behaviour based on past activities.

International agencies and organisations such as UN Global Pulse,[119] UN Economic Commission for Latin America and the Carribbean,[120] OECD[121] and the World Economic Forum[122] have all sung the praises of data as a tool to accelerate development, reduce poverty, spur innovation, and improve accountability and transparency. A recent report of the UN High Level Panel on the Post-2015 Development Agenda went so far as to call for "a New Data Revolution", drawing on existing and new sources of data "to fully integrate statistics into decision making, promote open access to, and use of, data and ensure increased support for statistical systems."[123]

Global mobile data traffic growth & forecast (terabytes per month)



Source: Cisco, “Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012–2017”, February 2013; “Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2009–2014”, February 2010.

5.2 The potential

The use of mobile phones in developing countries to collect or generate data, and the subsequent analysis of such data, has the potential to assist in development and humanitarian initiatives in multiple ways:

— Health services: mobile phones are used as a means to dispense health information and connect individuals to health services. mHealth for Development, founded by the UN Foundation and Vodafone, supports the use of mobile phones to send SMS text alerts to enable patients to adhere to their prescriptions, and to train health care workers. In Ghana, the Millennium Villages Project provides diagnosis and treatment support to rural health workers.[124]

— Health trends: big data analysis of mobile phone location and social media trends is used to track public health trends. Such tools have been employed with success in Haiti: research from the cholera outbreak there identified Twitter as a useful source of information about the extent of the outbreak. By analysing over 188,000 tweets spanning a three-month period, researchers were able to monitor the outbreak and its progress much faster than through government processes that involved surveying hospitals and clinics. Other researchers conducted analysis of cell tower data to plot the location of populations fleeing from the outbreak.[125]

— Crisis mapping: by using data submitted crowd-sourced from mobile phone users on security or humanitarian crises, crisis mapping platforms are able to map incidences of violence or disasters. A prominent example of such a platform is Ushahidi in Kenya, funded by, among others, the Ford Foundation and MacArthur. Ushahidi played an important role in the post-earthquake response in Haiti, enabling the creation of a crisis map of urgent humanitarian needs.[126]

— Infrastructure and services: big data can be used to map infrastructure and the use of public services like transport. Telecommunications company Orange recently opened a big dataset of 2.5 billion anonymised text messages and phone calls from Côte d'Ivoire, enabling researchers to analyses and redesign bus routes in the country.

— Reporting: mobile governance projects such as Mexico's Citivox and India's Kerala State IT Mission enable citizens to register to vote or report crime and corruption via their mobile phone.

— Conflict prevention: emerging research argues that big data can be used to prevent conflicts, by distinguishing digital patterns and interpreting them in the applicable socioeconomic and political context, or studying cause and expressions of concerns and stress in a given community.[127]

— Monitoring and evaluation: big data can be used to analyse large populations and report back to funders on the effectiveness of programmes.

5.3 The problems[128]

In an age of widespread communications surveillance by both State and non-State actors, using mobile networks to transmit sensitive data is inherently risky. Development and humanitarian initiatives that use mobile phones to collect or generate information thus risk such information being exposed to potentially malevolent third parties; or fraudulently amended or misappropriated.

Mobile health is an area around which particularly serious concerns arise. A recent report by TrustLaw, in collaboration with the mHealth Alliance, recognised that the lack of comprehensive data protection and privacy protections in developing countries has impeded the effective expansion of mHealth initiatives.[129] Numerous practical

barriers stand in the way of mobile health initiatives; although mobile phones are arguably the success story in the domain of information technology and development, their diffusion still is not universal. Not everyone has a mobile phone. Often phones are shared by families; in some contexts, the dominant male in the household (usually the father) 'owns' the phone. In this scenario, the use of mobile phones for notifying individuals about, for example, a test result, to report incidents of domestic violence, or to provide reminders about an appointment of which their family members were not previously aware is a complicated affair. What sort of information should be disclosed in the text message itself? While it may be possible to exclude specifics about a disease or medication, in certain areas the mere fact that one is being contacted by a health actor can be stigmatizing. Therefore, some eHealth systems have started obfuscating these messages, using codes such as sport scores or messages from 'friends' to communicate sensitive health data.

However, there are other complications to the use of mobile phones for health. Across the globe, governments are requiring citizens to register their SIM cards with personal information. An example of this is the case of VidaNet, a HIV patient reminder system in operation in Mexico City, which is currently struggling to provide a privacy-friendly service as the country enforces a national SIM registration program.

Not only disseminating information is problematic; gathering and analysing big data sets of mobile phone activity also presents a serious challenge to the protection of individuals. Digitising data and pairing it with multiple other data sources can result in the mosaic effect, allowing for data elements that in isolation appear non-personal or innocuous to be combined to enable the detailed profiling of individuals. It imagines that personal information is a resource that can be mined and disclosed by the organisation without any consideration of the wishes of the individual.

Proponents of big and open data argue that their information is anonymised, and the analyses are about the aggregate, not the individual. The serious problems with data anonymisation[130] and

the potential for de-anonymisation have been well publicised and continue to plague the big and open data movements, despite assurances by regulators that such risks can be mitigated.

The problems of anonymisation are enhanced by the lack of safeguards and standards inherent in data for development initiatives. International consensus on detailed data protection standards remains a work in progress, data protection legislation is still largely absent on the African continent, and few development and humanitarian organisations have self-standing data protection and privacy policies to guide their work in developing countries. As the UN itself admits, "while private-sector organisations and [g]overnment regulators have been grappling with this issue for almost a decade, humanitarian organisations appear further behind."[131] In the absence of strong legal safeguards and accountability institutions individuals in developing countries have little recourse against the violation of their privacy.

