International Review of the Red Cross (2020), **102** (913), 43–73.
Digital technologies and war
doi:10.1017/S1816383120000491

IRRC

"Doing no harm" in the digital age: What the digitalization of cash means for humanitarian action

Jo Burton*
Jo Burton is a Cash Transfers and Markets Specialist with over twelve years of field experience in conflict-affected countries. Having first worked with Cash and Voucher Assistance (CVA) in 2004, she has specialized in CVA in conflict and post-conflict contexts. She is currently the ICRC's Institutional Lead for CVA, ensuring that it is an integral and multidisciplinary part of the ICRC's response to the needs of people affected by armed conflicts and other situations of violence. Email: joburton@icrc.org.

Abstract
Cash transfers have changed the way the humanitarian sector delivers assistance, and at the same time, digitalization is changing the way our world works in fundamental ways. The digitalization of cash means that the simple click of a button can put money in the hands of hundreds of thousands, if not millions, of people within minutes. Digital payments have been a game changer, opening the door to faster and more efficient delivery of life-saving assistance. Although physical currency will not disappear with the rise of digital payments, it is essential to balance the benefits of these digital processes with the risks. As humanitarians, we need to articulate what "do no harm" means in the digital age, applying this equally to the way we use digital payments to support people affected by armed conflicts and other situations of violence.

* This article reflects the author's views alone and not necessarily those of the International Committee of the Red Cross.

Keywords: cash and voucher assistance, cash transfers, digitalization, digital payments, do no digital harm, digital risks, data protection, data responsibility.

Money makes the world go around, or so many would say. But why is cash – an item so familiar in our daily lives – such a talking point in the humanitarian sphere?

It is because the use of "cash", a common shorthand for Cash and Voucher Assistance (CVA),[1] has been one of the biggest changes in humanitarian action in the last decade. CVA use doubled between 2016 and 2019 – in 2019, $5.6 billion of international humanitarian assistance, or 17.9% of the total budget for such assistance, was delivered through cash or vouchers[2] – and it is transforming the way humanitarian assistance is being delivered.

This focus on delivering CVA – the provision of cash[3] and/or vouchers to individuals, households or communities to enable them to access the goods and services that they need,[4] rather than distributing goods – has changed the way we think about and deliver humanitarian assistance, putting an emphasis on the choices of affected people and changing the power dynamics within the humanitarian sector. At the same time, as the use of CVA has increased, we have seen a rise in digital transformation processes across the humanitarian sector, which has been further amplified by the onset of the COVID-19 pandemic. Digitalization is changing how our world works in fundamental ways, from how people communicate to how we form networks, how we travel, and how we make decisions and ensure our voices are heard. In short, digitalization is changing the way people interact with their social, political and built environment, not only in the digital space, but also in the physical space.

When it comes to CVA, digitalization has also changed the way we deliver vital assistance, significantly increasing both the speed of delivery and the volume of people we can reach with that assistance.

This article aims to unpack how CVA and digitalization processes have come together, exploring the "do no digital harm" concept specifically in relation to the use of digital payments to support people affected by armed conflicts and other situations of violence. Starting with a broad overview of some of the digital

1 CVA is the most current terminology used in the humanitarian sector, with the previously used synonyms being Cash Transfer Programming, Cash-Based Assistance and Cash-Based Interventions. See Cash Learning Partnership (CaLP), "Glossary of Terms", available at: www.calpnetwork.org/library-and-resources/glossary-of-terms/ (all internet references were accessed in December 2020).

2 CaLP, *The State of the World's Cash 2020: Cash and Voucher Assistance in Humanitarian Aid*, July 2020, p. 9, available at: www.calpnetwork.org/publication/the-state-of-the-worlds-cash-2020-full-report/.

3 "Cash" in this definition of CVA refers to both physical and digital payments.

4 The International Committee of the Red Cross's (ICRC) definition – in line with CaLP and other CVA providers – focuses on direct transfers to individuals, families and communities in need. The ICRC does not count larger transfers of money to partners like National Red Cross and Red Crescent Societies and large businesses, or salary top-ups to staff in the relevant authorities with whom the organization works. CVA also excludes remittances and micro-finance, although micro-finance institutions may be used for the actual delivery of CVA. ICRC, *Cash Transfer Programming in Armed Conflict: The ICRC's Experience*, Geneva, November 2018, p. 14, available at: www.icrc.org/en/publication/cash-transfer-programming-armed-conflict-icrcs-experience.

trends influencing humanitarian work, it will first define digital payments, exploring the rise of their use in the humanitarian sector. It will then explore how the "do no harm" concept must evolve in an increasingly digitalized world, accounting for the risks and potential pitfalls associated with digital payments, in particular with regard to data protection; here it will focus on the role of the International Committee of the Red Cross (ICRC) as an organization that has been a leading actor in this field over the last decade. The analysis will also highlight how the outlined digital risks associated with CVA can be mitigated. It will conclude with a call to action for humanitarians to be more mindful in our decision-making around digital payments and our interactions in the digital world, always putting affected people at the centre of our work.

Why are humanitarians talking about the digitalization of cash?

To understand the benefits and potential pitfalls associated with the digitalization of cash, it is necessary to unpack three major concepts: digitalization, digital payments, and do no harm.

Digitalization and digital payments

Digitalization covers a wide spectrum of different areas, many of which are explored in the articles collected in this issue of the *Review*. Major trends impacting humanitarian action and the wider world include, but are not limited to, ubiquitous connectivity; big data; the impact of technological disruptors on traditional business models; the spread of misinformation, disinformation and hate speech; cyber warfare; surveillance; and artificial intelligence. Ubiquitous connectivity means that people are better connected than ever; in 2019, more than 53% of the world's population were able to access the Internet[5] and 67% had subscribed to some form of mobile communications services.[6]

This digital connectivity – including the increased use of digital payments – both requires and generates huge quantities of data. The digitalization of this data, including financial data, is enabling increased surveillance, which today can be carried out by governments, lawfully or not, and by corporations that take advantage of the services they provide in order to gather, process or infer information. Additionally, as spying software becomes cheaper and easier to obtain, there are real-world risks beyond a basic invasion of privacy. Evidence shows that despite the duty of States to uphold and protect the rights of citizens, "surveillance of individuals – including government critics, journalists, and human rights advocates – is largely unimpeded, leading to detention, torture, and

5 International Telecommunication Union, *Facts and Figures 2019: Measuring Digital Development*, Geneva, 2019, available at: https://itu.foleon.com/itu/measuring-digital-development/home/.

