BETTER ASSISTANCE IN CRISES RESEARCH

UKaid
from the British people

Risks, accountability and technology thematic working paper

Becky Faith, Tony Roberts and Kevin Hernandez

BASIC Research

February 2022

Implemented by

institute of development studies

UNIVERSITY OF SUSSEX

CIDT Centre for International Development and Training

Better Assistance in Crises (BASIC) Research (funded by UKAid) aims to inform policy and programming on how to help poor and vulnerable people cope better with crises and meet their basic needs through more effective social assistance. All costs related to BASIC Research are covered by the UK Foreign, Commonwealth and Development Office.

Summary

Aid agencies, governments, and donors are expanding investment in digitisation of their beneficiary identification and registration systems, and remote and algorithmic control of humanitarian and social protection programmes. They are doing so in ways that may facilitate the move from humanitarian assistance to government provision, and facilitate the delivery of shock-responsive social protection.

This paper looks at evidence on the role of digital technologies in the nexus between humanitarian and social assistance, assessing their benefits and risks. We conclude with an exploration of emergent research themes, recommendations for future research in this area, and links with the broader Better Assistance in Crises (BASIC) Research programme themes.

About the authors

Dr Becky Faith is a Research Fellow and leads the Digital and Technology Research Cluster at the Institute of Development Studies (IDS), University of Sussex. She has 15 years of strategic and programme experience working in information and communications technology for development (ICT4D) and technology for human rights organisations. Becky's PhD focused on the use of mobile phones by young women. She is an international expert in research and strategy on the use of mobile phones in marginalised communities.

Dr Tony Roberts is a Research Fellow in the Digital and Technology Research Cluster at IDS. He has been working at the intersection of digital technologies, international development, and social justice since 1988. Tony founded and directed two international development agencies. He led Coda International and then Computer Aid International for a decade each. Tony then consolidated almost 25 years of field experience and learning about digital development in doctoral research with women using participatory video in Zambia.

Kevin Hernandez is a Research Officer at IDS. After completing an MA in Globalisation, Business and Development at IDS, Kevin now works with the Digital and Technology Research Cluster on various projects, including: the impact of digital technology on economic growth, productivity, employment, and equality; the use of real-time data for decision-making in the development sector; frontier technologies for development; and the use of predictive analytics in humanitarian action.

Contents

1. Introduction

The key research question underpinning BASIC Research is: 'how and at what costs can social assistance be delivered routinely in difficult, fragile and conflict-affected contexts?' The programme seeks to explore how, in crisis-affected contexts, it might be possible or desirable to move from humanitarian assistance to government-led social assistance. It also explores how social protection systems could be more responsive to crises and conflict, and be more climate-sensitive. In the project's Risks, Accountability and Technology thematic area, we look at the benefits and challenges of the digitisation of key elements of social assistance systems, including in processes of accountability and due diligence.

It is argued that a smooth transition from social assistance provided by humanitarian actors to ongoing social protection delivered by governments could be facilitated by more integration and interoperability of their information systems. Aid agencies, governments, and donors are expanding investment in the digitisation of their beneficiary identification and registration systems, as well as the remote and algorithmic control of humanitarian and social protection programmes in ways that may facilitate this move towards government provision, and facilitate the delivery of shock-responsive social protection.

However, there have been concerns in recent years that the digitisation of humanitarian action, which involves working with private sector technology companies, 'invites a potentially adverse combination of commercial incentives, ethical standards and operational priorities into the fragile environments of humanitarian response' (Sandvik, Jacobsen and McDonald 2017: 4). This 'adverse combination' may risk violating the humanitarian principle of ensuring that 'people are not put at risk as a result of the way that humanitarian actors record and share information' (Sphere Association 2018).

This concern reflects the issue that while these technologies introduce new possibilities for accountability and efficiency, they also bring risks of exclusions and violations of the rights of already vulnerable groups. These risks are widely acknowledged within the sector, and humanitarian actors have initiated a range of initiatives aimed at achieving the ethical use of data-driven technologies (e.g. Belina *et al*. 2020; Kuner and Marelli 2017; OCHA Centre for Humanitarian Data 2019). However, in the social protection sector, an International Labour Organization (ILO) report suggests that:

> [These] social protection programmes have expanded in low and middle-income countries without serious considerations of beneficiaries' privacy and data protection, even when these should have been a critical concern under those countries' international human rights obligations or national data protection laws.
> (Carmona 2018: 16)

While there have always been many private sector companies working in humanitarian contexts performing a range of operations, it has been recognised for some time now that digital technologies introduce a new set of challenges. Sandvik *et al*. (2014) outlined a critical research agenda for technology in humanitarian contexts, which showed how new technologies offered possibilities to better uphold the humanitarian principles of humanity, impartiality, and neutrality, but there was an urgent need to look at the impacts of technology on the distribution of resources and the definition of relationships, and how data collection creates new vulnerabilities.

The rapid adoption of often untested technologies in the absence of regulation and by unaccountable actors has highlighted these risks, as the controversial partnership between the World Food Programme (WFP) and the data analytics company Palantir demonstrates. This partnership raised major concerns about the threats from combining and merging huge data sets of sensitive personal information on vulnerable populations. In an open letter, humanitarian and human rights actors argued (ResponsibleData.io 2019) that this partnership risked undermining WFP's commitment to upholding the Principles for Digital Development. These Principles have been endorsed by governments, non-governmental organisations (NGOs) and United Nations (UN) organisations and include a commitment to responsible practices for organisations collecting and using individual data, which include considering the sensitivities around the data that has been collected, being transparent about how data will be collected and used, and minimising the amount of personal identifiable and sensitive information collected (Principles for Digital Development 2021).

2. Methodology

The paper does not aim to cover all technologies associated with the delivery of humanitarian aid and social assistance, and does not go into any depth about the technical aspects, which are covered effectively in the Social Protection Approaches to COVID-19 – Expert advice helpline (SPACE) report, *Linking Humanitarian and Social Protection Information Systems in the Covid-19 Response and Beyond* (Schoemaker 2020) and the technical paper by the United Kingdom (UK) Department for International Development (DFID) and Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) on *Building an Integrated and Digital Social Protection Information System* (Barca and Chirchir 2019). It should be noted that we focus on the role of large humanitarian organisations and the UN, since these entities dominate the delivery of cash assistance and the existing literature (CaLP 2020). How local and national state and non-state actors approach the risks and benefits of digitisation in social assistance programming during crises is a gap that future BASIC research will address.

We conducted a literature review of existing evidence on the role of digital technologies in delivering social assistance through government systems and in the humanitarian sphere, drawing on our recent work, *Digital Aid: Understanding the Digital Challenges Facing Humanitarian Assistance*, for the Global Challenges Research Fund (GCRF) (Roberts and Faith 2021) and our work for DFID on *Predictive Analytics in Humanitarian Action* (Hernandez and Roberts 2020). For this study we looked at academic literature from a range of disciplines, including development studies, humanitarian and legal studies, and information and communications technology (ICT) for development, as well as grey literature such as reports and blogs from humanitarian actors, donors, and civil society organisations (CSOs).

In this paper, we assess the potential benefits and risks of the overall use of digital technologies before exploring the key issues relating to the move from humanitarian assistance to government-led social assistance, and how social protection systems can be more crisis- and conflict-sensitive, and more climate-sensitive. It should be noted that overall, there is more literature on the potential exclusionary risks of digitisation in humanitarian and crisis contexts, particularly around the responsible use of data, than in nationally led social protection systems. We then look at four clusters of technologies being introduced at the nexus, with an example of implementation, an overview of the claims made, the risks and gaps in existing research (biometric identification, digital registration, artificial intelligence), and remote monitoring technologies. We identify gaps and areas where further research is necessary.

The paper concludes with an exploration of emergent research themes, proposing recommendations for future research in this area, and links with the broader BASIC Research programme themes.

3. The impacts of digitisation

This section explores the overall impact of digitisation in social protection and humanitarian assistance. It covers the risks and benefits, the impact on exclusion, and strategies used across governments and the humanitarian sector to address these potential harms.

The desire to integrate digitisation is by no means a new trend in the delivery of humanitarian aid; a blog from 2012 already identified 25 programmes using e-payment systems in 11 countries (Smith 2012). The digitisation of social protection systems has a longer history, particularly in European countries where the creation of databases and the monitoring of citizens has long been a fundamental part of assessing population needs (Dencik and Kaun 2020). However, along with many other sectors, the Covid-19 pandemic has dramatically accelerated this trend. The digitisation and 'datafication' of humanitarian assistance and social protection systems is now mainstream, with datafication being understood as the 'transformation of social action into online quantified data, thus allowing for real-time tracking and predictive analysis' (Van Dijck 2014: 198). Donors such as the UK Foreign, Commonwealth & Development Office (FCDO) and GIZ recognise that the digitisation of processes such as data collection and processing can reduce error, simplify, and speed up processes. Yet they also recognise that these systems can lead to systematic exclusion and automated profiling (Barca and Chirchir 2019).

3.1 Benefits

As with other sectors, digitised systems can reduce transaction costs, enable real-time analysis, and deliver affordances of scale and efficiency for humanitarian actors and governments. These include the ability to serve communities in hard-to-reach areas through electronic cash transfers using 'remote' programming, which reduces travel and waiting times (ICRC 2020), and streamlines aid and service delivery. For example, following the 2015 earthquake in Nepal, international aid agencies worked with the Department of Civil Registration to use Short Message Service (SMS) to transfer cash and food vouchers to those in need, reaching a record 11,000 cases in four hours (Handayani *et al*. 2017).

Digital payments have already mitigated some of the perceived risks of cash and voucher assistance (CVA): evaluations have shown that programmes using digital payments have reduced theft, reduced risks to staff in transporting money, and proved popular with recipients due to the privacy they afford (Burton 2020). The use of predictive analytics for targeting of CVA payments offers the potential for quicker, cheaper, and more efficient enrolment, verification, and delivery of cash at scale (Raftree and Kondakhchyan 2021a).

More broadly, it is argued that digital financial infrastructures offer greater benefits for governments by strengthening overall public financial management systems, reducing the size of shadow economies and thus opportunities for tax evasion (Cangiano, Gelb and Goodwin-Groen 2019). This is in line with broader G20 High-Level Principles for Digital Financial Inclusion, which encourage both the for-profit and the non-profit sector to make large-volume, recurrent payments such as CVA digitally rather than in cash (Global Partnership for Financial Inclusion 2016).

3.2 Risks

A recent report by the Office for the Coordination of Humanitarian Affairs (OCHA), *From Digital Promise to Frontline Practice*, warns of 'technology literacy' gaps in the humanitarian sector (OCHA 2021). Research by the Institute of Development Studies (IDS) flags how the use of digital technologies and pressure to innovate can be in tension with the precautionary principle (Hernandez and Roberts 2020), arguing that the voices and interests of affected populations must remain central.