Data is not context free. Developing countries are also plagued by historical divisions, ethnic conflicts and other social and cultural vulnerabilities that heighten the risk that big and open data will be misused. Discrimination or persecution could easily be the result of de-anonymisation of big data pertaining to, for example, electoral trends, public health issues, political activity or location. Call and text message records held by the private sector, for example, were used by the Egyptian authorities to track down and convict protesters in the aftermath of anti-government food protests in 2008.[132] The risk of the misuse of personal data is heightened when data is open and thus accessible by any one for any reason. Even the open digitisation and publication of seemingly banal information can have adverse effects – in Pakistan, for example, the publication of locations of food distribution points and clinics led to threats to aid workers responding to floods.[133] Big data initiatives such as that conducted by Orange in Côte d'Ivoire have shown that even a basic mobile phone traffic data set can enable conclusions about social divisions and segregation on the basis of ethnicity, language, religion or political persuasion. As Alex Pentland, director of the

Human Dynamics Lab at MIT, points out, "imagine what Muammar Qaddafi would have done with this sort of data."[134]

Data integrity challenges also emerge where false positives and false negatives may arise as systems are gamed or the wrong interpretations are applied to the data sets. The potential for fetishisation of data and the prospect that data will be misinterpreted or manipulated to support particular viewpoints is high. As Steve Song points out,[135] the big and open data movements are founded on an assumption that 'data', 'facts' and 'truth' are roughly equivalent. Data can be politicised or misrepresented and yet come to represent an authoritative version of the truth, having serious implications for decision-making that could deeply affect individuals' life choices and futures. A pertinent example is that of nutrition policy in Ethiopia, where a piece of data from a 2000 survey showing the high rate of stunting in Amhara, a region that at that time was not listed as food insecure, was used to show that malnutrition was a pervasive rather than acute problem and served as a motivating factor in the formation of a national nutrition policy, despite this data being incompatible with other pieces of data.[136]

Border surveillance and security

6.1 The promise

The nexus between security and development and the recognition that security helps to create the necessary conditions for development has long been at the heart of many development and humanitarian interventions.[137] The debate, however, about how to conceptualise and achieve security is an ongoing one, with the development community generally moving towards referencing an understanding of 'human security' over traditional conceptions of military security. Running in parallel with this discourse shift is the increasing priority given the transfer of knowledge, tools, and technologies as a means of achieving security in developing countries. Perceived as essential to ensuring the effectiveness of humanitarian aid and the growth of democratic institutions and the rule of law, foreign security assistance and training takes the form of the transfer of capacity, personnel and technologies to both the civilian and military sectors. As noted by US President Obama in the 2010 National Security Strategy:

> "Proactively investing in stronger societies and human welfare is far more effective and efficient than responding after state collapse. The United States must improve its capability to strengthen the security of states at risk of conflict and violence. We will undertake long-term, sustained efforts to strengthen the capacity of security forces to guarantee internal security, defend against external threats, and promote regional security and respect for human rights and the rule of law. We will also continue to strengthen the administrative and oversight capability of civilian security sector institutions, and the effectiveness of criminal justice."

According to donors and funding agencies, supporting security is essential to stemming human rights violations and promoting the rule of law. USAID's programme for civilian law enforcement assistance to developing countries is informed by "democratic policing principles" that include respect for human dignity and the basic human rights of all persons.[138]

Technology transfers in the field of security, at least the ones our research was able to identify, are particularly focused on achieving border security, which is perceived as a serious threat to security and development in developing countries. Proponents of border security technology – which includes the use of biometric registration schemes, automated gates and digitised entry and exit systems – argue that such technology, in addition to minimising illegal border flows, can improve mobility, efficiency and enable freedom of movement for legitimate travellers and migrants.

6.2 The potential

International development assistance designated for security and rule of law initiatives often takes the form of capacity building to law enforcement through Security Sector Reform (SSR), judicial reform and disarmament, and demobilisation and reintegration (DDR) projects in the case of post-conflict countries. International organisations like INTERPOL,[139] as well as mainstream aid and development agencies like the UK's Department for International Development (DfID), provide guidance and training to officials for reasons including "[t]o improve the capability, accountability and responsiveness of the Police, and demonstrate its commitment to reform".[140] DfID provided £60 million in funding to a programme in the DRC on accountability in the police sector[141] which was aimed at helping engagement with civil society and local communities and protecting human rights. A similar programme in South Sudan worth £20 million expects to see an increase in each "citizen's personal security, human rights protection and access to justice."[142]

Increasingly, however, international assistance for security comes in the form of the transfer of new technologies. Border surveillance technologies are commonly supplied to developing countries by bilateral donors or funding organisations. The Bolivian government, for example, has received assistance from Cuba to establish a centralised biometric registry to check everyone entering Bolivia against a list of criminals and suspects.[143] The World Bank is funding a Dutch company, Gemalto, to implement a digital visa and border management in Ghana.[144] Under a project called West Sahel, the Spanish Guardia Civil is providing border control assistance to police and gendarmerie forces in Senegal, Mauritania, Mali, Niger, Cape Verde, Burkina Faso, and Guinea-Bissau. The project has received €2.44 million, with 80 per cent of its funding coming from the EU[145] and the remaining 20 per cent from the Guardia Civil.

The US Government has provided a biometric border control system to the Maldives.[146] From 2010 to 2012, the US Department of State and USAID collectively allocated US$203 million in assistance to the Caribbean Basin Security Initiative, a security assistance programme in the Bahamas, the Eastern Caribbean, Guyana, Jamaica, Suriname, Trinidad and Tobago, and the Dominican Republic.[147] They have provided training on surveillance, investigation and interrogation techniques, as well as a polygraph operator training to Jamaica to develop a group of regional polygraph experts.[148]

The International Organization for Migration (IOM) has provided programmes throughout West Africa to encourage the use of secure travel documents and has been involved in helping boost border infrastructure (border posts and entry-exit databases) in Mauritania, a key 'transit' country for migrants heading towards Europe. It is noteworthy that this IOM program has been partly funded by the 9th European Development Fund (EDF). Senegal has also installed, with help from the European Union, automated border gates at Dakar airport (which lie unused).

Since the massive maritime migration to the Canary Islands in 2005/6, the EU's border control infrastructure is also heavily present in West Africa, and the EU's external borders agency FRONTEX is currently negotiating border control agreements with Senegal and Mauritania. These build on existing joint maritime border control measures put in place by FRONTEX and bilaterally between the Spanish Guardia Civil and local security forces. In addition to this, the EU's development goals for the Sahel region specifically aim to improve citizens' material livelihoods but explicitly identify low development as an incubator of state failure and transnational threats.