6 GSMA, *The Mobile Economy 2020*, London, 2020, p. 3, available at: www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_Global.pdf.

extrajudicial killings".[7] Beyond the data itself, our digital world requires both physical and digital infrastructure. Cyber attacks – in the sense of hostile operations conducted through data streams against computers, computer systems, connected devices or networks – have been increasing year on year, and this has only been amplified during the COVID-19 pandemic.[8] Cyber attacks can target any infrastructure relying on connected networks, with real-world consequences; this can include financial systems, as we will explore later.

How we use money has also changed as a result of digitalization. If I were to ask you how much cash you are carrying in your pocket right now, what would your answer be? One dollar? Ten dollars? Nothing at all? Increasingly, people rely on digital payments – by card, by mobile phone or using internet banking – to pay for the goods and services they need, whether that be paying for groceries, a meal out, rent, or health insurance. Many times, I've seen a look of consternation on a person's face on that (rarer and rarer) occasion where a shopkeeper utters the words, "We don't take cards." It does not follow, however, that cash will cease to exist. Numerous reports by central banks and financial experts, while recognizing the rise of digital payments, note that – to misquote Mark Twain – "reports of the death of cash have been greatly exaggerated".[9]

Though the terminology is likely to change as technology evolves, it is important to understand what is meant by the digitalization of cash, and digital payments, in order to have a common understanding of what we are speaking of, and to be able to analyze the impact of these phenomena on humanitarian action. In essence, we are talking about "digital payments" or "electronic transfers", where money is moved electronically – for example, a bank transfer or mobile money transaction. The Electronic Cash Transfer Learning Action Network (ELAN), which has been a pioneer in the humanitarian sector on the use of digital payments, defines them as a "digital transfer of money or vouchers from the implementing agency to a program participant. E-transfers provide access to cash, goods and/or services through mobile devices, electronic vouchers, or cards (e.g., prepaid, ATM, credit or debit cards)."[10]

7 Siena Anstis, Ron Deibert, Miles Kenyon and John Scott-Railton, "The Dangerous Effects of Unregulated Commercial Spyware", *Citizen Lab*, 24 June 2019, available at: https://citizenlab.ca/2019/06/the-dangerous-effects-of-unregulated-commercial-spyware/.

8 Maggie Miller, "FBI Sees Spike in Cyber Crime Reports during Coronavirus Pandemic", *The Hill*, 16 April 2020, available at: https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic.

9 A 2014 European Central Bank study which focused on cash and non-cash (including digital) payments across seven European countries found that cash is still widely in use, even where many other payment mechanisms exist. Importantly, the study found that use of cash is strongly correlated with demographics and point-of-sale characteristics. While this study looks at industrialized countries, it is important to consider how these results might be extrapolated into the types of contexts that humanitarians work in. See John Bagnall, David Bounie, Kim P. Huynh, Anneke Kosse, Tobias Schmidt, Scott Schuh and Helmut Stix, *Consumer Cash Usage: A Cross-Country Comparison with Payment Diary Survey Data*, Working Paper Series No. 1685, European Central Bank, June 2014.

10 ELAN, "Vocabulary and Usage", available at: www.calpnetwork.org/wp-content/uploads/2020/01/elan-vocab-and-usage-expanded-jan-2017.pdf.

Digital payments should not be confused with digital currencies such as Bitcoin, one of the most popular forms of cryptocurrency. Cryptocurrencies are digital forms of currency created by a public network, rather than any government, so they are not legal tender.[11] There are countries – like Canada – that are considering introducing digital legal tender, thus making paper and metallic currency obsolete.[12] However, a recent study of humanitarian CVA notes that despite the increased interest in distributed ledger technology and digital currency, "real-life application at scale is a long way off".[13]

For the purposes of this article, I will use the term "digital payments" to refer to end-to-end digital transactions. This means that both the payer and payee use an electronic medium of transfer (such as a bank transfer or mobile money transfer) and that the payment instrument (how the payment instructions are carried) is itself digital and not paper-based (i.e., not cash, cheques or money orders).

Of course, digital payments do not mean that no physical currency is involved. For example, a recipient might receive funds into their personal account and then withdraw some or all of the money in cash using an ATM card; or, with mobile money, the funds could be moved to the recipient's digital wallet, and then the person can make digital payments (e.g., an electronic payment in a shop) and can also "cash out" (e.g., withdraw cash from any point of sale).

In general, long gone are the days of humanitarians driving around with a Land Cruiser full of bank notes in order to be able to make payments to a community so that they can cover their needs, whether that entails buying food, clothes and households items, or paying for transport, shelter or health care. While it is true that there are still places where there are no means to transfer money electronically, humanitarians are increasingly disbursing funds digitally – through smart cards or mobile phones, or to people's bank accounts. It is the digitalization of the delivery of cash, and not just the cash itself, that is the game changer. The simple click of a button can put money in the hands of hundreds of thousands – if not millions – of people within minutes, and this is changing decades-old processes, opening the door to faster and more efficient delivery of life-saving assistance.

An evolution of the "do no harm" imperative: The example case of the ICRC

Hand in hand with the increasing use of digital payments comes the need to mitigate potential adverse spillover effects from this digitalization process. While recognizing that there is no such thing as a risk-free world, as a part of our duty of care to affected people, the humanitarian sector needs to think about the impact of its

11 Legal tender is anything recognized by law as a means to settle a public or private debt or meet a financial obligation, including tax payments, contracts, and legal fines or damages.
12 Better Than Cash Alliance (BTCA), "Payments Measurement Toolkit", available at: www.betterthancash.org/tools-research/toolkits/payments-measurement/focusing-your-measurement/introduction.
13 CaLP, above note 2, p. 116.

work, harnessing opportunities but also anticipating and minimizing possible negative impacts. This is where the imperative of "do no harm"[14] plays a crucial role. "Do no harm" requires humanitarian actors to endeavour not to cause further damage and suffering because of their actions.