Technological choices and systems are deeply political. As Goodman *et al*. (2020: 7) note in the BASIC paper on identification and registration systems in protracted and recurrent crises, '…donor-funded systems can entrench or exacerbate existing power imbalances, or can reduce these while increasing protection of rights to privacy and data protection'. As part of a transition to government-led social protection, Goodman *et al*. caution against sharing humanitarian data with governments that may present risks to affected populations. Instead, they propose principles of 'privacy by design' to protect privacy rights. While these are laudable aims, a paper on the challenges of harmonising cash frameworks in Somalia illustrates the real-world challenges. The author of that study notes key issues such as Somalia's lack of a national legal framework for data protection and digital security threats from Al-Shabaab (Owino 2020). In addition, it illustrates the very real dangers of poor digital security in these contexts where recipients can be targeted for violence or harassment if data are leaked to Al-Shabaab. In countries experiencing conflict, such as South Sudan, mobile data collection might be suspect or even forbidden by government (Raftree and Kondakhchyan 2021a).

Data protection is a key risk of digitised systems. When people provide personal information to humanitarian agencies in order to access social assistance, they do not renounce their rights to privacy, data security, and protection from harm. In an International Labour Organization (ILO) paper on social protection and biometrics, Carmona (2018) argues that there is a 'lack of comprehensive discussion about privacy and data protection among social protection practitioners contrasts sharply with increasing attention humanitarian practitioners lend the issue'.

Further research is also needed to understand the digital privacy issues in contexts such as Tigray (Ethiopia) or Myanmar, where governments are both providing social assistance and responsible for large-scale human rights violations. Beyond this, it would be valuable to understand the issues for people living in areas controlled by non-state armed groups, particularly those designated as terrorists, and what that means for how they are reached digitally. This speaks to the issue of invisibility in digital systems as a desirable state for those with unsettled migration status. Research by Privacy International shows how aid funds are being used

to fund a $30m biometric identity system in West Africa, which is to be used to assist in the identification of Ivorians irregularly residing in Europe and to organise their return more easily (Privacy International 2020).

3.3 Addressing harms and building capacity

The humanitarian sector is not lacking in initiatives aimed at reducing the potential harms of digitisation. This includes the recently updated handbook by the International Committee of the Red Cross (ICRC) on data protection in humanitarian action (Kuner and Marelli 2020), which aims to assist in the integration of data protection principles and rights in the humanitarian environment. The recommendations and guidelines contained in the handbook are based on key international instruments, and provide recommended minimum standards for the processing of personal data.

In the broader cash assistance field, the Cash Learning Partnership (CaLP) recently released a *Data Responsibility Toolkit* for CVA practitioners offering a range of ways to integrate data responsibility into programme planning, design, implementation, monitoring, evaluation, accountability, and learning activities. The toolkit offers a 'gold standard' to which organisations should aspire and identifies both legal and ethical implications that we should be mindful of in our treatment of data (Raftree and Kondakhchyan 2021b). While these are all laudable initiatives, there is a lack of research about how this guidance is being applied in practice. An interview with a former official from the UN Refugee Agency (UNHCR) on the risks arising from the Taliban's rise to power in Afghanistan suggests a lack of engagement with these risks. He reflected that a data protection risk assessment should have been carried out before the instigation of a cash programme, adding '…but we know from experience that no humanitarian agency does these impact assessments' (Loy 2021).

CaLP's *State of the World's Cash 2020* report recognised that there is increasing emphasis on digital identity provision and management as a critical enabler of access to aid and broader financial services, but that this has also given rise to 'new capacity gaps in relation to technology, data systems and digitisation of CVA' (CaLP 2020). In the social protection field, the ILO emphasises that recipients are protected by the privacy and data protection rights enshrined in international and national standards, emphasising that:

> Individuals do not waive their rights to privacy and data protection by becoming beneficiaries of social protection programmes. Beneficiaries of non-contributory programmes have rights related to their personal data that limit authorities' discretion regarding how government security bodies, tax authorities or private companies can access such data and how it is used.
> (Carmona 2018: 12)

Box 3.1: Research gaps

Informed consent: Can vulnerable populations in crisis contexts give meaningful informed consent about handing over sensitive personal data to humanitarian agencies when they perceive it to be a requirement of accessing assistance and protection?

Sharing humanitarian data with states: Given that governments have varying records on human rights and that the complexion of governments regularly changes, is the transfer of personal data by humanitarian agencies to states compatible with the precautionary principle, wider humanitarian principles, and data protection principles?

3.4 Inclusion and exclusion

Any discussion of digitisation must highlight the risks arising from unequal access to technologies and the skills to make effective use of them, as highlighted in IDS's previous work for DFID, *Leaving No One Behind in a Digital World* (Hernandez and Roberts 2018). These inequalities of access exist both between countries and within countries, and between humanitarian agencies and government departments. Digital inequalities risk leaving the most vulnerable people behind; this includes people without access to or unable to afford connectivity, while others may choose to self-exclude.

In their work on the digitisation of social protection during Covid-19, Gelb and Mukherjee (2020) show how the most vulnerable can be excluded by a digital divide, not only in that some people will lack access to mobile devices but that some will lack the digital skills to use those devices to apply for assistance. This was the case in a Save the Children study of mobile money in several regions of Somalia, where, despite mobile usage being high, this did not necessarily translate into knowledge about how to use mobile money, including how to manage account functions (Radice and Hussein 2017). The study also showed how women were less likely to have control over a phone. Sharing devices with others limits their autonomy and freedom on use of money. The gender and disability digital divides are often more acute for refugees (GSMA 2019). This is partly caused by limited livelihood opportunities; poverty means that refugee women and people with disabilities are less able to use mobile phones (*ibid*.). A recent World Bank study on women's inclusion in digital cash transfers during Covid-19 (Zimmerman *et al*. 2020) shows that even where programmes are targeting women, the risks of exclusion are significant. Citing an assessment of women's experiences of cash transfer programmes in India, Pakistan, and Tanzania, the study shows that women are often unaware of their benefit entitlements, the timing of disbursements, what money is available in their accounts, and how to use the accounts.

Older people are also at risk of exclusion as they often have lower levels of digital literacy and less access to the internet and mobile phones. A study on social protection for older people during Covid by HelpAge International shows that older people do not know how to register for the new Covid-19 cash transfers as most of the information is only available online (Juergens and Galvani 2021). BRAC's work distributing cash during the Covid-19 pandemic highlights another exclusionary risk in digitisation – that of unequal coverage. People in rural areas are less likely to have access to mobile money agents, and this has been exacerbated by Covid-19 social distancing measures in Bangladesh (Tasnin 2020). This was also the case in rural/remote settings in Somaliland, where mobile money distribution during the humanitarian cash-based response was challenged by poor signal in some remote areas (Daniels and Anderson 2018).

Unequal access to digital technologies often reflects, reproduces, and augments existing social and economic inequalities along intersecting dimensions of (dis)advantage (Hernandez and Roberts 2018). Economically marginalised communities, especially rural women living in the most remote settings, are often hampered by multiple barriers of digital access, including cellular availability, device and data affordability, and by low levels of awareness, literacies, and agency. As the BASIC paper on Exclusion demonstrates (Rohwerder and Szyp 2022), there are additional accessibility barriers for people living with disabilities (Robinson, Marella and Logam 2020); research by the Office for the High Commissioner for Human Rights (OHCHR) also shows that marginalised ethnic minority groups do not have equal access to digital connectivity or devices, placing them at a disadvantage when social assistance relies on digital methods (OHCHR 2020).

It is important to acknowledge both that the use of digital technologies can deliver clear benefits to those with good levels of connectivity, device ownership, and digital literacies (World Bank 2016), and that digital technologies were not the cause of the original inequalities, which were pre-existing. However, because digital technologies, literacies, and agency are unevenly distributed, social assistance that relies on digital methods unintentionally adds new dimensions to pre-existing inequalities. The use of digital technologies provides new advantages to those already privileged in terms of their device access, literacies, and agency, as well as relative disadvantages for those who are already under-privileged due to the unaffordability or inaccessibility of digital access (Hernandez and Roberts 2018).

The digitising of identity systems offers both benefits and the potential for exclusionary risks. Some argue that the very technological affordances (or action possibilities) and design of these systems will exclude some members of society. Privacy International (2021) argues that 'By virtue of their design, these systems inevitably exclude certain population groups from obtaining an ID and hence from accessing essential resources to which they are entitled'. It cites the example of an unconditional cash transfer programme in Kenya targeting ultra-poor households with orphaned and vulnerable children that struggled to reach child-headed households because ID cards are only issued at the age of 18, except when *ad hoc* individual adjustments are made to the distribution system. However, a recent article argued for a less 'totalising' view of digital ID practices, which recognises how identification can confer important rights and protections: 'Data subjects may accept new identity systems for complex reasons, ranging from recognition and belonging to efficiency and convenience' (Weitzberg *et al*. 2021: 3).

Further exclusionary risks lie in the use of automated systems for the automated profiling of individuals and households. These have been widely explored in the literature, looking at the implementation of these systems in Europe and the United States (Dencik and Kaun 2020; Eubanks 2018). In her work for the Australian Department of Foreign Affairs and Trade (DFAT), looking at integrating data and information management for social protection, Barca warns of the particular risks in 'contexts where registration and the assessment of needs and conditions is integrated across programmes and diverse regions, generating the risk of multiple and systematic exclusion across all social sector schemes' (2017: 44).

4. Humanitarian and state-led systems

This section reviews the literature on digital in the humanitarian–social protection nexus and assesses the challenges involved in moving from humanitarian assistance to state-led systems of social protection, and in making state-led systems more shock- and conflict-sensitive, and more climate-responsive. There are lots of continuities in the digitisation of the two scenarios of government and humanitarian cash assistance, often coming back to the simple questions of: 'Who asked for this system?' 'Who benefits?' and 'What interests are being served?' In many instances the answers to these questions are that the benefits of control, scale, cost, and time efficiency are enjoyed by the humanitarian agency, private company, or government. As a recent paper on humanitarian data governance argued, 'while technology platforms offer a range of exciting opportunities, they struggle to manage the kind of political and social complexity that are endemic to humanitarian response – especially around managing politically contested space, neutrality, and protecting human rights' (McDonald 2019: 2).

It should also be noted that the transition to national social protection systems is not a linear, one-way progression from humanitarian assistance. In some contexts, there are systems in place prior to a crisis; in others, there are non-existent or nascent systems; and in others still, systems may operate in one part of a country but not in the crisis-affected region. For example, in Yemen, the Social Welfare Fund (SWF) and the Social Fund for Development (SFD) existed prior to the conflict, but there are now three separate channels, including one run by WFP (Goodman *et al*. 2019a).

4.1 The transition from humanitarian to state-led social protection systems

Digital systems are commonly cited as key enablers – or inhibitors – in the transition from humanitarian to longer-term, state-led social protection systems (Barca and Beazley 2019). A recent SPACE report, *Linking Humanitarian and Social Protection Information Systems in the Covid-19 Response and Beyond* (Schoemaker 2020: 10), warned of the dangers of failures to coordinate with the broader social protection and government visions, resulting in '...a piecemeal approach that builds standalone, discrete systems that lack the wider components required to establish a digital ecosystem capable of supporting dynamic and responsive social welfare systems'. The report advocates for an ecosystem approach, which includes steps to strengthen regulatory frameworks such as data protection legislation and strengthening human capacity to implement these frameworks. Both the SPACE report and a DFID/GIZ technical paper, *Building an Integrated and Digital Social Protection Information System* (Barca and Chirchir 2019), outline the elements required for the creation of digital and integrated information systems to underpin the transition from humanitarian to longer-term, state-led social protection systems. Neither paper underplays the risks and challenges involved in these processes, particularly in relation to inclusion and data minimisation. This is a key aspect of data protection, which is defined in the ICRC *Handbook on Data Protection in Humanitarian Action* as seeking '…to ensure that only the minimum amount of Personal Data are processed to achieve the objective and purposes for which the data were collected' (Kuner and Marelli 2020: 38).