Finally, the Council of the European Union has established a civilian EU integrated border management assistance mission in Libya, costing €30.3 million over 12 months. It will be undertaken "mainly through the transfer of know-how, not funds."[149] The EU is proud of its role in border management funding, claiming "[t]he leading role of the EU in the field of support to border management is fully recognised by the international community." While the emphasis is only border management, "human rights and links to the wider rule of law reform will also be part of the activities."[150]

In addition to border security technologies, donors are also channelling funds into supporting the establishment of criminal databases in developing countries. EuropeAid funds the 'West Africa Police Information System' alongside INTERPOL and the Economic Community of West African States (ECOWAS). The programme will support the construction of a criminal database, with plans to allow data-sharing amongst countries in Africa and possibly across all INTERPOL member states. It is starting with five pilot countries: Benin, Ghana, Niger, Mauritania, and Mali.[151]

A final, and growing, area of technology transfer is that related to communications surveillance technologies. The US government has played a considerable role in supporting the establishment of communications surveillance capabilities. Reportedly, the

Paraguayan government uses communications surveillance capabilities developed by US agencies for narcotics-related investigations in Paraguay for political purposes.[152] The US military provided Iraq's Interior Ministry with a nation-wide communications surveillance facility.[153]

6.3 The problems

Serious risks exist in supporting the transfer of security technologies to the developing world. Without strong legal frameworks and constitutional protections to forestall abuse, improving the power and capacity of law enforcement and intelligence agencies represents a threat to the most vulnerable people. In 2008, DfID was forced to pull funding out of one capacity-building project in Somalia because "the systems were not in place to ensure funding was spent in accordance with objectives and allegations were arising of human rights abuses and conflict by internationally trained police".[154] Where projects are jointly instituted, such as the INTERPOL/ECOWAS criminal database, confusion as to the applicable laws and regulations creates a 'lowest common denominator' situation that puts individual rights at risk.

Political instability and corruption make new technologies vulnerable to misuse or misappropriation by repressive State actors or authoritarian elements. There is significant demand amongst such elements for surveillance capabilities.[155] Surveillance systems available on the private market have been widely sought by non-democratic governments, including those of Sudan, Somalia, Tonga, Democratic Republic of the Congo, Zimbabwe and Egypt.

The provision of security assistance may also compromise the independence of security forces and law enforcement. For example, by providing a costly border security system to the Maldives, the US government was potentially able to secure some de facto control of how that system is employed.[156]

The former Immigration Controller and now State Defence Minister Ilyas Hussain Ibrahim was previously quoted as being concerned about the system, stating that US involvement in the border control system would allow the country to exert its influence on Maldivian affairs, providing "a door for American influence" by allowing the US to take control of the system and use it to locate foreign nationals whenever it wished.

Development at the expense of human rights? The case for caution

7.0

The recent landmark UN report, 'Humanitarianism in a Networked Age', recommended that organisations should protect individuals through the adoption of "Do No Harm" standards for the ethical use of new forms of data, including protocols for protecting privacy, and develop frameworks to hold practitioners responsible for adherence to ethical and technical standards.

It is the contention of this paper that a far more active approach is needed to ensure that the adoption of new technologies in development and humanitarian initiatives do not imperil, but rather promote, the human rights of those they purport to benefit.

The cases and examples presented in this report show that technologies are indeed a key component of modern development and humanitarian policies and programmes, and will continue to inform development policy as technologies improve and enable development actors to not only be more effective but also to monitor and assess their own effectiveness. With increased pressures on aid agencies to improve their monitoring and evaluations and to ensure the efficient disbursement of aid funds, there will be ever-increasing pressure to collect data and replace expensive human resources with cheaper technological solutions. Yet it is also clear from this review that increasingly the technologies and techniques adopted by bilateral donors and international funding agencies are often supporting surveillance and undermining individual liberties. They are achieving development at the cost of human rights, particularly the right to privacy and protection of personal information.

The technologies identified in this report not only facilitate surveillance far beyond that which would be acceptable and lawful in more developed countries, but they do so in contexts

in which adequate legal safeguards are all but absent. Introducing technologies to solve complex social problems in resource-poor environments without strong democratic institutions is thus an exercise fraught with new types of risks.

It is essential that the development and humanitarian community has informed and realistic debates about whether a technological system should be developed, and deployed in a particular context. This debate is not about being against technology. Technologies undoubtedly have the potential to dramatically improve the provision of development and humanitarian aid and to empower populations. The expectations that are placed on technologies to solve problems, however, need to be significantly circumscribed, and the potential negative implications of technologies considered. Biometric identification systems, for example, may assist in aid disbursement, but if they also wrongly exclude whole categories of people, then the objectives of the original development intervention have not been achieved. Border surveillance and communications surveillance systems may help a government improve national security, but are equally likely to enable the surveillance of human rights defenders, political, immigrants, and other groups.

Beyond an ethical debate about whether surveillance technologies should or should not be employed, there are extensive legal debates about the compatibility of such programmes with national, regional and international human rights instruments.[157] Privacy is of course recognised at both the international and regional levels as a fundamental human right. The right to privacy is enshrined by the Universal Declaration of Human Rights (art. 12), the International Covenant on Civil and Political Rights (art. 17); the International Convention on the Protection of All Migrant Workers and Members of Their Families (art. 14); and the Convention on the Rights of the Child (art. 16). At a regional level privacy is protected by the African Charter on the Rights and Welfare of the Child (art. 10), the American Convention on Human Rights (art. 11), and the Arab Charter on Human Rights (art. 17). The recently adopted Association of Southeast Asian Nations Human Rights Declaration

also explicitly applies the right to privacy to personal data (art. 21). Many more countries have legislation providing for data protection: at last count there are at least 100 countries with data protection laws.

Importantly, the vast majority of developing countries also have explicit constitutional requirements to ensure that their policies and practices do not unnecessarily interfere with privacy. In fact, only five Medium and Low Human Development Index countries do not have explicit mentions of privacy in their constitutions (Cameroon, Comoros, India, Indonesia, and Samoa).

The benefits of development and humanitarian assistance can be delivered without surveillance. The choice between privacy and development creates a false dichotomy and spurs over-simplified arguments about the role of technology. The discussion reveals no nuance, no consideration of the values and priorities tied up in privacy and development, no reference to the potentials of technology or the changing nature of threats and security, and no indication of the other choices that exist. The challenge is to improve access to and understanding of technologies, ensure that policymakers and the laws they adopt respond to the challenges and potentialities of technology, and generate greater public debate to ensure that rights and freedoms are negotiated at a societal level. Technologies can be built to satisfy both objectives.

Even if privacy was deemed to be secondary to the building of effective, modern and secure States, and to the provision of basic aid, the moral question still arises: if the purpose of development is to empower those in developing countries to have access to the same rights and capabilities as those in the developed world, and if the transfer of knowledge and technology is essential to that, then why diminish those very same people by granting them lesser human rights protections? If privacy and the protection of personal information are essential as constitutional and human rights in developed societies, this must also be true in developing countries.

Endnotes

01_ The authors are grateful to Aaron Martin, Kevin Donovan, Philippe Frowd, Sunil Abraham and Courtenay Crawford for their input and feedback. We are grateful to the International Development Research Centre, particularly Matthew Smith, and to the Open Society Foundations, for their support.