First coined by Mary B. Anderson, this imperative is fleshed out in the first Protection Principle of the Humanitarian Charter and Minimum Standards in Humanitarian Response.[15] For its part, the ICRC emphasizes the "do no harm" imperative in its Protection Policy,[16] which highlights how it ensures that its actions do not have adverse impacts on, or create new risks for, individuals or populations. Beyond the ICRC, numerous humanitarian organizations have embedded "do no harm" into their work and policies over the decades, including when it comes to digital transformation processes, such as the digitalization of cash. Oxfam was one of the first agencies to develop an explicit policy on data responsibility[17] and has produced toolkits and training for staff to help operationalize data responsibility throughout its programmes.[18] More recently, the United Nations (UN) Office for the Coordination of Humanitarian Affairs (OCHA) Centre for Humanitarian Data's work on data responsibility applies a "do no harm" lens in creating tools and guidance to help staff navigate the technical and ethical aspects of working with humanitarian data, including but not limited to data generated by digital payments.[19]

Examining the digitalization of cash through the framework of "do no harm" – otherwise referred to as "do no *digital* harm" – is crucial as it allows humanitarian organizations to act ethically as we proceed in integrating digital transformations.

"Do no digital harm" is a critical imperative particularly in relation to the way humanitarian organizations and their partners manage data, implement activities and connect with affected people in the digital space. This applies equally to the way we use digital payments to support crisis-affected people. In the case of the ICRC, this means that not only does the organization use cash and vouchers (both physical and digital) in its responses, but it also has a clear understanding of how the digitalization of cash could impact humanitarian action, particularly in situations of armed conflict. The ICRC knows that "it is not enough to understand only the physical environment of armed conflict. It is

14 Mary B. Anderson, *Do No Harm: How Aid Can Support Peace or War*, Lynne Rienner, Boulder, CO, 1999. For a recent foundational text, see Hugo Slim, *Humanitarian Ethics: A Guide to the Morality of Aid in War and Disaster*, Oxford University Press, Oxford, 2015.

15 Sphere Project, *The Sphere Handbook: Humanitarian Charter and Minimum Standards in Humanitarian Response*, 2018, Protection Principle 1, available at: https://handbook.spherestandards.org/en/sphere/#ch004_002_002.

16 ICRC, "ICRC Protection Policy", *International Review of the Red Cross*, Vol. 90, No. 871, 2008, p. 753, available at: www.icrc.org/en/doc/assets/files/other/irrc-871-icrc-protection-policy.pdf.

17 Oxfam, "Responsible Program Data Policy", February 2015, available at: https://policy-practice.oxfam.org.uk/publications/oxfam-responsible-program-data-policy-575950.

18 Oxfam, "Responsible Data Management", 2017, available at: https://policy-practice.oxfam.org.uk/our-approach/toolkits-and-guidelines/responsible-data-management.

19 OCHA, Centre for Humanitarian Data, "Data Responsibility", available at: https://centre.humdata.org/data-responsibility/.

essential to overlay this with readings of the virtual or digital environment."[20] To harness the opportunities that digitalization brings – for cash, but also beyond – the ICRC's implementation of the "do no harm" imperative is centred on ensuring that we keep the people we serve at the centre of our analysis.

CVA supporting people-centred responses

The advantages of CVA are well known: it increases affected people's dignity, power, autonomy and choice in how they manage their survival and recovery.[21] When it comes to putting affected people at the centre of our work, CVA is a critical tool because it puts financial resources in the hands of crisis-affected people so that they can recover, whenever and however they choose. In so doing, it enables affected people to make their own decisions – decisions which may well be different from those a humanitarian organization would make on their behalf. CVA has the potential to be transformative because it starts to change the balance of power between humanitarian agencies and crisis-affected people, as well as the multiple other stakeholders involved in humanitarian responses: donors, governments and civil society. When agencies are well prepared, CVA can be delivered quickly and at scale. Additionally, CVA can provide greater operational flexibility and achieve wider social and economic multiplier effects beyond its specific purpose, compared with in-kind assistance (giving goods directly). This is due to the indirect effects of cash transfers whereby increased expenditure by recipients contributes to income growth for non-recipients, expansion of markets for local goods, and increased demand for services.

Nevertheless, the use of CVA is subject to risks similar to those involved in providing in-kind assistance – market interference, accountability tracking, social tensions, protection issues – and these need to be managed carefully. In this respect, the digitalization of CVA can enhance both the benefits and risks for affected people. This is the focus of this analysis going forward: to highlight how the digitalization of cash is impacting humanitarian action, what the potential risks of the digitalization of cash are, and how we in the humanitarian sector can work to mitigate those risks.

How the digitalization of cash is transforming humanitarian action

However we look at it, digital payments are here to stay – both in the wider society and in humanitarian action. According to an analysis from MasterCard, "the ways

20 ICRC, *Symposium Report: Digital Risks in Situations of Armed Conflict, London, 11–12 December 2018*, Geneva, 2019, p. 1, available at: www.icrc.org/en/publication/4403-symposium-report-digital-risks-armed-conflicts.

21 Overseas Development Institute (ODI), *Doing Cash Differently: How Cash Transfers can Transform Humanitarian Aid. Report of the High Level Panel on Humanitarian Cash Transfers*, London, September 2015.

we pay for things has been changing more in the past 15 years than in the previous 150, and nearly every innovation we have seen has taken share away from cash."[22] Although when looked at from a global perspective, cash remains the most commonly used method of payment, there has been a significant increase in the growth of digital payments, with several countries moving rapidly towards becoming "cashless".

Why digital payments?

This has been mirrored in a shift away from cash payments and towards digital payments in the humanitarian sector. For example, in the International Red Cross and Red Crescent Movement, more than half of all payments to affected people are today made digitally.[23] This is in part because of the general global shift towards digitalization, but also because digital payments, transfers and remittances are considered by many actors, such as the World Bank, as contributing to the G20 goals of broad-based economic growth, financial inclusion and women's economic empowerment.[24] The Better than Cash Alliance (BTCA)[25] examined five main drivers behind the rise in digital payments, and concluded that digital payments bring:

- Cost savings through increased efficiency and speed
- Transparency and security by increasing accountability and tracking, reducing corruption and theft as a result
- Financial inclusion by advancing access to a range of financial services, including savings accounts and insurance products
- Women's economic participation by giving women more control over their financial lives and improving economic opportunities
- Inclusive growth through building the institutions that form the bedrock of an economy and the cumulative effect of cost savings, increased transparency, financial inclusion, and greater women's economic participation.[26]

Additional factors have played a role in the shift towards digital payments, including safety and security concerns, as handling large amounts of cash can be very visible and can put recipients or humanitarian staff delivering the cash at risk of theft or looting – much as can be the case with in-kind assistance. For the recipient, holding money in an account rather than keeping cash under their mattress is generally safer. Another important factor is the recipient's preferences – where

22 Hugh Thomas, "Measuring Progress towards a Cashless Society", MasterCard Advisors, available at: https://newsroom.mastercard.com/wp-content/uploads/2014/08/MasterCardAdvisors-CashlessSociety-July-20146.pdf.