There is a welcome focus in both reports on the risks from removing human elements from decision-making by digitising data collection and automated decision-making. These risks are outlined in detail in section 5.3.1. and include augmenting and automating inequalities contained within historical data, as well as the accountability problems inherent in the fact that algorithms are 'black-boxed' and not subject to scrutiny by those who are affected by their use. These risks are not unique to developing country or crisis contexts; they are seen in digitised welfare states around the world, leading the UN Special Rapporteur on extreme poverty and human rights to warn of 'the grave risk of stumbling, zombie-like, into a digital welfare dystopia' (Alston 2019: 2).

Key resources in understanding the implications of the shift from humanitarian to social protection systems in crisis contexts include Schoemaker (2020) and the accompanying BASIC Technical Assistance Services paper on identification and registration systems in protracted and recurrent crises (Goodman *et al*. 2020). Both reports outline the steps required for sharing data and technologies to enable the transition to state assistance, including issues such as pushing for greater interoperability within and beyond the humanitarian sector. The particular enablers for integrated digital social protection systems are outlined by Barca and Chirchir (2019). They include political will, long-term financial support, and what they describe as 'brainware' or the necessary human resources to support these programmes. This includes people who can bridge both the information technology (IT) understanding required and sectoral knowledge of social protection systems, who are (arguably) a rare and expensive commodity.

While these reports outline the enablers for this shift to happen effectively, the realities of the process and the challenges for governments are illustrated by a recently released internal audit of WFP's supply of digital assistance services as part of its overall engagement with governments. The audit looked at this process in Iraq, Namibia, and Nigeria, and found that 'country ownership and sustainability, and critical elements to ensure data protection and privacy, were noted to be missing from the three sampled projects' (Office of the Inspector General WFP 2021: 13).

The role of digital is not always disclosed in programme reports. In some papers that directly address humanitarian assistance and government social protection, the digital is what we might call 'present but invisible'. So, for example, in the BASIC report, *Review of Cash Programming and Linkages to Social Protection in Lebanon* (Smith 2019), the benefits and challenges of linking with social protection systems are discussed without explicit reference to the digitally enabled information systems that underpin them. In Gentilini *et al*.'s (2018) paper on connecting humanitarian assistance and social protection, the authors discuss enablers in case studies such as data gathered by WFP in Liberia for its proprietary beneficiary registration system and a common registry system in Palestine. Finally, in another paper looking at the forced displacement context (Pelly 2020), a digital platform (Kizilaykart) in Turkey has delivered cash assistance to 2.4 million people. Now obviously these are digital systems, requiring a certain level of capacity, bandwidth, cybersecurity, and all the other factors that we know are all enablers of effective digital service delivery, but they are largely discussed without reference to these issues.

Finally, a critical issue with the literature and guidance on shock-responsive social protection – and more broadly with the literature on the humanitarian–development nexus – is the assumption of an unproblematic transition from conflict to peace and to governments that donors can support. This does not account for the setbacks that inevitably occur. This was apparent in South Sudan in 2013, and is now coming into painfully sharp relief with the Taliban takeover of Afghanistan in September 2021. With the takeover, it is possible that large amounts of data collected by agencies over the past 20 years will end up in the hands of the Taliban, leading one expert formerly employed by UNHCR to comment that 'the Taliban have been given the keys to the server room' (Loy 2021).

Box 4.1: Research gaps

More needs to be done to make the digital 'visible' in studies of humanitarian action and government social assistance to understand the affordances of the technology, and the role of private sector technology companies.

4.2 Crisis, displacement, and climate shocks

The key research question underpinning the BASIC Research programme is how to help poor and vulnerable people cope better with crises and meet their basic needs through more effective social assistance in contexts of protracted crises, displacement, and recurrent climate shocks. Barca and Beazley's (2019) report, *Building on Government Systems for Shock Preparedness and Response: The Role of Social Assistance Data and Information Systems*, is of particular value in this regard. It outlines the value and processes for building on existing data and information systems in enabling more timely responses and supporting targeting. The report emphasises the value of digitised systems in supporting these processes, but it is important to recognise that digital infrastructures themselves are at risk from climate shocks, cyber-attacks, and political threats.

Effectively functioning digital systems rely on stable energy infrastructures, which are increasingly under attack in conflicts, as research on the targeting of civilian infrastructure in the Yemen war demonstrates (Sowers and Weinthal 2021). A World Bank study (Sandhu and Raja 2019) shows how telecommunication infrastructures are vulnerable both from risks related to climate change (such as earthquakes and flooding) and threats from deliberate sabotage (such as divers cutting cables). The same report also outlines how the 'last mile connectivity' that is vital in disaster settings is dependent on energy supply continuity. The report warns that only a limited number of countries are carrying out information and communications technology (ICT) and datacentre-specific climate risk assessments.

Governments and humanitarian organisations are also vulnerable to the same cyber-attacks as any large institutions. In 2019, three UN offices and dozens of UN servers were victims of a cyber-attack that had 'the hallmarks of a sophisticated threat actor' (Parker 2020). IDS research shows that governments across sub-Saharan Africa are also using a range of tactics to control online spaces, including shutdowns, bandwidth throttling (slowing down), bans, and blocking (Roberts *et al*. 2021). The number of intentional internet shutdowns by governments in Africa rose to 25 in 2020, up from 21 in 2019, with Algeria, Ethiopia, and Sudan the worst-affected countries. While these shutdowns are intended to have a political impact, they have unintended consequences in terms of affecting all digitally enabled systems and services. This reinforces the fact that effective transition to government-led, shock-responsive systems will need to be underpinned by secure digital infrastructures, although these infrastructures themselves are vulnerable to shutdowns and closures.

Using digital systems in fragile and conflict-affected environments also poses a particular set of risks, yet there is currently a knowledge gap about the digital threat landscape in conflict environments. An ICRC blog on this issue argued for the need for research on '…how different actors, including parties to the conflict, are making use of technologies, what consequences this may have for affected populations and what are the implications for possible protection response by humanitarian actors are' (van Solinge 2019). OCHA's Data Responsibility Guidelines point out the absence of guidance on data protection related to 'survey results and datasets containing information that could be used to target individuals in conflict areas' (OCHA 2019).

These warnings are echoed in the BASIC Technical Assistance Services paper on ID systems in protracted and recurrent crises, which warns that 'further development of MIS [management information systems] in humanitarian and social protection work in fragile and conflict contexts risks further exclusion, marginalisation and political polarisation by subjecting beneficiaries to significant, unnecessary risk' (Goodman *et al*. 2020: 3). Further risks are identified in that paper, including high levels of insecure data collection practices (such as storing data in unencrypted Excel/Google Sheets), and a significant trend in the use of biometric data without due consideration of the implications. Findings from a BASIC report on linking humanitarian cash and social protection in Yemen (Phase II) shows how these challenges are playing out; UNICEF is using a photo ID card rather than a digital biometric system, as this is thought to offer sufficient levels of accountability (Goodman *et al*. 2019a).

Box 4.2: Research gaps

What are the contextual factors that can threaten digital infrastructures in fragile and conflict-affected states, and how do these affect humanitarian and government-led social assistance?

What is the impact of internet shutdowns on digitised systems for delivery of cash assistance?

5. Tools and technologies

It is beyond the scope of this paper to assess every digital tool used in humanitarian assistance and government social protection systems. Instead, we focus on four clusters of technologies that are used in both humanitarian and government-led social assistance systems:

1. Digital payment systems;
2. Digital registration and identity;
3. Artificial intelligence and predictive analytics;
4. Remote monitoring and accountability systems.

Each section is structured as follows: we start by describing the functionality of the technology and its relevance for both humanitarian and government-led social protection. We then explore examples of how each technology is implemented, the risks associated with it, and the research gaps. The key benefits and risks are also summarised in Table 5.1.

Table 5.1: Risks and benefits of key technologies

Technology	Benefits	Risks
Digital payment systems	Scale and efficiency. Reach communities in remote or conflict-affected areas instantly. Reduce security risks for donors and recipients.	Reaching new beneficiaries requires creating new payment mechanisms /adapting existing ones. Challenging in cash-reliant contexts with poor infrastructure. Data protection challenges.
Digital registration and identity	Reduce enrolment times, travel and waiting times for affected populations. Address fraud and corruption. Speed up process of delivery assistance.	Use of existing biometric data for unintended purposes. Some groups such as manual workers have faint fingerprints.
Artificial intelligence and predictive analytics	Enable data-driven decision-making to improve targeting of social assistance. Improve readiness for future disasters.	Replaces human deliberation and dialogue with automated algorithmic decision-making processes that can augment existing inequalities in data and cannot be scrutinised by affected populations. Challenges for transparency and accountability in decision-making.
Remote monitoring and accountability	Contribute to rapid and near real-time monitoring and accountability. Provide different types of data to assess programming. Allow for more systematic tracking of indicators.	Governance relationships transformed by social and political processes, not technologies. Currently not used for upstream leakage and corruption.

Source: Authors' own.

5.1 Digital payment systems

Box 5.1: Digital payment systems

Function:

Direct cash payments to affected populations through a range of digital means: mobile money, e-cards redeemable for goods at specific shops, and cardless transactions using one-time personal identification numbers (PINs).

Claims/impact:

Scale and efficiency;

Reach communities in remote or conflict-affected areas instantly;

Reduce security risks for donors and recipients.

It is now widely acknowledged that transferring cash directly to individuals can be faster, safer, easier, and cheaper to achieve on a large scale using digital rather than alternative analogue methods. From 2015 to 2019, the number of countries with UNHCR cash programmes increased, such that more than 20 million people were receiving cash assistance, 35 per cent of it digital cash (Landa 2020). In 2019, CVA worth $5.6bn was programmed, constituting 17.9 per cent of total international humanitarian assistance (CaLP 2020). There is evidence that these mechanisms lower the security risks for donors and recipients, such as reducing the need for warehouses; it is also a less 'visible' form of aid, which can reduce stigma (ICRC 2020). There has been a rapid acceleration of this trend during the Covid-19 pandemic (Aneja and DuBois 2020). In their paper for the SPACE programme looking at rapid cash support during Covid-19, Beazley, Barca and Derban (2020) analyse the pros and cons of different mechanisms in detail. This is supported by a Strategy Decision Matrix, a Delivery System Decision Matrix, and a similar tool to assess registration/enrolment options.