02_ David Lyon, Surveillance Society: Monitoring Everyday Life. Buckingham: Open University Press, 2001.

03_ David Lyon, Surveillance Studies: An Overview, Polity Press, 2007.

04_ For a good overview, see 'A Report on the Surveillance Society: for the UK Information Commissioner', the Surveillance Studies Network, September 2006, available at: http://www.ico.org.uk/~/media/documents/library/Data_Protection/Practical_application/SURVEILLANCE_SOCIETY_FULL_REPORT_2006.ashx

05_ Anthony Giddens, The Nation State and Violence, Cambridge: Polity, 1985.

06_ Although there are early indications that the tide may be turning in this respect. As an example, the elections in Kenya in 2013 were heralded originally for the millions spent on biometric and other technologies, and being more advanced than Europe's elections. At the time of writing this report, other narratives had emerged, e.g. 'Safaricom warned of Kenya count problems', Financial Times, March 7 2013; and 'School Socket Syndrome', NY Times blog, March 7 2013, available at: http://latitude.blogs.nytimes.com/2013/03/07/in-kenyas-high-tech-election-almost-everything-that-could-have-gone-wrong-did/?smid=tw-share&pagewanted=all

07_ Whitley, E.A. & Hosein, G., 2010. Global Challenges for Identity Policies, Basingstoke: Palgrave Macmillan; and 'Global Identity Policies and Technology: Do we Understand the Question?', Edgar Whitley and Gus Hosein, Global Policy, Vol. 1, Issue 2, May 2010 available at: http://www.globalpolicyjournal.com/articles/science-and-technology/global-identity-policies-and-technology-do-we-understand-question

08_ ‘Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations’, Gus Hosein and Aaron Martin, The London School of Economics and Political Science, available at: http://www2.lse.ac.uk/management/documents/electronic-health-privacy.pdf

09_ See, for example, the work of the Center for Global Development, http://international.cgdev.org/

10_ This paper refers to the ‘development community’ or ‘development and humanitarian communities’ as monolithic entities, although of course they are not. We have sought to focus here on the overwhelming trends, but we acknowledge that there are some elements of such communities that are pushing back against the wholesale adoption of new technologies and see privacy and the protection of personal information as important.

11_ ‘Scrapping ID cards is a momentous step: ID cards represented the worst of government. Abolishing them is a statement of our intent to create a fairer and freer society’, Damian Green, The Guardian, December 21, 2010, available at: http://www.guardian.co.uk/commentisfree/2010/dec/21/scrapping-id-cards-momentous-step

12_ ‘High Court: Israel’s biometric database is ‘extreme and harmful’, Haaretz, July 24 2012, available at: http://www.haaretz.com/news/national/high-court-israel-s-biometric-database-is-extreme-and-harmful-1.453155

13_ ‘South Korea’s real-name net law is rejected by court’, BBC, August 23, 2012, available at: http://www.bbc.co.uk/news/technology-19357160

14_ See S and Marper v UK, European Court of Human Rights Grand Chamber, December 4 2008, available at: http://www.bailii.org/eu/cases/ECHR/2008/1581.html

15_ See ‘NHS told to abandon delayed IT project’, the Guardian, September 22 2011, available at: http://www.guardian.co.uk/society/2011/sep/22/nhs-it-project-abandoned

16_ See ‘DNA profiles to be deleted from police database’, BBC, February 11 2011, available at: http://www.bbc.co.uk/news/uk-12433116

17_ See ‘Privacy Commissioner applauds dismantling of database’, Office of the Privacy Commissioner of Canada, May 29 2000, available at: http://www.priv.gc.ca/media/nr-c/archive/02_05_b_000529_e.asp; and ‘Contactpoint to be disconnected today and deleted in eight weeks’, Computerweekly, August 29 2010, available at: http://www.computerweekly.com/news/1280093489/Contactpoint-to-be-disconnected-today-and-deleted-in-eight-weeks

18_ See ‘Statement of support from provincial and territorial Information and Privacy Commissioners in letter to Minister of National Revenue’, November 12, 2002, available at: http://www.priv.gc.ca/media/le_021113_e.asp

19_ See ‘Strategic Solution for US-VISIT Program Needs to be Better Defined, Justified, and Coordinated’, Government Accountability Office, February 2008, GAO-08-361.

20_ ‘MEPs reject EU passenger data storage scheme’, Euractiv, April 30 2013, available at: http://www.euractiv.com/infosociety/meps-reject-eu-passenger-data-st-news-519327

21_ ‘Air passenger data collection plan dropped: Homeland Security chief reportedly heeds cites privacy concerns’, NBC, July 18, 2004, available at: http://www.nbcnews.com/id/5440542/ns/technology_and_science-tech_and_gadgets/t/air-passenger-data-collection-plan-dropped/

22_ See ‘Joint U-US group to assess US spy ops’, BBC, 3 July 2013, available at: http://www.bbc.co.uk/news/world-europe-23165257

23_ See ‘UN human rights chief says whistleblowers need protection’, 13 July 2013, available at: http://rt.com/news/un-chief-snowden-protection-048/

24_ See ‘NSA and GCHQ spy programmes face legal challenge’, The Guardian, 8 July 2013, available at: http://www.theguardian.com/uk-news/2013/jul/08/nsa-gchq-spy-programmes-legal-challenge

25_ For this discussion, see pages 22, 26–28 of ‘Can ID? Vision for Canada’s Identity Policy’, Krista Boa, Andrew Clement, Simon Davies, Gus Hosein, University of Toronto and the London School of Economics and Political Science, 2009, available at: http://www2.lse.ac.uk/management/documents/Visions-for-Canadas-Identity-Policy.pdf

26_ 'Update: Nigerian lawmakers order immediate suspension of $40 million internet surveillance contract', Premium Times, May 30 2013, available at: http://premiumtimesng.com/news/136926-breaking-nigerian-lawmakers-order-immediate-suspension-of-40-million-internet-surveillance-contract.html

27_ Available at: https://docs.unocha.org/sites/dms/Documents/WEB%20Humanitarianism%20in%20the%20Network%20Age%20vF%20single.pdf

28_ Available at: http://www.post2015hlp.org/the-report/

29_ Philip Alston and Mary Robinson, 'The Challenges of Ensuring the Mutality of Human Rights and Development Endeavours', in Alston and Robinson (eds), Human Rights and Development: Towards Mutual Reinforcement (Oxford: Oxford University Press, 2005).