23 See the Cash Hub interactive cash maps, available at: www.cash-hub.org/resources/cash-maps.

24 Leora Klapper and Dorothe Singer, *The Opportunities of Digitizing Payments*, World Bank, Washington, DC, 28 August 2015, p. 91.

25 The BTCA is a partnership of seventy-five governments, companies and international organizations intended to accelerate the "transition from cash to digital payments in order to reduce poverty and drive inclusive growth". See the BTCA website, available at: www.betterthancash.org.

26 BTCA, "Why Digital Payments?", available at: www.betterthancash.org/why-digital-payments.

people already use digital payments in their daily lives, it makes sense to use the same mechanisms that they are familiar and comfortable with.

At the time of writing, almost a year into the COVID-19 pandemic, a new driver can potentially be added: the perception that digital payments decrease the risk of virus transmission. Although it has been concluded in previous studies looking at influenza that "handling banknotes and coins is not practically avoidable and will confer no discernible increased risk compared with handling almost any other communal object used in daily life",[27] there has been a general preference for digital payments during the COVID-19 pandemic. Digital payments, such as mobile money transactions or using debit or credit cards, require less handling than physical currency. Additionally, the hardware involved (cards, mobile phones, point-of-sale devices etc.) can be regularly cleaned with a simple disinfectant. A guidance note on CVA and health during COVID-19 issued by the World Health Organization (WHO) and the Global Health Cluster emphasized the preference for digital payments, which reduce the need for people to gather at distribution points and allow for regular disinfection of surfaces such as ATM keypads, noting that "where this is possible, contact-less electronic or mobile payments should be the preferred option to reduce the risk of transmission".[28]

How humanitarians have embraced digital payments

Although different humanitarian organizations have used cash assistance over the decades, it was the formation of the Cash Learning Partnership (CaLP) in 2005, to promote and improve CVA across the humanitarian sector, which first structured the conversation around CVA, and with it, digital payments. By the early 2010s, and with increasing evidence of the effectiveness of CVA behind us, there was a convergence, and several collaborative initiatives emerged. The BTCA, which launched in 2012 in response to public and private sector demand, continues to provide strategic advocacy, research and guidance on how to transition to electronic payments. 2016 saw the launch of the ELAN, and during a four-year project this network produced numerous valuable resources for practitioners, hosted learning events, and contributed to growth and foresight in the humanitarian sector's work on digital payments. This period also saw a significant investment by the world's largest humanitarian network, the International Red Cross and Red Crescent Movement, in building its capacity to

27 European Centre for Disease Prevention and Control, *Technical Report of the Scientific Panel on Influenza in Reply to Eight Questions concerning Avian Flu*, Stockholm, 5 June 2006, p. 26, available at: www.ecdc.europa.eu/sites/default/files/media/en/publications/Publications/0606_TER_Eight_Questions_Concerning_Avian_Flu.pdf.

28 WHO and the Global Health Cluster, *Guidance Note on the Role of Cash and Voucher Assistance to Reduce Financial Barriers in the Response to the COVID-19 Pandemic, in Countries Targeted by the Global Humanitarian Response Plan COVID-19*, Geneva, April 2020, p. 8, available at: www.who.int/health-cluster/about/work/task-teams/Guidance-note-CVA-COVID.pdf?ua=1.

deliver CVA,[29] with the majority of its payments being made digitally. Such approaches require a level of interoperability between the various humanitarian agencies carrying out this work, which means in terms of risk-benefit analysis, the entire humanitarian sector is affected by the use of digital payments in its operations.

As outlined above, digital payments are becoming more and more prominent in the humanitarian sector. However, this raises the question: what are the risks and benefits of this facet of digital transformation? In the following section, I will address this question by outlining how the ICRC analyzes when to use digital payments.

How the ICRC uses digital payments in armed conflict and other situations of violence

Like many others within the humanitarian sector, the ICRC has embraced the use of both physical and digital payments, based on a thorough analysis of the risks and benefits for people affected by armed conflict and other situations of violence. As will be highlighted in the following sections, not only has the ICRC been using CVA for over 100 years, but the organization also has a critical focus on digital risk and data protection.[30] Thus, the ICRC's work can serve as an example of how to examine digital risks in CVA.

A dip into the ICRC's archives shows that it was already using cash transfers during the First World War, when its International Prisoners of War Agency was in charge of processing money orders and forwarding registered letters, including money, sent to interned civilians and prisoners of war by their families.[31] Today, the ICRC uses CVA in the majority of its eighty-plus operations, and its experience demonstrates that it is possible to use CVA in armed conflicts and other situations of violence.[32] From 2012 to 2020, the ICRC has seen a 600% increase in the number of people reached with CVA across its programmes, ranging from small cash-in-hand transfers to help families pay for transport costs to visit detained relatives, to larger grants for rebuilding homes or starting income-generation activities. During this time there has been a huge increase in digital payments, with most large-scale transfers – those to large numbers of people – being made digitally.

The choice between (physical) cash payments or digital payments is made very pragmatically by ICRC teams, based on what resources and services are available in a given country. In South Sudan, for example, where there are extremely limited means of digital payments, small-scale payments – for example, to help a separated person pay for transport to be reunited with their family – are

29 International Red Cross and Red Crescent Movement, *Cash Transfer Programming: Guidelines for Mainstreaming and Preparedness*, Geneva, 2015, available at: https://cash-hub.org/wp-content/uploads/sites/3/2020/10/Cash-Transfer-Programming-Guidelines-for-Mainstreaming-and-Preparedness.pdf.

30 See "Q&A: Humanitarian Operations, the Spread of Harmful Information and Data Protection", in this issue of the *Review*.