CaLP's report on mobile money in Somaliland – where mobile money made up 10–15 per cent of CVA beneficiaries (with vouchers and smartcards making up the rest) – captures some of the key risks and benefits of these programmes (CaLP 2019). In a context where 78 per cent of the adult population has access to mobile money, the system has the potential to go to scale, but there have also been disadvantages such as a lack of verification of beneficiaries and traceability of use, weak regulation, and coverage issues in rural/remote areas. The CaLP report on Iraq (Savage 2021) shows that while mobile money has been largely effective for delivery of humanitarian programmes, some limitations have emerged. For example, there is limited capacity to oversee the vendors that the system relies on, with complaints about the practices employed by some vendors, such as forcing clients to withdraw the entire value of the mobile money account through aggressive means. The report also highlights the exclusionary risks of these systems, since many vulnerable Iraqis do not engage with the formal banking system, and even fewer engage with mobile money. Refugees are excluded from formal financial services as they lack national ID cards and refugee status alone is not sufficient to gain access to a bank account or mobile money.

Restricted smartcards that can be used at specific shops are used in Lebanon (Bailey and Harvey 2017) using a card system established with the Banque Libano-Française (BLF). While restricted mobile money was used by WFP in the Kalobeyei settlement in Kenya (Sterck *et al*. 2020), this could only be used to buy food in participating stores and could not be used to purchase alcohol. WFP is currently diversifying cash-based transfer payment instruments – including mobile money and PINs to be used at automated teller machines (ATMs) without the need to open a bank account – in Colombia, Dominican Republic, and Peru (WFP 2020).

This wide range of mechanisms and tools available suggests that mechanisms and tools should fit contextual specificities, which may require organisations or governments to apply different mechanisms or tools in different areas of the same country. These contextual specificities also reflect the fact that in crisis-affected environments, there might well be humanitarian and social protection systems operating at the same time.

For example, the Phase 1 report of the BASIC Technical Programme in Yemen showed a strong preference for pure cash transfers:

> …mainly because of the flexibility and freedom it grants compared to vouchers and food distribution. Moreover, cash transfers were seen to pose lower costs on beneficiaries than vouchers, as they can be used at all vendors. On the contrary, vouchers are only accepted by designated vendors, with travel being unbearably costly due to the rising fuel prices.
> (Goodman *et al*. 2019b)

There are advantages to using digital cash payments in remote and conflict-affected settings, since handling large amounts of cash can put recipients or humanitarian staff delivering the cash at risk of theft or looting (Burton 2020). However, information and communications systems are often early targets in conflicts. There may be a lack of functioning financial institutions, or they may be linked to conflict actors. In the process of digitisation, it is vital to keep analogue options available, particularly in conflict settings. In its publication on cash transfer programming in armed conflict, the ICRC (2020) discusses how it used three different tools in three different areas of Nigeria based on the contextual peculiarities to achieve the same objective – one of which was a mobile money solution and two of which were not. Their decisions were partly informed by identifying which financial service providers were available and what options they could offer. In some cases, they use only paper vouchers, reflecting that:

> …there are times when data protection concerns mean that electronic cash transfers are not the best type of response, even if all the right financial services are in place. This is particularly common in conflict environments and other sensitive settings, where the choice of financial-services providers is often limited and tends towards control by one particular party to the conflict.
> (Goodman *et al*. 2019b)

5.1.1 Risks

Passing the data generated by humanitarian cash payments to government or private sector actors could conflict with humanitarian and data protection principles. Such data can provide real-time information about a person's location, patterns of behaviour, associations, and affiliations. If the data contain names, inferences can be made about ethnicity and religion. Even if a data set has been anonymised, the mosaic effect means that it can be de-anonymised. The digital nature of the data makes it possible to combine it with other data sets from mobile phone records, electoral rolls, and social media profiles. Even without the detailed contents about transactions, the metadata are sufficient to target abductions, arrests, or air strikes. As General Michael Hayden (former director of the US National Security Agency and the Central Intelligence Agency) publicly stated, 'We kill people based on metadata' (ICRC and Privacy International 2018: 22).

The second edition of the ICRC *Handbook on Data Protection in Humanitarian Action* (Kuner and Marelli 2020) outlines a range of risks associated with the data collected during digital cash transfers and the metadata generated by each transaction. Data are often shared in what the writers describe as 'opaque relationships' with non-humanitarian third parties (such as domestic and international mobile network providers and financial institutions) to comply with a legal obligation or partnership agreement. The technologies used in digital financial transactions also render previously invisible people 'visible' to these financial institutions, introducing new risks, since 'the mere fact that they are seeking assistance from a humanitarian organization can reveal their affiliation with a particular group and expose them to discrimination' (Kuner and Marelli 2020: 147).

The SPACE programme paper (Beazley *et al*. 2020), which looks at both government to person (G2P) transfers and humanitarian cash delivery, recognises that reaching new beneficiaries with digital payment systems is more challenging than reaching existing beneficiaries, since it requires creating new payment mechanisms or adapting/leveraging existing ones. In terms of broader development goals of 'financial inclusion', a review showed that these systems can have limited impact, at least in countries where much of the economy still relies on cash and there is limited formal financial infrastructure and electronic payment

ecosystems. This makes 'electronic payments tedious, insecure and expensive compared to the use of cash' (Gronbach 2020: 28). In these contexts, electronic payments are likely to be 'cashed out' immediately upon receipt.

Box 5.2: Research gaps

Comparative studies across countries: There is some research documenting how digital cash has worked differently within the same country, but insufficient studies comparing experiences across countries. Existing studies show that providing multiple mechanisms for beneficiaries to access money is preferable to providing only one blanket mechanism across a country. It is important to give beneficiaries a choice by offering multiple ways for them to access money so that citizens who are less banked or less connected can still access money. This is the case in most places (Beazley *et al*. 2020; Gronbach 2020).

Conflict and digital: There is also currently only a limited understanding about the digital threat landscape in conflict settings. For example, during a recent CaLP webinar on data protection, a representative from the Yemen Cash Consortium discussed the challenges they faced in collecting data in a country with multiple authorities; and the fact that different authorities demand data as a cost for collaboration. They face constant challenges to assess the 'red lines' of what they are willing to share with these different authorities. The danger is that data are shared with an apparently trustworthy or benign government, which is then replaced by a more repressive government. An ICRC blog stated that 'Stronger knowledge is needed on how different actors, including parties to the conflict, are making use of technologies, what consequences this may have for affected populations and what are the implications for possible protection response by humanitarian actors are' [sic] (van Solinge 2019).

5.2 Digital registration and identity

Box 5.3: Digital registration and identity

Function: Proof of identity and entitlement to assistance.

Claims/impact:

Reduce enrolment times, travel and waiting times for affected populations;

Address fraud and corruption;

Speed up process of delivery assistance.

This section looks at the tools and technologies of systems for identity proofing and authorisation, which are increasingly underpinned by digital identity systems. For some, the idea of interoperability between humanitarian and government identity systems is a holy grail that would facilitate the smooth transition from humanitarian assistance to government-delivered social protection, and would deliver more conflict-sensitive, shock-sensitive and climate-smart social protection. Currently, in crisis settings, affected populations may need to go through multiple registration processes with different agencies to access different humanitarian services and social protection; this may involve travelling to multiple locations and enduring time-consuming processes there, at the end of which the resulting registration may not be valid as proof of identity for the government system.

Digital information systems for social protection are the product of a set of components that work together as a system. A database of records of households and individuals, their socioeconomic situation, and the

benefits they receive is often referred to as a registry. It is important to note that, according to a recent paper by the International Monetary Fund (IMF) (Prady 2020), ID systems do not need to be in place to expand social protection coverage to groups like informal workers; instead, this can be done by building on existing information infrastructures.

These systems have the potential to reduce the transaction costs, waiting times and 'inclusion errors' of humanitarian and government service provision. A good example of this is the Common Cash Facility in Jordan; prior to its implementation, refugees were required to verify their identity directly at the bank to receive cash assistance from agencies, with different banks needing different documentation, which could include a passport or a Ministry of Interior registration card; yet many refugees do not have a passport, and getting an ID card could take up to six months. Even with proper identification, enrolment at the bank could take up to three months due to the large numbers of people enrolling each month (Gilert and Austin 2017).

The second edition of the World Bank's *Principles on Identification for Sustainable Development* (World Bank 2021) describes identification as a 'right, an instrument of protection, and a gateway to access services, benefits, and opportunities' and suggests that 'when designed and used appropriately, identification systems have the potential to help countries accelerate inclusive development'. These principles also warn that poorly implemented or inappropriately used systems can 'disproportionately affect already disadvantaged groups and can be amplified by digital technology'. In a response to these principles, a global coalition of CSOs coordinated by Access Now warns that 'Once deployed, digital identification systems can be powerful tools used for techno-social engineering, censorship, exclusion, discrimination, persecution, targeted deployment of social credit systems, torture, and surveillance – all intended to achieve and/or enhance obedience to authority structures' (Access Now 2020). The coalition recommends that CSOs need to be formally recognised as partners with governments and corporations in designing and implementing digital identification systems.

For some years, humanitarian agencies have been using biometric identification systems that use a person's fingerprints, iris scan, facial recognition, or other unique biological identifier. These systems are also widely used in social protection programmes, although a 2018 ILO report suggests that information on their use is not systematically available. The same report suggests that critical factors for their success, such as reliable access to electricity and strong legal as well as institutional frameworks, are often not available in low-income countries (Carmona 2018). Despite these challenges, some governments have begun to implement national biometric identification for all citizens, such as Huduma Namba in Kenya and the Aadhaar system in India. However, the larger the database, the larger the potential data risk (1.1 billion personal records were leaked in India – see below), while the expansion of data entry agents necessary to complete whole population identification systems introduces 'multiple points of failure' and potential corruption (O Foundation (OFDN) 2021).

Decentralised smartcard systems – where the data are not held centrally by agencies, corporations or governments but instead by each citizen on their own smartcard – may be a means to both increase citizen agency and control over their data and security (Abraham *et al*. 2020).

5.2.1 Risks

The transfer of responsibility for managing the resulting information systems to government will often require infrastructure and technical expertise beyond their current levels, as reflected in the WFP audit of the transfer of their SCOPE system to governments (as discussed earlier) (Office of the Inspector General WFP 2021).

The increasing drive for the adoption of biometric digital IDs poses additional risks for negative impacts and a lack of accountability (Privacy International 2018). The World Economic Forum's *Global Risks Report 2019* reported that the world's largest data breach 'was in India, where the government ID database, Aadhaar, reportedly suffered multiple breaches that potentially compromised the records of all 1.1 billion registered citizens' resulting in criminals selling access to the database (World Economic Forum 2019). There have also been a raft of problems recorded with digital ID systems in Uganda, including exclusion of those people who face challenges in having biometric data collected (such as manual labourers) and data-sharing without consent (Unwanted Witness 2020).

There are a number of digital identification systems risks that relate directly to the drive to migrate humanitarian assistance systems to governments. Humanitarian digital ID can put a strain on agencies that are often faced with demands to share personal data with governments (including from governments that

affected populations may be fleeing from). There is a high risk of data breaches when humanitarian workers are robbed or lose devices or drives containing beneficiary data. Along with data loss, security breaches create a reputational risk for humanitarian organisations (with beneficiaries, local partners, and donors) that are unable to protect data. There is also a risk of misinformation about security breaches (Roberts and Faith 2021). In the context of social protection, an ILO report identifies notable evidence gaps: 'comprehensive independent studies on biometric technology use in social protection programmes are not available; nor are there many accessible studies addressing risks to privacy and data protection' (Carmona 2018: 9). While biometrics, like other digital tools, offer an impression of infallibility, they are notoriously unreliable, with many groups in society – including elderly people, Asian women, manual workers, and workers in the care, health or beauty sectors – reportedly having faint fingerprints (Madianou 2019).