30_ Report of the Secretary-General of the United Nations, In Larger Freedom: Towards Security, Development and Human Rights for All, 2005, available at: http://www.un.org/largerfreedom/

31_ 'USAID Launches new strategy on democracy, human rights and governance to advance freedom, dignity and development,' USAID, July 11 2013, available at: http://www.usaid.gov/news-information/press-releases/usaid-launches-new-strategy-democracy-human-rights-and-governance

32_ 'World Bank criticized over human rights checks,' BBC, 22 July 2013, available at: http://www.usaid.gov/news-information/press-releases/usaid-launches-new-strategy-democracy-human-rights-and-governance

33_ 'Remarks on Building Sustainable Partnerships in Africa', August 2 2012, Dakar Senegal, http://www.state.gov/secretary/rm/2012/08/195944.htm

34_ Hillary Clinton launches African tour with veiled attack on China', The Guardian, August 1 2012, http://www.guardian.co.uk/world/2012/aug/01/hillary-clinton-africa-china

35_ 'Development Note – EU Somalia Unit', September 2011 to May 2012, available at: http://eeas.europa.eu/delegations/somalia/documents/press_corner/newsletters/dev_note_en.pdf

36_ 'US Support for Strengthening Democratic Institutions, Rule of Law and Human Rights in Sub-Saharan Africa,' The White House Office of the Press Secretary, 27 June 2013, available at: http://m.whitehouse.gov/the-press-office/2013/06/27/fact-sheet-us-support-strengthening-democratic-institutions-rule-law-and

37_ 'M-PESA: 1 million Kenyans bank by phone,' DFiD, 19 October 2007, available at: http://webarchive.nationalarchives.gov.uk/+/http:/www.dfid.gov.uk/media-room/news-stories/2007/M-PESA-1-million-kenyans-bank-by-phone/

38_ UN OCHA, Humanitarianism in a Networked Age, 2012.

39_ Strengthening the role of the United Nations in enhancing the effectiveness of the principle of periodic and genuine elections and the promotion of democratization: Report of the Secretary-General, August 14, 2009, A/64/304.

40_ "Procuring and Using Technology in Electoral Management: solutions and risks", UNDP, 2011, available at: http://www.undp.org/content/undp/en/home/ourwork/democraticgovernance/global_programmes/global_programmeforelectoralcyclesupport/highlights/procuring_and_usingtechnologyinelectoralmanagement0.html

41_ 'Evaluation of DFID's Electoral Support through UNDP', Independent Commission for Aid Impact, Report 8, April 2012.

42_ See 'Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations', Policy Engagement Network, The London School of Economics and Commissioned by the International Development Research Centre, December 2010, available at: http://www.lse.ac.uk/management/documents/Electronic-Health-Privacy.pdf. It was later referenced by the World Health Organisation report on 'Legal Frameworks for ehealth', available at: http://whqlibdoc.who.int/publications/2012/9789241503143_eng.pdf

43_ See a review in Whitley, E.A. & G Hosein, 2010. Global Challenges for Identity Policies, Basingstoke: Palgrave Macmillan.

44_ 'Kenya: Spy system tender for cops frozen', Carole Maina, The Star, January 23 2013, available at: http://allafrica.com/stories/201301231371.html

45_ 'US to provide Maldives with cost-free border control system', Neil Merrett, Minivan News, March 28 2013 http://minivannews.com/society/us-to-provide-maldives-with-cost-free-border-control-system-55343

46_ 'Update: Nigerian lawmakers order immediate suspension of $40 million internet surveillance contract', Premium Times, May 30 2013.

47_ ILO, World Social Security Report 2010/2011: Providing coverage in time of crises and beyond, 2010, pp.13–15.

48_ G20, "Cannes Summit Final Declaration; Building our Common Future: Renewed Collective Action for the Benefit of All," 4 November 2011, para 4.

49_ Which collaborates on social protection programmes in Bangladesh, Pakistan, Yemen, the Occupied Palestinian Territories, Ethiopia, Kenya, Mozambique, Rwanda, Uganda, Zambia, Zimbabwe, South Sudan, Ghana, Nigeria and India. See Paul Wafer, "Current DFID engagement on social protection", May 2010, presentation to ILO Geneva 'Show & Tell event'.

50_ See, for example: http://www.spss.am/

51_ See, for example: http://ec.europa.eu/social/main.jsp?catId=750&langId=en

52_ See, for example: http://siteresources.worldbank.org/SOCIALPROTECTION/Resources/280558-1274453001167/7089867-1279223745454/7253917-1291314603217/SPL_Strategy_2012-22_FINAL.pdf

53_ See, for example: http://www.unicef.org/socialprotection/framework/

54_ For a comprehensive study on the impact of cash transfer programmes, see Barrientos, A., and Niño-Zarazua M., The effects of non-contributory social transfers in developing countries: A Compendium, (Brooks World Poverty Institute, University of Manchester, 2010).

55_ The World Bank, The Contribution of Social Protection to the Millennium Development Goals, Washington, D.C, 2003, p.04; and A/HRC/11/9 p.19.

56_ Barrientos A. and R. Holmes, Social Assistance in Developing Countries Database (Brooks World Poverty Institute, The University of Manchester, and the Overseas Development Institute, 2006).

57_ Rosati, F.C., Cigno, A. and Z. Tzannatos, Child Labor Handbook, Social Protection Discussion Paper No.0206, (World Bank, 2002).

58_ For example, surveys of beneficiaries of Kenya's Hunger Safety Net Programme showed that 8.3 per cent of households walked more than four hours to collect their benefit, and the average walking time to and from the benefit collection location was 92 minutes, during which time almost half of all participants did not feel safe. See Valentina Barca, Alex Hurrell, Ian MacAuslan, Aly Vishram and Jack Willis, "Paying Attention to Detail: How to Transfer Cash in Cash Transfers," Oxford Policy Management Working Paper 2010–04, p.09.

59_ Stephen Devereau and Katharine Vincent, "Using technology to deliver social protection: exploring opportunities and risks," 20 Development in Practice 3 (May 2010).

60_ Stephen Devereau and Katharine Vincent, "Using technology to deliver social protection: exploring opportunities and risks," 20 Development in Practice 3 (May 2010), 373.