31 ICRC, *L'agence internationale des prisoners de guerre, Genève, 1914–1918*, Geneva, 1919, p. 105.

32 ICRC, above note 4, p. 7.

made in cash directly to the affected person. Compare this to Somalia, where the ICRC makes most of its payments digitally as the population have long been using mobile money. The ICRC asks itself what payment instruments people are familiar with, which ones they have access to, which will be fast, efficient and safe for affected people and for ICRC staff alike. This sometimes means using multiple payment methods in one country. For example, in the Democratic Republic of the Congo, the ICRC uses three: cash payments directly to people, digital payments via mobile money, and digital payments via personal accounts held with cooperatives.

Of course, it is not a choice between digital payments or no payments at all; cash remains a valid payment instrument in many cases. In Ukraine, to accompany its work supporting families with the search for missing persons, strengthening the authorities' capabilities to conduct the search according to international standards, and providing psychosocial, legal and administrative support to families, the ICRC also provided monthly payments to enable the families to better meet their basic needs. These payments were made in cash directly to the families by ICRC staff, in part because this gave the staff a practical reason to visit the families regularly. ICRC staff noted that they would not feel comfortable visiting the families every month if they had no new information about the missing person, whereas making the cash payments provided a reason to visit. The team considered that with digital payments, this vital contact would have been much less frequent and the relationships – and trust – with the families may have taken longer to build.

What are the risks of digital payments in humanitarian action?

Understanding the possible risks and potential pitfalls of digital payments in humanitarian settings and taking steps to mitigate them is a core part of the critical broader work of redefining what the "do no harm" principle means in our increasingly digitalized world. In fact, digital payments have already mitigated some of the traditionally perceived risks of CVA: evaluations of programmes using digital payments have shown that these programmes have reduced theft, reduced risks for staff in transporting money, and proved popular with recipients due to the privacy they afford.[33] However, it is important to start with the understanding that it is impossible to eliminate all risk; the risks in using digital payments can never be entirely avoided, only mitigated. Risk is a part of daily life – we take a risk just crossing the road in the morning. Humanitarian organizations must weigh the benefits to the recipient (as well as the organization) of the speed and efficiency of digital payments, versus the potential risks explored below. Therefore, risk assessment remains vital: allowing the identification and analysis of risks, understanding which can be mitigated and which cannot, putting relevant

33 Laura Gordon, *Risk and Humanitarian Cash Transfer Programming: Background Note for the High Level Panel on Humanitarian Cash Transfers*, ODI, London, May 2015, available at: www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9727.pdf.

measures in place, and documenting these decisions, thus also improving accountability and promoting learning.

Digital payments are not universally accessible.

We must start this examination of "do no digital harm" with a focus on the affected people themselves. The fact is, digital payments are not accessible to everyone in the same way that cash is, and the increase in digital payments may deepen the "digital divide" (defined as inequality in access to technology and its associated benefits). Any person can use cash if they can get their hands on it, and providing the goods and services they need to pay for are available. For the recipient, cash does not require any formal identification or any physical infrastructure. Cash is not linked to the person, and as such does not discriminate or identify.[34] It simply requires the coins or notes that are the means of exchange, and a basic level of numeracy.[35] However, to use digital payments, the recipient will require a level of digital and financial literacy. It is estimated that only one in three adults globally shows an understanding of basic financial concepts, and that there are lower standards of financial literacy amongst women and the poor.[36] The recipient will also require a personal account with a financial service provider and will be subject to Know Your Customer (KYC)[37] regulations set globally by the Financial Action Task Force (FATF), transposed into national law by States and applied by every commercial service provider. While the FATF requires "identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information",[38] most States transpose this to mean a legally accepted form of identification such as a passport, birth certificate or national identity card. According to the World Bank, an estimated 1 billion people – that is, 13% of the world's population – do not have an official proof of identity.[39] Some 91% of these live in low-income or lower middle-income

34 AGIS Consulting, *Cash Essentials: Beyond Payments*, Paris, 2015, available at: https://cashessentials.org/?ref=xranks.

35 It has been argued that cash is the preferred means for criminal activities seeking to avoid detection. However, digitalization is changing this, with reports that "electronic money laundering, also known as Transaction Laundering, is the most common, but least enforced, method of money laundering". Ron Teicher, "Transaction Laundering – Money Laundering Goes Electronic in the 21st Century", *Finextra*, 4 June 2018, available at: www.finextra.com/blogposting/15423/transaction-laundering—money-laundering-goes-electronic-in-the-21st-century.

36 Leora Klapper, Annamaria Lusardi and Peter van Oudhuesden, *Financial Literacy around the world: Insights from Standard & Poor's Ratings Services Global Financial Literacy Study*, 2015, available at: https://gflec.org/wp-content/uploads/2015/11/3313-Finlit_Report_FINAL-5.11.16.pdf?x28148.

37 KYC is a process enabling businesses to check the identity of their customers in order to comply with regulations and legislation on money laundering and corruption, and includes collecting information from the customer such as name, identity document number, phone number and address. PwC, *Know Your Customer: Quick Reference Guide*, January 2016, available at: www.pwc.lu/en/anti-money-laundering/docs/pwc-kyc-qrg-final-interactive-2016.pdf.

38 FATF, "FATF Recommendation 5: Customer Due Diligence and Record-Keeping", available at: www.un.org/sc/ctc/wp-content/uploads/2016/03/fatf-rec05.pdf.

39 World Bank, "ID4D Data: Global Identification Challenge by the Numbers", available at: https://id4d.worldbank.org/global-dataset.

countries, and among these, one in two are women in low-income countries.[40] There are many reasons why people do not have an official proof of identity, including low levels of literacy, the often high costs of official documents (which are a barrier for the poorest), legal requirements that vary for different sections of the population in a given country, absence or paucity of national identity management systems or lack of resources committed to ensuring that all citizens are registered, or simply that it is not common practice in a community to register with the authorities. These issues are often exacerbated by armed conflict and other situations of violence, where State services may be disrupted and shifting frontlines inhibit movement of people and change geographical boundaries, sometimes leaving people living in territories where their identity documents are no longer recognized as valid.