Other issues have been raised about the use of digital ID in humanitarian settings, including: function creep (the use of existing biometric data for unintended purposes); the use of biometric data with national law enforcement, national security, and migration officials; unauthorised access by third parties (e.g. scammers or militias) and the fact that data could be used by third parties to profile and discriminate against individuals (Rahman, Verhaert and Nyst 2018). It was recently revealed that UNHCR collected and shared personal information (including biometric data) from ethnic Rohingya refugees with the Bangladesh government, which then shared it with Myanmar to verify people for possible repatriation, in contravention of UNHCR's own policies (Human Rights Watch 2021).

The BASIC technical assistance report on Yemen, Phase II, shows how these issues play out in other ways that are deeply political (Goodman *et al*. 2019a). WFP insisted that for accountability purposes, it is necessary to record personal biometric data on recipients, but the *de facto* Houthi authority in Sana'a objected to the registration and storage of digital biometric data by WFP on national security grounds, noting that this must be seen against the backdrop of the WFP/Palantir global data management agreement. The report states that an agreement was finally reached by which anonymised biometric data was stored on a server within the National Authority for Management and Coordination of Humanitarian Affairs and Disaster Response (NAMCHA) in Sana'a and would not be made available to WFP or its suppliers. These compromises show the importance of adapting data protection processes to local contexts.

These examples highlight the asymmetric power relations between humanitarian organisations, governments, and affected populations. Agencies require beneficiaries to provide biometric data for systems without understanding the potential implications, and beneficiaries are largely unable to voice their discomfort or interests. By 2018, a report reflecting on Oxfam's two-year self-imposed moratorium on the introduction of biometrics into its programmatic work found that organisations implementing cash transfers were often 'obliged to integrate their programmes with biometrics-based systems of private sector actors involved in the cash transfer value chain' (Rahman *et al*. 2018). The ICRC has decided not to make the provision of biometric data a mandatory condition of service provision.

Box 5.4: Research gaps

Evidence on impact and harms: As the work of the Everyone Counts! programme points out, there is a 'yawning evidence gap on digital ID' (Van Veen and Cioffi 2021), citing examples from their research in Uganda about the risk of significant harms from digital ID. This also extends to concerns about the technical effectiveness of these systems: a 2018 report from Oxfam found that there were 'no quantitative studies or available stats on frequency of false matches in biometrics systems deployed by humanitarian actors' (Rahman *et al*. 2018).

Research with users of the systems: Beyond these empirical gaps, Weitzberg *et al*. (2021) set out a research agenda in digital ID that looks beyond the binaries of 'surveillance and recognition' to examine local exercises of agency and resistance, the role of mediators, and deep research engagement with the users of these systems to understand how they are viewing and interacting with them.

Value for money in procurement relationships with technology companies: The WFP/Palantir relationship is just one example of a high-profile technology company engaging with humanitarian actors. There is a need to look at the role of these companies across the whole landscape of ID systems in social protection.

Social protection systems and digital ID: Research is needed to promote debate and discussion among social protection practitioners about the privacy risks related to the adoption of digital ID.

5.3 Artificial intelligence, algorithmic decision-making, and predictive analytics

Box 5.5: Artificial intelligence, algorithmic decision-making, and predictive analytics

Function: The use of big data to feed machine learning and statistical models to automate decision-making or predict the probable characteristics of humanitarian emergencies.

Claims/impact:

Enables data-driven decision-making to improve humanitarian practices;

Improve readiness for future disasters.

As in other sectors of business and government, there are now significant investments being made to pilot the use of artificial intelligence (AI) in social protection and humanitarian assistance.

According to Siegel (2016: 15), predictive analytics is 'technology that learns from experience to predict the future behaviour of individuals in order to drive better decisions'. This form of AI trains algorithms to recognise patterns found in big data and to use them alongside statistical models to predict the probability of future events. Humanitarian predictive analytics is the use of humanitarian big data to calculate the probable characteristics of humanitarian emergencies (Hernandez and Roberts 2020). The technology is being used to forecast the likely trajectory and characteristics of humanitarian emergencies, including pandemics, famines, natural disasters, and refugee movements. The most commonly predicted features include where and when disasters will unfold, what the defining characteristics of the situation will be, and which populations will be most affected. Predictions are used to inform evacuations and pre-positioning of emergency relief finance, supplies, and personnel. The use of predictive analytics is still in its infancy and most projects remain in the early stages of development, but funder appetite for its use in conflict settings is among the drivers of innovation in this space.

There are a number of early warning and disaster risk systems in place, including the Google programme to calculate inundation and flooding probabilities (Nevo 2019). Real-time data measurement is used to predict

the target of incoming missiles and provide evacuation warnings in Syria (Hala Systems Inc. 2019), and UNHCR's Jetson project can predict the displacement of people in Somalia at least a month in advance (UNHCR Innovation Service 2019). More research needs to be carried out to verify the claims made for these early-stage innovations (Hernandez and Roberts 2020). A report by OCHA's Centre for Humanitarian Data recognises their value in disaster risk financing frameworks, but recommends local participation in the design phase to improve accuracy of models and foster buy-in from local governments and other stakeholders (Bodanac 2020).

The Novissi programme in Togo uses machine learning-based targeting, basing the predictions using satellite data to find the poorest geographies, and then identifying the poorest people in those areas using mobile usage data. They then put out radio adverts inviting people to send an SMS to enrol; the self-enrolment tool matches an applicant's ID and phone number against the poverty scores determined by the machine learning algorithm. If they qualify, people are paid immediately using mobile money (Blumenstock 2021). The principle underlying the design of these non-traditional targeting systems is that they can, in theory, identify people who might be excluded from official lists for a range of reasons, including the fact that they might be living in a marginal community located in a wealthy area (Raftree and Kondakhchyan 2021a).

The programme's designers recognise that the system risks excluding the very poorest by virtue of the fact that it relies on mobile connectivity; however, in the context of Covid-19, the only way the government could quickly distribute cash at scale during the pandemic was by using mobile money. They have also made it possible for people who have a SIM card but no mobile phone to use the system as well, and kept an offline channel open through partnering with community-based organisations (CBOs) in target geographies to enrol and pay their constituents remotely.

5.3.1 Risks

Replacing human deliberative and decision-making processes with AI, algorithms, and automated decision-making delivers cost-efficiency gains but it is not without risks; it risks amplifying and automating the inequalities and prejudices that are contained within the historical data on which algorithms are trained (Hernandez and Roberts 2020).

A series of studies have shown how the use of big data to train algorithms in automated decision-making systems is already being applied in the United States to determine who will get access to housing, welfare payments, job interviews, bail/probation, and a growing list of services from government and agencies. The evidence from a growing number of studies shows how algorithms reproduce, accelerate, and automate the historical patterns of gender, race, and class bias contained in the historical data sets on which the technology is trained (Eubanks 2018; O'Neil 2017; Benjamin 2019; Criado Perez 2019).

Replacing human deliberation and inclusive decision-making with AI also risks dehumanising humanitarian work in ways that are arguably inconsistent with its foundational ethics. Humanitarianism is partly about restoring humanity by engaging on a human level with persons experiencing traumatic events, and it increasingly includes a commitment to keeping the voices and needs of affected populations centre stage (World Humanitarian Summit Secretariat 2015). AI, by contrast, is dehumanising to the extent that it replaces human deliberation and dialogue with automated algorithmic decision-making processes (Roberts and Faith 2021).

The use of AI algorithms in humanitarian action also carries accountability risks. The algorithms at the heart of many AI systems are proprietary 'black-boxed' systems (Pasquale 2015). They are generally considered to be the intellectual property of the company responsible for their production and classified as trade secrets. The machine learning processes used to train algorithms mean that even the companies are not necessarily aware of the logic that their algorithms use to produce their predictions (Siegel 2016). This can make transparency and accountability impossible, and presents a formidable barrier to learning lessons from errors.

These risks are the focus of a significant amount of reflection in the sector. The OCHA Centre for Humanitarian Data is active in reviewing developments, and the Data Science and Ethics Group has published a *Framework for the Ethical Use of Advanced Data Science Methods in the Humanitarian Sector* (2020). The emerging area of 'algorithmic accountability' in humanitarian action seeks to address this issue by making algorithms open and subject to audit (van den Homberg, Gevaert and Georgiadou 2020). Without

sufficient attention to addressing these risks, use of these technologies may lead to a form of digital humanitarianism that reflects, reproduces, and amplifies patterns of historic inequality and dependency

Box 5.6: Research gaps in artificial intelligence and predictive analytics

There has been limited research to date on artificial intelligence (AI), algorithmic decision-making, and predictive analytics more broadly in the humanitarian–development–peace-building field and also specifically in the humanitarian–social protection nexus. The research that does exist has relied on agencies' own accounts of their own pilot projects. Independent primary research is necessary to understand whether these early initiatives are ongoing, what forward investments are being made, and what the main drivers, actors, technologies, and outcomes in this emerging area of digital humanitarianism are. The claims that these technologies can help to predict and prevent disasters mean that there is good reason to research promising case studies and to track attempts to scale and adapt the initial pilot studies.

5.4 Remote monitoring and accountability systems

Box 5.7: Technology for remote monitoring and accountability

Function: Handheld devices for digital data collection, mobile phone-based feedback mechanisms, remote sensing with satellites or delivery tracking, blockchain for tracking funds, and supply chains.

Claims/impact:

Contribute to rapid and near real-time monitoring and accountability;

Provide different types of data to assess programming;

Allow for more systematic tracking of indicators.

Against a backdrop of increased political scrutiny and cuts to development budgets, there is pressure from donors to adopt remote monitoring via digital tools with the intention of cutting costs, monitoring from a safe distance, and achieving increased transparency and accountability. Remote monitoring can be conducted using a growing range of digital technologies including satellite images, drone footage, remote sensing, and mobile phone surveys. In relation to the humanitarian nexus and the transfer from humanitarian assistance to government-led social protection, there is potential for the research and development costs of system innovation to be borne by humanitarian agencies and the relatively low-cost monitoring via the 'finished' dashboard handed over to the government in question.

In an ideal world, the affordances of these technologies could be used by humanitarian and government actors to improve the speed and accuracy of service delivery. A 2016 report, *Technologies for monitoring in insecure environments* (Dette, Steets and Sagmeister 2016), outlined a range of benefits of phone-based monitoring mechanisms, including wide reach, direct interaction, specificity and detail of information, and two-way communication. Remote monitoring surveys have been used to good effect by WFP to conduct food security surveys in conflict settings where household surveys are either impossible or high risk. Oxfam's Responsive Listening through Improved Feedback Mechanisms Project (Valteri 2019) uses secure mobile data collection tools to collect feedback from the communities they have been working with across the Middle East, starting with a pilot in Zaatari refugee camp in Jordan. The project sought to 'strengthen accountability through feedback mechanisms which are safe, confidential and trustworthy'.