61_ HelpAge International, 2011, Good practice in the development of management information systems for social protection, available at: http://www.helpage.org/silo/files/good-practice-in-the-development-of--management-information-systems-for-social-protection.pdf

62_ Veronica Silva Villalobos, Gaston Blanco and Lucy Bassett, Management Information Systems for CCTs and Social Protection Systems in Latin America: A Tool for Improved Program Management and Evidence-Based Decision Making, October 2010, available at: http://siteresources.worldbank.org/SAFETYNETSANDTRANSFERS/Resources/MIS_brief_dec2010_FINAL.pdf

63_ HelpAge International, 2011 Good practice in the development of management information systems for social protection, p.12.

64_ Veronica Silva Villalobos, Gaston Blanco and Lucy Bassett, Management Information Systems for CCTs and Social Protection Systems in Latin America: A Tool for Improved Program Management and Evidence-Based Decision Making, October 2010, available at: http://siteresources.worldbank.org/SAFETYNETSANDTRANSFERS/Resources/MIS_brief_dec2010_FINAL.pdf

65_ "Kenya's Shift to Electronic Payments, an Example of Courageous Government," Better Than Cash, 17 July 2013, available at: http://betterthancash.org/from-calculated-risk-to-transformative-success-why-kenyas-shift-from-cash-to-electronic-payments-is-a-model-of-courageous-tenacious-government/

66_ Kristina Pitula, Daniel Sinnig and T Radhakrishnan, "Making Technology Fit: Designing an Information Management System for Monitoring Social Protection Programmes in St. Kitts, available at: http://sta.uwi.edu/conferences/09/salises/documents/D%20Dysart-Gale.pdf

67_ Kristina Pitula, Daniel Sinnig and T Radhakrishnan, "Making Technology Fit: Designing an Information Management System for Monitoring Social Protection Programmes in St. Kitts, available at: http://sta.uwi.edu/conferences/09/salises/documents/D%20Dysart-Gale.pdf

68_ Richard Heeks, "Information Systems and Developing Countries: Failure, Success, and Local Improvisations," The Information Society: An International Journal (2002) 18:2, 101–112.

69_ HelpAge International, 2011, Good practice in the development of management information systems for social protection, available at: http://www.helpage.org/silo/files/good-practice-in-the-development-of--management-information-systems-for-social-protection.pdf

70_ Kristina Pitula, Daniel Sinnig and T Radhakrishnan, "Making Technology Fit: Designing an Information Management System for Monitoring Social Protection Programmes in St. Kitts, available at: http://sta.uwi.edu/conferences/09/salises/documents/D%20Dysart-Gale.pdf

71_ Stephen Devereau and Katharine Vincent, "Using technology to deliver social protection: exploring opportunities and risks," 20 Development in Practice 3 (May 2010), 375.

72_ Stephen Devereau and Katharine Vincent, “Using technology to deliver social protection: exploring opportunities and risks,” 20 Development in Practice 3 (May 2010), 376.

73_ “Countering terror in humanitarian crises: the challenges of delivering aid to Somalia,” Program on Humanitarian Policy and Conflict Research, Harvard University, available at: http://www.hpcrresearch.org/sites/default/files/publications/Somalia%206-30-12%20final.pdf

74_ “Road improvement in Afghanistan,” UNOPS, available at: http://www.unops.org/english/whatwedo/UNOPSinaction/Pages/Road-improvement-Afghanistan.aspx

75_ ‘Improved Targeting Would Help Enable USAID to Reach Vulnerable Groups’, GAO-12-862, September 2012.

76_ Szreter, S., (2007) ‘The right to registration: development, identity and social security’ World Development, 35 (1): 67–86.

77_ ibid.; Article 7 of the UN Convention on the Rights of the Child states: “the child shall be registered immediately after birth and shall have the right from birth to a name, the right to acquire a nationality and, as far as possible, the right to know and be cared for by his or her parents.”

78_ “The Science of Delivering Online IDs to a Billion People: The Aadhaar Experience”, World Bank Live, 24 April 2013, available at http://live.worldbank.org/science-delivering-online-ids-billion-people-aadhaar-experience

79_ Alan Gelb and Caroline Decker, “Cash at your fingertips: biometric technology for transfers in developing and resource-rich countries,” Center for Global Development, June 2011.

80_ Alan Gelb and Caroline Decker, “Cash at your fingertips: biometric technology for transfers in developing and resource-rich countries,” Center for Global Development, June 2011, 17.

81_ Alan Gelb and Caroline Decker, “Cash at your fingertips: biometric technology for transfers in developing and resource-rich countries,” Center for Global Development, June 2011, 17.

82_ Alan Gelb and Caroline Decker, “Cash at your fingertips: biometric technology for transfers in developing and resource-rich countries,” Center for Global Development, June 2011, 21.

83_ UNDP Annual Report 2011/2012, available at: http://www.undp.org/content/dam/undp/library/corporate/UNDP-in-action/2012/English/UNDP-AnnualReport_ENGLISH.pdf

84_ UNDP, (2010), Procurement Notices, ‘Services and equipment for Biometric Duplicate Analysis of Voters Database and Printing of voters cards for upcoming elections in Benin’, available at: http://procurement-notices.undp.org/view_notice.cfm?notice_id=5624 Date accessed: 22.05.2012

85_ United Nations, (nd.), ‘Cape Verde: Election 2011: A Rooted Democracy’ available at: http://www.un.cv/arquivo-democracy.php

86_ UNDP, (2011), Procurement Notices, ‘Supply of Digital Voters’ Registration System (including mobile kits) for upcoming Voter Registration in Comoros’ available at: http://procurement-notices.undp.org/view_notice.cfm?notice_id=6871

87_ Zetes Corporation, (nd.), ‘Zetes delivers 10,000 biometric enrolment kits to the Democratic Republic of Congo’ available at http://www.zetes.com/en/references/people-id/congo, date accessed: 15.05.2012; UNDP, (nd.) ‘More than 30 million Congolese register to vote’, available at: http://www.undp.org/content/undp/en/home/ourwork/democraticgovernance/successstories/drc-voter-registration-second-national-elections.html

88_ UNDP, ‘New procedures contribute to credible elections, higher voter turnout in Sierra Leone’, available at: http://www.undp.org/content/sierraleone/en/home/ourwork/democraticgovernance/successstories/New-procedures-contribute-to-credible-elections/

89_ UNDP, (2010), ‘Peace and Security: two priorities for the Togo presidential elections’, available at: http://content.undp.org/go/newsroom/2010/march/paix-et-scurit--des-priorits-pour-les-prsidentielles-togolaises--.en

90_ UNDP, (2011), 'Zambians praised for peaceful elections', available at: http://www.undp.org/content/undp/en/home/presscenter/articles/2011/09/23/zambians-praised-for-peaceful-elections.html