Of course, if communities have no access to digital payments, humanitarians can choose to provide cash payments, vouchers, in-kind assistance or services. The problem arises when most of a population do have access, leading agencies to choose digital payments and thus resulting in the possible – albeit unintentional – exclusion of those groups without access. Humanitarians must always have the flexibility to offer a variety of solutions, in order to ensure that no one is left behind.

Digital payments are often promoted based on the concept that they drive financial inclusion; however, financial inclusion does not necessarily translate to financial well-being. Clear links have been established between increased financial inclusion, poverty reduction and economic security, but it is not as simple as ensuring that people have access to financial services. A 2017 study conducted by the ICRC and the British Red Cross in Nigeria and Kenya found that, in these contexts, "people's main problem remains poverty and not financial inclusion".[41] The provision of digital payment options will not, in and of itself, automatically lead to financial inclusion.

The increased focus on linking humanitarian cash assistance to social protection adds governments – the main providers of social protection systems – into the mix, bringing complicated protection and coordination concerns. This focus is only increasing due to the COVID-19 pandemic and the predicted global economic depression, which will stretch existing governmental social protection and humanitarian aid systems to the limits of their capacities and beyond. However, making these links is not a straightforward matter; the findings of a recent practitioner survey[42] show that the main perceived challenges of linking CVA with social protection systems remain a lack of coordination between actors, the fact that social protection systems are not designed to be shock-

40 Vyjyanti T. Desai, Anna Diofasi and Jing Lu, "The Global Identification Challenge: Who Are the 1 Billion People without Proof of Identity?", *Voices: World Bank Blogs*, 25 April 2018, available at: https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity.

41 Paul Harvey, Kokoévi Sossouvi and Annie Hurlstone, *Humanitarian Cash and Financial Inclusion: Findings from Red Cross Movement Projects in Kenya and Nigeria*, British Red Cross and ICRC, London, February 2018, p. 6.

42 CaLP, above note 2, p. 144.

responsive, lack of experience of humanitarians in social protection, and that governments are not perceived as impartial in addressing the needs of the most vulnerable. As the UN has noted:

> Many laws that formally restricted access to social protection and public services to certain population groups have been repealed. Nevertheless, discrimination continues to reinforce some of the barriers they face, including a lack of information on entitlements or the political voice or representation necessary to claim such entitlements.[43]

These exclusions can be exacerbated in times of crisis, and particularly in conflict. In contexts where the rule of law is weak and corruption is endemic, certain people and groups will benefit – and some will suffer – from the changes to the economic model brought about by conflict. Humanitarians have a role to ensure that marginalized groups and those that face protection risks are supported, whether that be through existing systems or through humanitarian protection and assistance activities.

There is also a risk of conflating digital and physical proximity. Digital payments may allow vital assistance to be provided to communities remotely, but this does not mean that humanitarians do not need to be present in communities; field teams still need to conduct assessments in order to get a true picture of needs and then follow these up with monitoring and evaluation to gauge the impact of interventions on the affected communities. Digital proximity – for example, through digital payments – "does not replace the need for physical access to vulnerable communities nor can it replace wider efforts to ensure they enjoy protection under relevant laws".[44]

Data responsibility in humanitarian action

To ensure inclusion in digital payments, humanitarian organizations must collect and process an enormous amount of data, including the personal data of affected people who wish to access those payments. Whether using a "closed loop" system managed entirely by the humanitarian agency, or working through local financial service providers, this data must be securely collected, managed, stored and shared in line with good data management practices.

CaLP's 2020 *State of the World's Cash* report highlights that "digital risk and data management is a 'newly emerged risk'" and notes that "whilst some large operational CVA actors (by their own admission) are now on top of responsible data management, many CVA practitioners still find this a paralysing topic".[45]

43 UN, *Promoting Inclusion through Social Protection: Report on the World Social Situation 2018*, New York, 2018, p. 18, available at: www.un.org/development/desa/dspd/wp-content/uploads/sites/22/2018/07/1-1.pdf.
44 ICRC, above note 4, p. 9.
45 CaLP, above note 2, p. 52.

A series of events in 2019,[46] some focusing specifically on CVA and others on humanitarian action more broadly, explored digital risks and the concepts of "do no digital harm" and "digital dignity" as part of the digital transformation of humanitarian action. Several themes emerge when examining digital risks in humanitarian action, and more specifically the risks associated with digital payments, but fundamentally they are all rooted in the core topic of data responsibility, "a set of principles, processes and tools that support the safe, ethical and effective management of data in humanitarian response. This includes data privacy, protection, and security, as well as other practical measures to mitigate risk and prevent harm."[47] Data responsibility requires humanitarians to collect, manage, store and share data conscientiously.

The issue of data responsibility is frequently raised when aiming for collaboration between humanitarian agencies. There have been several initiatives related to improving collaboration for delivery of CVA, including the Collaborative Cash Delivery Network[48] and the UN common cash system.[49] Such collaborative approaches have been broadly welcomed in the spirit of fostering greater collaboration, in line with Grand Bargain[50] commitments to increase the effectiveness, efficiency and accountability of CVA operations and provide better support to those affected by crises.[51] However, they have experienced various challenges. Questions have been raised around intellectual property rights in co-created systems, the complexity of data interoperability, and issues of power and resource control between different agencies. Lack of data interoperability and data sharing between agencies that are using collaborative platforms is a significant impediment to programme quality, contributing to delays in programming and meaning that use of information cannot be maximized. Data sharing requires trust in each other's systems and data management and protection practices. In February 2019, the World Food Programme (WFP) and data analytics and

46 The ICRC convened a symposium on "Digital Risks in Armed Conflicts" in December 2018 in London: see ICRC, above note 20. CaLP convened a data responsibility workshop in April 2019 in Geneva: see CaLP, "Data Responsibility: Let's Not Wait for Another Wake-Up Call", 8 May 2019, available at: www.calpnetwork.org/blog/data-responsibility-lets-not-wait-for-another-wake-up-call/. Findings from the CaLP workshop were taken into a first meeting on "Data Responsibility in Humanitarian Action" convened by the OCHA Centre for Humanitarian Data, in collaboration with Wilton Park, in May 2019: see Wilton Park, "Data Responsibility in Humanitarian Action: From Principle to Practice", available at: www.wiltonpark.org.uk/event/wp1688/. A second Wilton Park event in October 2019 focused more broadly on "Digital Dignity in Armed Conflict": see Wilton Park, *Digital Dignity in Armed Conflict: A Roadmap for Principled Humanitarian Action in the Age of Digital Transformation*, October 2019, available at: www.wiltonpark.org.uk/wp-content/uploads/WP1698-Report.pdf.