Digital tools have been used to encourage beneficiaries to apply for cash support during pandemics. This has been particularly relevant during Covid-19, when face-to-face contact was limited due to public health-related restrictions. Digital applications for emergency relief were encouraged via mobiles, WhatsApp or websites in Namibia, South Africa, Brazil, Pakistan, and Togo, and resulted in very large volumes of applications in a short period (Gelb and Mukherjee 2020).

Another key aspect of transparency and accountability is the flow of aid funds and the challenges of tracking money through the system. A reflection paper, *Money Flows and Blockchains in Aid* (Currion 2020b), looks at the implicitly hierarchical structure of aid in which money flows through centralised financial structures, seeing aid disbursement as a 'collective action' problem that cannot be solved by a single agency. That paper reflects on the Disberse pilot projects, which were set up to assess whether the distributed ledger technology blockchain could enhance transparency, increase the speed at which money flows to the end recipient, and reduce intermediary costs. Blockchain provides a means to share information and transfer digital assets in a fast and traceable way; it offers a range of potential benefits, particularly in cash programming and supply chain tracking (Ko and Verity 2016). However, despite a degree of hype about the potential of this technology, there are yet to be sustainable examples of these platforms working at scale, including the Disberse project, which was discontinued.

5.4.1 Risks

In their reflections on the Disberse project, those who designed it raise key points about the bigger issue of transparency in the aid industry:

> For many reasons, power generally rests towards the beginning of the delivery chain, and diminishes the further along the delivery chain you travel… standardised datasets on aid are of little use to a person affected by disaster, if they lack the power to act on what they learn through that transparency... if you do not have other tools that will enable you to hold those institutions accountable.
> (Currion 2020a)

These reflections also apply to the broader use of technology for accountability. Research from the Making All Voices Count programme at IDS concluded that increased transparency and accountability is not achieved via remote monitoring technologies: 'the kinds of democratic deliberation needed to challenge a systemic lack of accountability are rarely well supported by technologies'. Furthermore, it concluded that 'The capacities needed to transform governance relationships are developed offline and in social and political processes, rather than by technologies' (McGee *et al*. 2018: 20).

The process of data collection for monitoring and accountability in conflict settings raises additional challenges. The newly formed Humanitarian Data and Trust Initiative warns that in conflict settings with a high degree of insecurity, remote monitoring by donors means that informal data requests beyond formal, codified agreements 'may be motivated by other, non- humanitarian uses for disaggregated data that are not always made explicit' (Belina *et al*. 2020: 3). A recent blog exploring the use of biometric tracking in Yemen argued that it was unlikely that this would stop aid from being redirected upstream to armed groups (Raftree and Steinacker 2019).

Box 5.8: Research gaps in technology for accountability

Greater understanding of the mediating role of technology in systems for upward and downward accountability.

Most research, and humanitarian and social protection innovation in this space, has focused on the use of technology to protect against the risk of inclusion errors, ghost recipients, and other leakages and downstream corruption. There has been far less research and innovation on exclusion errors and upstream leakage and corruption.

Digital identity, registration, data analytics, and remote sensing technologies can be seen as mechanisms to increase the power/knowledge of power-holders over affected populations. The technologies themselves are equally capable of making the detailed transactions and expenditures of humanitarian and government consultants transparent and accountable to affected populations and local staff.

More research is needed into the opportunities for using technology to make humanitarian and government systems more transparent and accountable to affected populations.

6. Research themes

The overview of technologies for digital humanitarian action and social protection in crises has highlighted some emergent themes that we have clustered broadly under the headings of power, exclusion, and transparency and accountability. Many of these issues are related to the reordering and transformation of social life through increasing 'datafication' of social relations as we increasingly interact with our social and political environment through digital media (Couldry and Mejías 2019; Hintz, Dencik and Wahl-Jorgensen 2018). This has resulted in a power asymmetry between citizens and those who control the data-driven systems through which their daily practices are governed (Van Dijck 2020: 1). The challenges raised by the governance of corporate technology platforms in undermining classic distinctions between humanitarian agencies, private companies, and governments are widely acknowledged but are, arguably, even more urgent in the context of providing social assistance to vulnerable people in conflict settings.

Agencies, companies, and governments working in the humanitarian and social protection spaces increasingly rely on data in their everyday operations and are gathering more and more data during the processes described in the previous section. For example, the range of data collected during cash transfer operations includes Know Your Customer (KYC) data, such as name, surname, mobile phone number, as well as geolocation/other phone metadata and biometrics (ICRC 2020). The most vulnerable people often have the least power and agency in the use of these data. In a study on humanitarian data justice in the context of post-earthquake Nepal, Mulder argues that in many disaster contexts, the 'least resilient are behind digital or virtual divides and have little control over if and how they are represented in humanitarian data sets and information products. They may be included or excluded against their will or knowledge' (2020: 443). Refugees are required to use digital cash transfers in some places, which produces a lot of data, but they cannot necessarily consent if it is the only option (Jacobsen and Fast 2019). This is not inevitable.

Key points in relation to the challenges of the move from humanitarian to state-led systems seem to be that governments might not have the institutional and governance frameworks to support integrated digital social protection systems – both data protection legislation and digital security capacity. The SPACE/BASIC frameworks cited earlier lay out clearly the 'best practice' in terms of supportive ecosystems; but these best practices are challenging to implement, particularly in relation to costly resources such as the specialised personnel who have both sectoral expertise in cash assistance and digital skills. Research exploring the challenges of implementing these ecosystem approaches in target countries would be very valuable. This speaks to the need for context-specific research that highlights the particularities of issues around identity, visibility, and exclusion in a particular region or setting.

6.1 Decentralised technologies

The clients of humanitarian assistance and government social protection could be the owners of decentralised smartcard systems, which they use to retain their own digital identity and service user information. They could be the arbiters of decisions about if and when to share any part of their data. The data do not need to be centrally held on a national or agency database for humanitarian assistance or government social protection systems to function (Abraham *et al*. 2020). This could provide a more streamlined system for transferring responsibility from humanitarian assistance to government provision without the need for massive information technology projects that attempt to make uniform all legacy systems in disparate agencies and government departments.

Other decentralised systems include Community Inclusion Currencies, which are a regional means of exchange that supplements the national currency system, offering an interesting alternative to existing 'top-down' models of cash assistance. People can trade goods and services with each other using a simple mobile phone-based system that does not require any internet connectivity. Advocates suggest that these programmes can improve food security, rewarding environmental restoration and refugee inclusion efforts. The Sarafu Network, for example, has around 40,000 users and was adopted by the Kenya Red Cross as part of its humanitarian response to the Covid-19 pandemic, with research showing a positive economic impact on beneficiaries (Mqamelo 2021). Further exploration of these systems in other contexts would be valuable.

All these themes point to a broader research agenda which asks: 'Where do the benefits of these technologies accrue?' Against this backdrop, OCHA's recently released report on new and emerging technologies in humanitarian action called for a 'comprehensive research and practice agenda for the development, application and scaling of new and emerging technologies in humanitarian action' (OCHA 2021).

6.2 Value for money (VfM)

The recent SPACE paper argues that VfM analyses of digital systems should go beyond measures of efficiency and effectiveness to a broader notion of digital dignity that:

> …recognises the importance of beneficiary rights, and that individuals need to be respected as active data agents, and not purely as a passive data subject. They need to be given the opportunity (and capacity) to request data erasure and rectification, as well as be informed about data use and implications – and crucially to manage consent, especially as interoperability introduces changes to data use.
> (Schoemaker 2020)

There are also issues relating to the transparency of the claimed financial benefits of digitised systems, which connect to the VfM theme. An audit of WFP's beneficiary information and transfer management platform, SCOPE, which was established in 2015, reflected that the 'framework is not yet present to rigorously account for the costs and benefits accrued from implementing the technology platform' (Office of the Inspector General WFP 2021: 20). CaLP's forecasting work looking at the future of financial assistance warns of 'concerns about the potential for user exploitation and the risks of dependency on any single company or platform' (CaLP and Inter-Agency Research and Analysis Network (IARAN) 2019).

While claims for the benefits of digitisation often rest on cost savings, data relating to these costs and benefits are not easily accessible. The procurement of the digital ID scheme in Uganda was conducted through a 'classified procurement' contrary to the Public Procurement and Disposal Act 2003, and with limited public access to tender or contract documents (Unwanted Witness 2020). The WFP SCOPE audit found that a system had only recently been put in place 'to rigorously account for the costs and benefits accrued from IT projects and investments. Cost recovery mechanisms were also lacking, to allow for SCOPE's continuous improvement and the sustainability of associated support services' (Office of the Inspector General WFP 2021). The open letter signed by civil society groups in response to the WFP/Palantir agreement (ResponsibleData.io 2019) warns of a lack of transparency in procurement processes between humanitarian organisations and technology companies, suggesting that no third-party audits are possible under current arrangements. This makes it impossible to carry out a future cost analysis of the relationship. It could be that

this relationship cuts costs in the short term but significantly increases them in the longer term. There is also a risk that ending the partnership may be costly for humanitarian organisations, or they may end up locked into technologies.

There are now thousands of public–private partnerships (PPPs) in the humanitarian sector. Arguably, humanitarian contexts provide a less-regulated space for corporate piloting of new tech, extracting data, and gaining market share in emerging markets to secure future revenue streams. As Professor Sir Michael Aaronson (former chief executive of Save the Children) argued in a recent report, private sector innovation poses 'particular challenges of governance, as companies, not unreasonably, pursue their own profit rather than act from altruistic motives' (Roberts and Faith 2021). Madianou (2019) argues that 'the convergence of digital developments with humanitarian structures and market forces reinvigorates and reshapes colonial relationships of dependency'. There is a gap in the existing research for the mapping of corporate actors in digital registration, identity, artificial intelligence, and remote monitoring. There is little understanding of the dimensions of the market, the scale or direction of the investments being made, or the drivers, key actors, or tools. Such data would be important in understanding the process of privatisation and the implication for the move away from humanitarian provision to government and corporate provision.

7. Conclusion

Further research is needed to better understand how these wider political and commercial drivers, as well as the pressures of crisis contexts and the desire to move to government provision are shaping the adoption of digital technologies. There is also a need to improve understanding of the opportunities, risks, and implications for accountability upwards to donors but also downwards to affected populations.

Some actors strongly believe that digital technologies will facilitate greater integration across the humanitarian–development–peace-building nexus and that they will smooth the transition from humanitarian assistance to government-led provision. This paper has assessed only a modest subset of the digital technologies in which such hope is invested: technologies of digital registration and identity, algorithmic decision-making, and remote monitoring. We have noted that powerful donor, corporate, and wider economic forces lead to pressure to innovate and adopt digital technologies at the humanitarian–development–peace nexus.

This paper has also shown that humanitarian and social protection actors are increasingly concerned about a range of risks and accountability vacuums associated with the adoption of these technologies, and are taking steps to address perceived challenges. Humanitarian agencies and governments currently have insufficient knowledge about how the movement towards biometric identification and algorithmic management using humanitarian data will impact on the interests of vulnerable populations. There are also fears that the kind of massive data breach that has affected government and corporations will at some point affect a humanitarian database of sensitive personal data about thousands of acutely vulnerable people. There is considerable uncertainty about the risks of sharing data with companies and governments that may, some years hence, be headed up by very different personnel who may have quite different (even repressive) interests and commitments.