91_ Harmonization for Health in Africa, (2010), Benin Improves Mechanism to Identify Poorest Households for Targeted Financial Access to Healthcare' available at: http://www.hha-online.org/hso/financing/news/1238/hso-supports-benin-identify-poorest-households-targeted-financial-access-health-

92_ World Bank, (2012), 'Social Safety Nets on the Rise in Africa' from the World Bank [online] available at: http://web.worldbank.org/WBSITE/EXTERNAL/COUNTRIES/AFRICAEXT/0,,contentMDK:23179724~menuPK:2246551~pagePK:2865106~piPK:2865128~theSitePK:258644,00.html

93_ Opportunity International, (2009), 'Overcoming Back-End Barriers, Opportunity International and Bank Switching Solutions' available at: http://c187197.r97.cf1.rackcdn.com/wp-content/uploads/2012/02/8_SwitchingSolutions.pdf

94_ USAID, (nd.), 'Guinea: Overview' from USAID [online], available at: http://www.usaid.gov/locations/sub-saharan_africa/countries/guinea/

95_"Giving Fresh Credibility to Kenya's Electoral System," USAID Kenya, 8 February 2013, available at: http://kenya.usaid.gov/success-story/1438

96_ EISA, (2010), "Voter Registration in Africa: A Comparative Analysis' p.219 available at: http://www.eisa.org.za/PDF/vrafrica.pdf

97_ Olusegun Ogundeji, "Sierra Leone: SDI Cites Flaw in NEC/UNDP Biometric Machines Procurement", All Africa, 07 December 2011, http://allafrica.com/stories/201112080807.html

98_ Kakaire, S., (2012), 'Uganda: National ID card scheme rakes in billions of losses' from www.allAfrica.com available at: http://allafrica.com/stories/201204130995.html

99_ EISA, (2010), "Voter Registration in Africa: A Comparative Analysis' p.219 available at: http://www.eisa.org.za/PDF/vrafrica.pdf, p.120.

100_ Mamdani, M., (2002), When Victims Become Killers: Colonialism, Nativism and the Genocide in Rwanda, Princeton University Press: Princeton.

101_ ibid. p.260–261.

102_ Longman, T., (2001), 'Identity Cards, Ethnic Self-Identification, and Genocide in Rwanda' in Caplan, J., and Torpey, J., (eds.), Documenting Individual Identity: the development of state practices in the modern world, Princeton University Press: Princeton.

103_ EISA, (2010), "Voter Registration in Africa: A Comparative Analysis' Case study of Rwanda by Ukumiah, H., pgs 246-280 available at: http://www.eisa.org.za/PDF/vrafrica.pdf. Date accessed: 15.05.2012

104_ ibid. p.246.

105_ ibid. p.267.

106_ Breckenridge, K., (2005) 'The Biometric State: The Promise and Peril of Digital Governance in the New South Africa' in Journal of Southern African Studies, 31 (2) p.275.

107_ "Mauritanie: reduction des activities du HCR dans le camp de refugies maliens de Mbera," Medias for Africa, September 9, 2013, available at: http://www.mediaforafrica.net/mauritanie-reduction-des-activites-du-hcr-dans-le-camp-de-refugies-maliens-de-mbera/

108_ 'Electronic Health Privacy and Security in Developing Countries and Humanitarian Operations', Gus Hosein and Aaron Martin, The London School of Economics and Political Science, available at: http://www2.lse.ac.uk/management/documents/electronic-health-privacy.pdf

109_ Pedersen, A.,(2009), 'Danish-Egyptian Biometric ID-Card Scrutinized Before Take-off' from Global Voices Advocacy, 7th September [online], available at: http://advocacy.globalvoicesonline.org/2009/09/07/danish-egyptian-biometric-id-card-scrutinized-before-take-off/. Date accessed: 15.05.2012

110_ Zetes Group, (nd.) 'Stronger Identity with Biometrics' available at: http://www.zetes.co.uk/en/press-and-events/newsletter/globe-7/biometrics. Date accessed: 15.05.2012

111_ Gyezaho, E., (2011), 'Uganda Fresh Rot Revealed in National ID Deal' from www.allafrica.com 30th November available at: http://allafrica.com/stories/201111300145.html. Date accessed: 15.05.2012

112_ Anonymous, (2010) 'Interior Minister Defends Contract with Semlex' from Club of Mozambique [online] 25th November available at: http://www.clubofmozambique.com/solutions1/sectionnews

113_ http://mg.co.za/article/2012-08-28-sassa-ruling-illegal-but-wont-be-set-aside

114_ Anonymous, (nd.), 'Rivals cry foul as German firm wins Cameroon poll deal' from www.cameroononline.org available at: http://www.cameroononline.org/2012/04/21/rivals-cry-foul-as-german-firms-wins-cameroon-poll-deal/. Date accessed: 15.05.2012

115_ EISA, (2010), p.50, "Voter Registration in Africa: A Comparative Analysis', 'Introduction' by Astrid Evrensel pgs 1-57 available at: http://www.eisa.org.za/PDF/vrafrica.pdf. Date accessed: 15.05.2012

116_ Gyezaho, E., (2011), 'Uganda Fresh Rot Revealed in National ID Deal' from www.allafrica.com, 30th November, available at: http://allafrica.com/stories/201111300145.html. Date accessed: 15.05.2012

117_ MasterCard to Power Nigerian Identity Card Program, MobileMoneyAfrica, May 9 2013, available at: http://mobilemoneyafrica.com/details.php?post_id=1206

118_ Stephen Devereau and Katharine Vincent, "Using technology to deliver social protection: exploring opportunities and risks," 20 Development in Practice 3 (May 2010), 372.

119_ http://www.unglobalpulse.org/projects/BigDataforDevelopment

120_ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2205145

121_ http://www.oecd.org/sti/sci-tech/new-data-for-understanding-the-human-condition.htm

122_ http://www3.weforum.org/docs/WEF_IT_RethinkingPersonalData_Report_2012.pdf

123_ http://www.post2015hlp.org/wp-content/uploads/2013/05/UN-Report.pdf

124_ "Rural medics to get mobile advice 'hotline', SciDevNet, 7 July 2009, available at: http://www.scidev.net/global/health/news/rural-medics-to-get-mobile-advice-hotline-.html

125_ Donald G. McNeil Jr, 'Haidi: Cellphone Tracking Helps Groups Set Up More Effective Aid Distribution, Study Says', New York Times, 5 September 2011, available at: http://www.nytimes.com/2011/09/06/health/06global.html?_r=0

126_ Patrick Meier, 'Crisis Maps: Harnessing the Power of Big Data to Deliver Humanitarian Assistance,' Forbes, 2 May 2013, available at: http://www.forbes.com/sites/skollworldforum/2013/05/02/crisis-maps-harnessing-the-power-of-big-data-to-deliver-humanitarian-assistance/

127_ Francesco Mancini (ed), New Technology and the Prevention of Violence and Conflict, International Peace Institute, April 2013, p.16.