47 Wilton Park, *Data Responsibility in Humanitarian Action: From Principle to Practice*, June 2019, available at: www.wiltonpark.org.uk/wp-content/uploads/WP1688-Report-1.pdf.

48 See Collaborative Cash Delivery Network, "Our Story", available at: www.collaborativecash.org/the-network.

49 See Inter-Agency Standing Committee (IASC), "Statement from the Principals of OCHA, UNHCR, WFP, and UNICEF on Cash Assistance", 5 December 2018, available at: https://interagencystandingcommittee.org/other/content/statement-principals-ocha-unhcr-wfp-and-unicef-cash-assistance-5-december-2018.

50 See the official Grand Bargain website, available at: https://interagencystandingcommittee.org/grand-bargain.

51 IASC, "Increase the Use and Coordination of Cash-Based Programming", available at: https://interagencystandingcommittee.org/increase-the-use-and-coordination-of-cash-based-programming.

intelligence-gathering firm Palantir Technologies signed a $45 million partnership, attracting criticism

> from human rights and data transparency advocates, who argued that Palantir has facilitated rights abuses through its previous work with organisations including the Central Intelligence Agency (CIA), Immigration and Customs Enforcement (ICE) and Cambridge Analytica. … They argued that, in the name of increased efficiency and cost savings, the highly sensitive data of the 92 million people served annually by the WFP was being put at risk.[52]

The partnership raised questions about the implications for the UN common cash system and how data collected by any organization participating will be protected, along with how this could impact the affected people that the system seeks to serve.

The rise of digital identities and the use of biometrics

Technology-assisted innovation in digital identity has increased in recent years and is often used in programmes providing CVA. But what is digital identity?

> A digital identity is a collection of electronically captured and stored identity attributes that uniquely describe a person …. A person's digital identity may be composed of a variety of attributes, including biographic data (e.g., name, age, gender, address) and biometric data (e.g., fingerprints, iris scans, hand prints) as well as other attributes …. [These data] can be used to identify a person by answering the question "who are you?"[53]

Combined with other credentials, they can also answer the question, "Are you who you claim to be?"

A digital identity is not automatically an official or legal proof of identity; only governments can provide legal identification to citizens, although many are choosing to do so digitally. In Estonia, seen as the world leader in digital integration, it is mandatory for every Estonian citizen above the age of 15, and every European citizen residing in Estonia, to obtain the Estonian digital identity card.[54] India has the world's single largest biometric-based digital identification system, called Aadhaar.[55]

The digital identities created by humanitarian organizations, enabling people to have access to their programmes, are therefore not official legal identities, and as such have limited use beyond their specified purpose, unless negotiated with the relevant authorities (such as in the case of refugee ID cards

52 Barnaby Willitts-King, John Bryant and Kerrie Holloway, *The Humanitarian "Digital Divide"*, Humanitarian Policy Group Working Paper, ODI, London, November 2019, p. 15.

53 World Bank Group, GSMA and Secure Identity Alliance, *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*, July 2016, available at: www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/07/Towards-Shared-Principles-for-Public-and-Private-Sector-Cooperation.pdf.

54 World Bank Group, *Privacy by Design: Current Practices in Estonia, India, and Austria*, Washington, DC, 2018, available at: https://id4d.worldbank.org/sites/id4d.worldbank.org/files/PrivacyByDesign_112918web.pdf.

55 *Ibid.*

issued by the Office of the UN High Commissioner for Refugees (UNHCR), which provide access to services beyond those provided by the UNHCR, including financial services in some cases[56]). The creation of digital identities also raises the question of ownership of those identities. The 2019 Wilton Park conference on "Digital Dignity in Armed Conflict" concluded that "to promote digital dignity, individuals who receive aid should be perceived as data agents who have agency over their digital identity and digital anonymity".[57] There could be significant risks in creating interoperable systems and identity frameworks for vulnerable groups, who may have very good reasons for wishing to remain anonymous, and who could face discrimination or worse by virtue of their being identifiable.

Biometrics are one such form of digital identity. Biometrics were primarily developed and deployed for the purposes of border and migration control, and were then widely deployed in updated national identity systems. It is the drive for legal identity meeting due diligence requirements that makes biometrics so attractive, because they cover both needs. However, this blurring of the boundaries between immigration control and counterterrorism or security makes biometrics collected by private actors and humanitarian organizations particularly interesting for States.[58]

The use of biometric identification systems by humanitarian organizations to support digital identity has significantly increased, due to the perception that they bring efficiency and accountability to operations, in particular with regard to reducing fraud.[59] However, this rapid uptake of biometrics has caused much debate. The early use of biometrics by the UNHCR was seen as a success story, but a UN internal audit in 2016 found that in four out of five country operations reviewed, the information being given to refugees about the biometric programme was insufficient for them to be properly informed. [60] As an example, in response to the Rohingya refugee crisis, biometrics enabled the UNHCR and its partners to cope with a crisis of enormous scale and speed, but some have argued that this has created risks for the Rohingya refugees:

> The biometric data which humanitarian agencies and the government have been collecting is not only being used to distribute aid to the Rohingya people; it is also being used to control their movements. … The fear for the

56 UNHCR, "Documentation", available at: www.unhcr.org/registration-guidance/chapter5/documentation/.
57 Wilton Park, *Digital Dignity in Armed Conflict*, above note 46, p. 4.
58 UN Security Council Resolution 2396 requires all States to use "biometric data, which could include fingerprints, photographs, facial recognition, and other relevant identifying biometric data, in order to responsibly and properly identify terrorists, including foreign terrorist fighters". See UNSC Res. 2396, 21 December 2017, available at: http://unscr.com/en/resolutions/doc/2396; Fionnuala Ní Aoláin, "The UN Security Council, Global Watch Lists, Biometrics, and the Threat to the Rule of Law", *Just Security*, 17 January 2018, available at: www.justsecurity.org/51075/security-council-global-watch-lists-biometrics/.
59 The Engine Room and Oxfam, *Biometrics in the Humanitarian Sector*, March 2018, p. 8, available at: www.theengineroom.org/biometric-tech-review-report/.
60 Elsie Thomas, "Tagged, Tracked and in Danger: How the Rohingya Got Caught in the UN's Risky Biometric Database", *Wired*, 12 March 2018, available at: www.wired.co.uk/article/united-nations-refugees-biometric-database-rohingya-myanmar-bangladesh.