From a rigorous review of the literature, it is clear that there is an overall research gap and a lack of comparative studies exploring whether the processes of digitisation and datafication of social assistance systems enable or inhibit accountability and inclusion. Specifically, there are key issues relating to informed consent and data-sharing, the digital threat landscape in conflict settings, and the true value of predictive analytics in improving issues such as targeting in the humanitarian/social protection field. We need to understand how digital technologies can address power asymmetries by making humanitarian and government systems more accountable and transparent to affected populations, or by powering decentralised systems to allow people to retain agency over their own digital identity and service user information. Addressing those gaps suggests an agenda for BASIC research on these issues that is focused on the standpoints, interests, and priorities of affected populations, building their understanding and the understanding of humanitarian and social protection staff about the implications of this rapidly developing technological environment.

References

Abraham, A.; More, S.; Rabensteiner, C. and Hörandner, F. (2020) 'Revocable and Offline-Verifiable Self-Sovereign Identities' (pp. 1020–1027), paper presented at the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 29 December 2020 – 1 January 2021

Access Now (2020) *Recognizing Human Rights Norms in the 'Principles on Identification for Sustainable Development'. CSO Consultation Report*, (accessed 4 May 2021)

Alston, P. (2019) Report of the Special Rapporteur on Extreme Poverty and Human Rights, Seventy-fourth session Agenda item 70 (b), United Nations General Assembly (accessed 5 January 2022)

Aneja, U. and DuBois, M. (2020) 'Covid-19 Futures in Humanitarian Action', Humanitarian Practice Network, 29 September (accessed 5 January 2022)

Bailey, S. and Harvey, P. (2017) *The DFID/ECHO Approach to Cash Assistance for Refugees in Lebanon*, Working Paper 525, London: Overseas Development Institute

Barca, V. (2017) *Integrating Data and Information Management for Social Protection: Social Registries and Integrated Beneficiary Registries*, Canberra: Commonwealth of Australia, Department of Foreign Affairs and Trade (accessed 5 January 2022)

Barca, V. and Beazley, R. (2019) *Building on Government Systems for Shock Preparedness and Response: The Role of Social Assistance Data and Information Systems*, Canberra: Commonwealth of Australia, Department of Foreign Affairs and Trade

Barca, V. and Chirchir, R. (2019) *Building an Integrated and Digital Social Protection Information System*, Bonn, Germany: Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH/Department for International Development (accessed 5 January 2022)

Beazley, R.; Barca, V. and Derban, W. (2020) *Options for Rapid Delivery (Payment) of Cash Transfers for COVID-19 Responses and Beyond*, Social Protection Approaches to COVID-19 (SPACE), London: Department for International Development and Die Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) (accessed 5 January 2022)

Belina, J. *et al*. (2020) *Responsible Data Sharing with Donors: Accountability, Transparency and Data Protection in Humanitarian Action*, Report, Thursday 17 – Friday 18 September 2020, Switzerland: Wilton Park, (accessed 8 December 2020)

Benjamin, R. (2019) *Race After Technology: Abolitionist Tools for the New Jim Code*, Medford, MA: Polity

Blumenstock, J. (2021) *Using Mobile Phone and Satellite Data to Target Emergency Cash Transfers*, Center for Effective Global Action (CEGA) blog, 16 February (accessed 5 January 2022)

Bodanac, N. (2020) *Predictive Analytics for Anticipatory Action: Challenges and Opportunities*, OCHA Centre for Humanitarian Data (accessed 5 January 2022)

Burton, J. (2020) '"Doing No Harm" in the Digital Age: What the Digitalization of Cash Means for Humanitarian Action', *International Review of the Red Cross* 102.913: 43–73, DOI: 10.1017/S1816383120000491 (accessed 5 January 2022)

Cangiano, M.; Gelb, A. and Goodwin-Groen, R. (2019) *Public Financial Management and the Digitalization of Payments*, CGD Policy Paper 144, Washington DC: Center for Global Development (accessed 5 January 2022)

Carmona, M.S. (2018) *Is Biometric Technology in Social Protection Programmes Illegal or Arbitrary? An Analysis of Privacy and Data Protection*, ESS (Extension of Social Security) Working Paper 59, Geneva: International Labour Office

CaLP (2020) *The State of the World's Cash 2020: Cash and Voucher Assistance in Humanitarian Aid*, Cash Learning Partnership (accessed 6 January 2022)

CaLP (2019) *Addressing Challenges in Humanitarian Cash and Voucher Assistance Using Mobile Money in Somaliland*, Cash Learning Partnership, Mobile for Humanitarian Innovation Workshop, 8 April 2019, Ambassador Hotel, Hargeisa (accessed 5 January 2022)

CaLP and IARAN (2019) *The Future of Financial Assistance: An Outlook to 2030*, CaLP and Inter-Agency Research and Analysis Network (accessed 6 January 2022)

Couldry, N. and Mejías, U.A. (2019) *The Costs of Connection: How Data is Colonizing Human Life and Appropriating it for Capitalism*, Stanford: Stanford University Press

Criado Perez, C. (2019) *Invisible Women: Exposing Data Bias in a World Designed for Men*, London: Chatto & Windus

Currion, P. (2020a) *What Does Transparency Look Like?* Frontier Technologies Hub blog, 4 February (accessed 29 January 2021)

Currion, P. (2020b) *Reflection Paper: Money Flows and Blockchains in Aid*, Medium blog, 14 December (accessed 29 January 2021)

Daniels, C. and Anderson, G. (2018) *Evaluation of the 2017 Somalia Humanitarian Cash-Based Response*, Mogadishu: Inter-Agency Cash Working Group

Dencik, L. and Kaun, A. (2020) 'Datafication and the Welfare State', *Global Perspectives* 1.1, DOI: 10.1525/gp.2020.12912 (accessed 6 January 2022)

Dette, R.; Steets, J. and Sagmeister, E. (2016) *Technologies for Monitoring in Insecure Environments*, Toolkit from the Secure Access in Volatile Environments (SAVE) Research Programme, Humanitarian Outcomes (accessed 6 January 2022)

Eubanks, V. (2018) *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, New York: St. Martin's Press

Gelb, A. and Mukherjee, A. (2020) *Digital Technology in Social Assistance Transfers for COVID-19 Relief: Lessons from Selected Cases*, CGD Policy Paper 181, Washington DC: Center for Global Development (accessed 6 January 2022)

Gentilini, H.; Laughton, S. and O'Brien, C. (2018) *Human(itarian) Capital? Lessons on Better Connecting Humanitarian Assistance and Social Protection*, Social Protection & Jobs Discussion Paper 1802, Washington DC: World Bank and World Food Programme (accessed 6 January 2022)

Gilert, H. and Austin, L. (2017) *Review of the Common Cash Facility Approach in Jordan*, Jordan: Cash Learning Partnership and the UN Refugee Agency (UNHCR) (accessed 6 January 2022)

Global Partnership for Financial Inclusion (2016) *G20 High-Level Principles for Digital Financial Inclusion* (accessed 6 January 2022)

Goodman, R.; Frey, C.; Ahmed, Z.; Steller, R. and Qatinah, A. (2019a) *Yemen – Linking Humanitarian Cash and Social Protection (Phase II Report)*, BASIC (Better Assistance in Crises) – TAS, London: UKaid

Goodman, R.; Frey, C; Steller, R.; Ahmed, Z. and Qatinah, A. (2019b) *Yemen – Linking Humanitarian Cash and Social Protection (Phase I Report)*, Version 2, London: DAI/DFID

Goodman, R.; Schoemaker, E.; Messenger, C. and Steller, R. (2020) *Review and Analysis of Identification and Registration Systems in Protracted and Recurrent Crises*, BASIC (Better Assistance in Crises), London: UKaid (accessed 6 January 2022)

Gronbach, L. (2020) *Social Cash Transfer Payment Systems in Sub-Saharan Africa*, South Africa: University of Cape Town (accessed 6 January 2022)

GSMA (2019) *The Digital Lives of Refugees: How Displaced Populations Use Mobile Phones and What Gets in the Way*, GSMA (accessed 5 January 2022)

Hala Systems Inc. (2019) 'Protect Everything that Matters' (accessed 6 January 2022)

Handayani, S.W.; Domingo-Palacpac, M.; Chi Burkley, C. and Lovelock, P. (2017) *Improving the Delivery of Social Protection Through ICT: Case Studies in Mongolia, Nepal, and Viet Nam*, ADB Sustainable Development Working Paper Series No. 50, Manila, Philippines: Asian Development Bank (accessed 6 January 2022)

Hernandez, K. and Roberts, T. (2020) *Predictive Analytics in Humanitarian Action: A Preliminary Mapping and Analysis*, K4D Emerging Issues Report 33, Brighton: Institute of Development Studies (accessed 5 January 2022)

Hernandez, K. and Roberts, T. (2018) *Leaving No One Behind in a Digital World*, K4D Emerging Issues Report 34, Brighton: Institute of Development Studies (accessed 6 January 2022)

Hintz, A.; Dencik, L. and Wahl-Jorgensen, K. (2018) *Digital Citizenship in a Datafied Society*, Medford MA: Polity Press

Human Rights Watch (2021) 'UN Shared Rohingya Data Without Informed Consent', 15 June (accessed 15 June 2021)

ICRC (2020) *Cash Transfer Programming in Armed Conflict: The ICRC's Experience*, Geneva: International Committee of the Red Cross (accessed 6 January 2022)

ICRC and Privacy International (2018) *The Humanitarian Metadata Problem – 'Doing No Harm' in the Digital Era* (accessed 6 January 2022)

Jacobsen, K.L. and Fast, L. (2019) 'Rethinking Access: How Humanitarian Technology Governance Blurs Control and Care', *Disasters* 43: S151–S168

Juergens, F. and Galvani, F. (2021) *Social Protection for Older People During COVID-19 and Beyond*, London: HelpAge International (accessed 6 January 2022)

Ko, V. and Verity, A. (2016) *Blockchain for the Humanitarian Sector: Future Opportunities*, Digital Humanitarian Network (accessed 5 January 2022)

Kuner, C. and Marelli, M. (eds) (2020) *Handbook on Data Protection in Humanitarian Action*, 2nd ed., Geneva: International Committee of the Red Cross and Brussels Privacy Hub (accessed 6 January 2022)

Kuner, C. and Marelli, M. (eds) (2017) *Handbook on Data Protection in Humanitarian Action*, Geneva: International Committee of the Red Cross (accessed 6 January 2022)

Landa, N. (2020) *Emerging Field Practices to COVID-19 in Refugee Contexts*, Social Protection blog, 14 July (accessed 10 January 2022)

Loy, I. (2021) 'Biometric Data and the Taliban: What Are the Risks?', *The New Humanitarian*, 2 September (accessed 6 January 2022)

Madianou, M. (2019) 'The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies', *Television & New Media* 20.6: 581–99, DOI: 10.1177/1527476419857682 (accessed 10 January 2022)

McDonald, S. (2019) *From Space to Supply Chains: A Plan for Humanitarian Data Governance*, SSRN (accessed 6 January 2022)