128_ Hibah Hussein, Dialing Down Risks: Mobile Privacy and Information Security in Global Development Projects, New America Foundation, August 2013. This report provides a detailed summary of the various risks associated with employing mobile technologies in development operations.

129_ Patient Privacy in a Mobile World: A Framework to Address Privacy Law Issues in Mobile Health, TrustLaw, June 2013, available at: http://www.mhealthalliance.org/images/content/trustlaw_connect_report.pdf

130_ Nicholas D. Lane, Junyuan Xie, Thomas Moscriboda, and Feng Zhao, 'On the Feasibility of User D-Anonymisation from Shared Mobile Sensor Data,' PhoneSense'12, November 6, 2012, available at: http://niclane.org/pubs/lane_phonesense.pdf; Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation,' UCLA Law Review, Vol 57, p.1701, 2010, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006

131_ OCHA, Humanitarianism in a Networked Age, p.40, available at: https://docs.unocha.org/sites/dms/Documents/WEB%20Humanitarianism%20in%20the%20Network%20Age%20vF%20single.pdf

132_ Mohamed Hossam Ahmed, 'Threats to Mobile Phone Users' Privacy', a report funded by the Office of the Privacy Commissioner oF Canada, March 2009, available at: http://www.engr.mun.ca/~mhahmed/privacy/mobile_phone_privacy_report.pdf

133_ Humanitarianism in a Networked Age, p.40.

134_ David Talbot, 'Big Data from cheap phones', MIT Technology Review, April 23, 2013, available at: http://www.technologyreview.com/featuredstory/513721/big-data-from-cheap-phones/

135_ Steve Song, 'The Open Data Cart and Twin Horses of Accountability and Innovation', June 19 2013, blogpost available at: http://manypossibilities.net/2013/06/the-open-data-cart-and-twin-horses-of-accountability-and-innovation/

136_ Linnet Taylor, 'From food crisis to nutrition: challenges and possibilities in Ethiopia's nutrition sector,' Institute of Development Studies, February 2012.

137_ See, for example, Department for International Development, Ministry of Defence and Foreign Commonwealth Office, undated, 'GCPP SSR Strategy 2004-2005', DFID, Ministry of Defence and Foreign and Commonwealth Office, London.

138_ USAID, 'A Field Guide for USAID Democracy and Governance Officers: Assistance to civilian law enforcement in developing countries', January 2011.

139_ Interpol provides international police training and capacity building. See: http://www.interpol.int/@en/INTERPOL-expertise/Training-and-capacity-building

140_ DFID's Nepal Police Modernisation Programme, available at: http://projects.dfid.gov.uk/project.aspx?Project=201167

141_ DFID's Security Sector Accountability & Police Programme in the DRC, available at: http://projects.dfid.gov.uk/project.aspx?Project=113961

142_ DFID Safety and Access to Justice Programme in Sudan, available at: http://projects.dfid.gov.uk/project.aspx?Project=113400

143_ ‘Bolivia to secure borders with biometrics, using Cuban aid’, Stephen Mayhew, Biometric Update, October 30 2012, available at: http://www.biometricupdate.com/201210/bolivia-to-secure-borders-with-biometrics-using-cuban-aid/

144_ ‘Ghana set for e-visa, border management system’, Ghana Business News, 8 April 2013, available at: http://www.ghanabusinessnews.com/2013/04/08/ghana-set-for-e-visa-border-management-system/

145_ For more information see: http://ec.europa.eu/anti-trafficking/entity.action?path=EU%20Projects/DCI_MIGR_2010_224_349

146_ ‘US and Maldives Enhance Cooperation with Border Security Program’, March 28, 2013, US Virtual Presence Post, available at: http://maldives.usvpp.gov/pr-28march2013.html

147_ ‘Status of Funding, Equipment and Training for the Caribbean Basin Security Initiative’, US Government Accountability Office, 18 April 2013, available at: http://www.gao.gov/assets/660/653909.txt

148_ ‘Status of Funding, Equipment and Training for the Caribbean Basin Security Initiative’, US Government Accountability Office, 18 April 2013, available at: http://www.gao.gov/assets/660/653909.txt

149_ ‘Fact Sheet: EU Border Assistance Mission (EUBAM) in Libya’, Common Security and Defence Policy, http://www.eeas.europa.eu/csdp/missions_operations/eubam-libya/eubam_factsheet_en.pdf

150_ ‘Green light for civilian mission to support border security in Libya’, Council of the European Union, May 22, 2013, 9478/13 Presse 189, available at: http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/EN/foraff/137189.pdf

151_ ‘Millions of euros for new police databases in West Africa’, Statewatch, March 7 2013, available at: http://www.statewatch.org/news/2013/mar/02eu-wapis.htm

152_ ‘The Politics of Surveillance: The Erosion of Privacy in Latin America’, Katitza Rodriguez, EFF, available at: https://www.eff.org/deeplinks/2011/07/politics-surveillance-erosion-privacy-latin-america

153_ ‘U.S. Providing Iraq With Phone, SMS Monitoring Devices’, Radio Free Europe, August 21, 2011, available at: http://www.rferl.org/content/us_providing_iraq_with_phone_and_sms_monitoring_devices/24303623.html

154_ Business Case for Governance and Peace-building in Somalia 2012–2015, available at: http://projects.dfid.gov.uk/project.aspx?Project=201462

155_ See the ‘Surveillance Who’s Who’, available at: http://bigbrotherinc.org/v1/

156_ ‘US to provide Maldives with cost-free border control system’, Neil Merrett, Minivan News, March 28 2013 http://minivannews.com/society/us-to-provide-maldives-with-cost-free-border-control-system-55343

157_ c.f. ‘ECJ To Rule On The Biometric Passports’, European Digital Rights, October 10 2012, available at: http://www.edri.org/edrigram/number10.19/ecj-rule-biometric-passports

Written by Gus Hosein and Carly Nyst

www.privacyinternational.org
Register Charity No. 1147471

Design by Paul Belford Ltd.

October 2013

www.privacyinternational.org
Twitter @privacyint

Registered Charity No. 1147471