McGee, R.; Edwards, D.; Hudson, H.; Anderson, C. and Feruglio, F. (2018) *Appropriating Technology for Accountability: Messages from Making All Voices Count*, Making All Voices Count Research Report, Brighton: Institute of Development Studies (accessed 6 January 2022)

Mqamelo, R. (2021) 'Community Currencies as Crisis Response: Results From a Randomized Control Trial in Kenya', *Frontiers in Blockchain* 4, DOI: 10.3389/fbloc.2021.739751 (accessed 6 January 2022)

Mulder, F. (2020) 'Humanitarian Data Justice: A Structural Data Justice Lens on Civic Technologies in Post-Earthquake Nepal', *Journal of Contingencies and Crisis Management* 28.4: 432–445

Nevo, S. (2019) *An Inside Look at Flood Forecasting*, Google AI Blog, 18 September (accessed 6 January 2022)

O Foundation (OFDN) (2021) *MarginalizedAadhaar*, documentary (accessed 10 January 2022)

OCHA (2021) *From Digital Promise to Frontline Practice: New and Emerging Technologies in Humanitarian Action*, United Nations Office for the Coordination for Humanitarian Affairs (accessed 6 January 2022)

OCHA (2019) *Data Responsibility Guidelines*, UN OCHA Centre for Humanitarian Data (accessed 6 January 2022)

OCHA Centre for Humanitarian Data (2019) *OCHA Data Responsibility Guidelines*, Centre for Humanitarian Data (accessed 10 January 2022)

Office of the Inspector General WFP (2021) *Internal Audit of SCOPE WFP's Digital Management of Beneficiaries*, Draft Internal Audit Report AR/21/08 (accessed 6 January 2022)

OHCHR (2020) *Racial Discrimination in the Context of the COVID-19 Crisis*, Topic in Focus, 22 June, Office of the High Commissioner for Human Rights (accessed 6 January 2022)

O'Neil, C. (2017) *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, London: Penguin Books

Owino, B. (2020) 'Harmonising Data Systems for Cash Transfer Programming in Emergencies in Somalia', *Journal of International Humanitarian Action* 5.1: 11, DOI: 10.1186/s41018-020-00077-1 (accessed 10 January 2022)

Parker, B. (2020) 'Exclusive: The Cyber Attack the UN Tried to Keep Under Wraps', *The New Humanitarian*, 29 January (accessed 6 January 2022)

Pasquale, F. (2015) *The Black Box Society: The Secret algorithms That Control Money and Information*, Harvard University Press (accessed 10 January 2022)

Pelly, I. (2020) *Linking Cash and Voucher Assistance and Social Protection in Forced Displacement Contexts*, Social Protection blog, 18 February (accessed 6 January 2022)

Prady, D. (2020) *Reaching Households in Emerging and Developing Economies: Citizen ID, Socioeconomic Data, and Digital Delivery*, Special Series on Fiscal Policies to Respond to COVID-19, IMF Fiscal Affairs (accessed 6 January 2022)

Principles for Digital Development (2021) 'Address Privacy & Security' (accessed 8 June 2021)

Privacy International (2021) 'Exclusion By Design: How National ID Systems Make Social Protection Inaccessible to Vulnerable Populations', Privacy International, 29 March (accessed 10 May 2021)

Privacy International (2020) 'Here's How a Well-Connected Security Company is Quietly Building Mass Biometric Databases in West Africa with EU Aid Funds', Privacy International, 10 November (accessed 12 January 2021)

Privacy International (2018) '"Do No Harm" in the Digital Age: Privacy and Security Cannot be Ignored', Privacy International, 11 December (accessed 10 January 2022)

Radice, H.W. and Hussein, M.J. (2017) *More Phones, More Transfers? A Case Study From Save the Children's Emergency Food Security Program Using Mobile Money in Bari, Nugaal, & Hiran Regions of Somalia*, Washington DC: Save the Children International (accessed 10 January 2022)

Raftree, L. and Kondakhchyan, A. (2021a) *Data Responsibility and Digital Remote Targeting During COVID-19*, CaLP (accessed 10 January 2022)

Raftree, L. and Kondakhchyan, A. (2021b) *Data Responsibility Toolkit: A Guide for CVA Practitioners*, CaLP (accessed 9 April 2021)

Raftree, L. and Steinacker, K. (2019) 'Head to Head: Biometrics and Aid', *The New Humanitarian*, 17 July (accessed 10 January 2022)

Rahman, Z.; Verhaert, P. and Nyst, C. (2018) *Biometrics in the Humanitarian Sector*, Oxford: Oxfam, The Engine Room

ResponsibleData.io (2019) *Open Letter to WFP re: Palantir Agreement*, Responsible Data blog, 8 February (accessed 10 January 2022)

Roberts, T. and Faith, B. (2021) *Digital Aid: Understanding the Digital Challenges Facing Humanitarian Assistance*, Brighton: Institute of Development Studies, DOI: 10.19088/IDS.2021.030 (accessed 6 January 2022)

Roberts, T. *et al*. (2021) *Digital Rights in Closing Civic Space: Lessons from Ten African Countries*, Brighton, UK: Institute of Development Studies

Robinson, A.; Marella, M. and Logam, L. (2020) *Gap Analysis: the Inclusion of People with Disability & Older People in Humanitarian Response*, London: Elrha (accessed 10 January 2022)

Rohweder, B. and Szyp, C. (2022) *The Risks and Outcomes of Getting Help for Marginalised People: Navigating Access to Social Assistance in Crises*, BASIC Research Working Paper 7, Brighton: Institute of Development Studies, DOI: 10.19088/BASIC.2022.007

Sandhu, H.S. and Raja, S. (2019) *No Broken Link: The Vulnerability of Telecommunication Infrastructure to Natural Hazards*, Washington DC: World Bank

Sandvik, K.B.; Jacobsen, K.L. and McDonald, S.M. (2017) 'Do No Harm: A Taxonomy of the Challenges of Humanitarian Experimentation', *International Review of the Red Cross* 99.904: 319–44, DOI: 10.1017/S181638311700042X (accessed 10 January 2022)

Sandvik, K.B.; Jumbert, M.G.; Karlsrud, J. and Kaufmann, M. (2014) 'Humanitarian Technology: A Critical Research Agenda', *International Review of the Red Cross* 96.893: 219–42, DOI: 10.1017/S1816383114000344 (accessed 10 January 2022)

Savage, E. (2021) *Humanitarian Cash and Social Protection in Iraq*, CaLP and Meraki Labs (accessed 10 February 2021)

Schoemaker, E. (2020) SPACE *Linking Humanitarian & Social Protection Information Systems in the COVID-19 Response and Beyond*, London: United Kingdom Department for International Development (DFID) and Die Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) (accessed 10 January 2022)

Siegel, E. (2016) *Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die*, Hoboken NJ: Wiley

Smith, G. (2019) *Review of Cash Programming and Linkages to Social Protection in Lebanon*, Better Assistance in Crisis, London: Department for International Development

Smith, G. (2012) *New Technologies in Cash Transfer Programming and Humanitarian Assistance*, Humanitarian Practice Network blog, May (accessed 10 January 2022)

Sowers, J. and Weinthal, E. (2021) 'Humanitarian Challenges and the Targeting of Civilian Infrastructure in the Yemen War', *International Affairs* 97.1: 157–77, DOI: 10.1093/ia/iiaa166 (accessed 10 January 2022)

Sphere Association (2018) *The Sphere Handbook: Humanitarian Charter and Minimum Standards in Humanitarian Response* (accessed 10 January 2022)

Sterck, O.; Rodgers, C.; Siu, J.; Flinder Stierna, M. and Betts, A. (2020) *Cash Transfer Models and Debt in the Kalobeyei Settlement*, World Food Programme (accessed 11 February 2021)

Tasnin, T. (2020) *Distributing Relief in a Pandemic: Lessons Learned About Digital Cash Transfers During COVID-19*, Social Protection blog, 9 July (accessed 10 January 2022)

UNHCR Innovation Service (2019) *Is It Possible to Predict Forced Displacement?*, 13 May (accessed 10 January 2022)

Unwanted Witness (2020) *Uganda's Digital Identification Systems and Processes in a Protracted Crisis: What Can Be Done?*, Kampala: Unwanted Witness (accessed 10 January 2022)

Valteri, E.T. (2019) *The Future is Bright for Digital Accountability*, Oxfam Views & Voices blog, 23 September (accessed 6 January 2022)

van den Homberg, M.J.; Gevaert, C.M. and Georgiadou, Y. (2020) 'The Changing Face of Accountability in Humanitarianism: Using Artificial Intelligence for Anticipatory Action', *Politics and Governance* 8.4: 456–67

Van Dijck, J. (2020) 'Seeing the Forest for the Trees: Visualizing Platformization and its Governance', *New Media & Society* 23.9: 2801–19, DOI: 10.1177/1461444820940293 (accessed 10 January 2022)

Van Dijck, J. (2014) 'Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology', *Surveillance & Society* 12.2: 197–208

van Solinge, D. (2019) *Digital Risks for Populations in Armed Conflict: Five Key Gaps the Humanitarian Sector Should Address*, Humanitarian Law & Policy blog, 12 June (accessed 6 January 2022)

van Veen, C. and Cioffi, K. (2021) *Everyone Counts! Ensuring That the Human Rights of All are Respected in Digital ID Systems*, NYU School of Law – Centre for Human Rights and Global Justice blog, 6 April (accessed 10 January 2022)

Weitzberg, K.; Cheesman, M.; Martin, A. and Schoemaker, E. (2021) 'Between Surveillance and Recognition: Rethinking Digital Identity in Aid', *Big Data & Society* 8.1, DOI: 10.1177/20539517211006744 (accessed 10 January 2022)

WFP (2020) *COVID-19 Level 3 Emergency*, External Situation Report 12, World Food Programme (accessed 6 January 2022)

World Bank (2021) *Principles on Identification for Sustainable Development : Toward the Digital Age* (accessed 10 January 2022)

World Bank (2016) *World Development Report 2016: Digital Dividends*, Washington DC: World Bank (accessed 10 January 2022)

World Economic Forum (2019) *The Global Risks Report 2019*, World Economic Forum (accessed 30 April 2021)

World Humanitarian Summit Secretariat (2015) *Restoring Humanity: Synthesis of the Consultation Process for the World Humanitarian Summit*, New York: United Nations (accessed 10 January 2022)

Zimmerman, J.; May, M.; Kellison, E. and Klugman, J. (2020) *Digital Cash Transfers in Times of COVID-19 : Opportunities and Considerations for Women's Inclusion and Empowerment*, Washington DC: World Bank Group (accessed 30 April 2021)

Acknowledgements and Disclaimer

This document was developed by the Better Assistance in Crises (BASIC) Research programme. BASIC is implemented by the Institute of Development Studies (IDS), the University of Sussex and the Centre for International Development and Training, funded by UKAid from the UK government. The views expressed in this document are entirely those of the authors and do not necessarily represent views or policies of the UK governments official policies.

Published by IDS.

Suggested citation

Faith, B.; Roberts, T. and Hernandez, K. (2022) *Risks, Accountability and Technology Thematic Working Paper*, BASIC Research Working Paper 3, Brighton: Institute of Development Studies, DOI: 10.19088/BASIC.2022.003