> Rohingya is that this biometrically-enabled control system could be used to send them back to Myanmar.[61]

Taking a measured approach, in 2015 Oxfam imposed a moratorium on the use of biometrics in its work,[62] later stating that "given the number of unknowns … we felt it was best not to become an early adopter".[63] The ICRC has long used biometrics, but only to support the implementation of its mandate where particular objectives cannot be realized without using them, for example in forensics and the restoration of family links: "In this case the ICRC processes the biometric data as a matter of 'public interest' (in the implementation of the ICRC's mandate)."[64] When it comes to using biometrics for beneficiary management and assistance distribution, the ICRC's stance differs:

> Because the purpose here is primarily linked to efficiency, and insofar as aid can be (and long has been) distributed without the need for biometrics, the ICRC would have to establish that the "legitimate interest" it has in establishing any biometric identity management system does not outweigh the potential impact on the rights and freedoms of the individuals concerned.[65]

While the use of biometrics is increasing in daily life – fingerprint scans are promoted as an easy way to secure your smartphone, for example – it can still be possible to "opt out". However, increasingly in humanitarian programming, this possibility is somewhat theoretical, as proving your identity is linked to assistance delivery. Biometrics in and of themselves are not inherently risky, but as we will explore below, the processing of any personal data is sensitive and subject to various risks and concerns.

Data protection: Protecting life, integrity and dignity

The risks highlighted so far have the issue of identity at their core: how do people prove who they are, who owns that identity, and what is done with the identity data that people provide? Directly related to the issue of identity is that of data protection. Anyone with an email account will remember the introduction of the European Union's General Data Protection Regulation, which became enforceable in May 2018, and with it the flood of emails asking us to give our consent to our data being used. Who among us ever reads the reams of pages of terms and conditions before shopping online or downloading an application on our smartphones? People give away their data freely all the time without necessarily considering the implications, the desire for convenience and connectivity often overriding the potential risks, even when their trust in

61 *Ibid.*
62 The Engine Room and Oxfam, above note 59.
63 E. Thomas, above note 60.
64 Ben Hayes and Massimo Marelli, "Facilitating Innovation, Ensuring Protection: The ICRC Biometrics Policy", *Humanitarian Law and Policy Blog*, 18 October 2019, available at: https://blogs.icrc.org/law-and-policy/2019/10/18/innovation-protection-icrc-biometrics-policy/.
65 *Ibid.*

companies or governments is low. For example, despite initial concerns after the Facebook/Cambridge Analytica privacy scandal,[66] and with very little actual improvement to privacy for its users, Facebook's user numbers continue to climb, with a 12% rise year on year.[67]

Protecting individuals' personal data is an essential part of protecting their life, integrity and dignity, which makes the protection of personal data of fundamental importance for humanitarian organizations. Humanitarians frequently collect personal data in order to carry out their mandate, whether that be to trace missing people, to help reunite separated families or to provide life-saving assistance. When it comes to digital payments, data protection is a critical issue because in order to make or receive payments through a financial service provider, recipients must identify themselves, and humanitarian organizations must therefore collect and share people's personal data. As new technologies allow for exponentially faster and easier processing of this data, there are increasing concerns about privacy. While the right to privacy has been recognized globally as a human right since 1948,[68] the right to have one's personal data protected is more recent, with the first regional data protection treaty entering into force almost forty years later.[69] Today, a majority of States, the UN and international organizations with a humanitarian mandate recognize core data protection principles, even if the content of policies and scope of legislation varies across the world.[70] However, the very circumstances within which humanitarian organizations operate – crisis situations – create unique challenges regarding data protection.

For humanitarians, obtaining the consent of recipients for the processing of their personal data is one of the first challenges. In the context of data protection, consent means the freely given, specific and informed indication of a data subject's (i.e., the recipient's) wishes by which they signify agreement to personal data relating to themselves being processed. This means that "the individual must be put in a position to fully appreciate the risks and benefits of data Processing, otherwise Consent may not be considered valid".[71] Using consent as a legal basis for data processing differs from the way the humanitarian sector has traditionally

66 Julia Carrie Wong, "The Cambridge Analytica Scandal Changed the World – but It Didn't Change Facebook", *The Guardian*, 18 March 2019, available at: www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook.

67 Dan Noyes, "The Top 20 Valuable Facebook Statistics", Zephoria, October 2020, available at: https://zephoria.com/top-15-valuable-facebook-statistics/.

68 See Universal Declaration of Human Rights, UN Doc. 217 A (III), 10 December 1948, Art. 12; International Covenant on Civil and Political Rights, 999 UNTS 171, 16 December 1966 (entered into force 23 March 1976), Art. 17.

69 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, 28 January 1981 (entered into force 1 October 1985), available at: www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

70 United Nations Conference on Trade and Development, "Data Protection and Privacy Legislation Worldwide", available at: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

71 Christopher Kuner and Massimo Marelli (eds), *Handbook on Data Protection in Humanitarian Action*, 2nd ed., ICRC and Brussels Privacy Hub, Geneva, June 2020, p. 51, available at: www.icrc.org/en/data-protection-humanitarian-action-handbook.

used consent as a basis for its humanitarian responses. Data processing by humanitarian organizations – including the ICRC – is often "based on vital interest or on important grounds of public interest, for example in the performance of a mandate established under national or international law".[72] This means that consent does not have to be valid for data processing to go ahead, provided that the processing is being carried out on the legal basis of "public interest".

However, we must recognize that the very concept of freely given consent in a crisis is a misnomer, particularly if consenting to the processing of personal data is a precondition for receiving assistance. If you had lost everything and someone was offering to help you, you would likely accept that help with very few questions asked and would pay very little heed to complex legal questions about what might happen to your data and what the potential future risks may or may not be. Ensuring informed consent is also a challenge when data protection policies include complex legal concepts which many of us would struggle to understand, regardless of levels of literacy and education. One of the key recommendations from the 2019 Wilton Park conference was that:

> The notion of informed consent should be reformulated as meaningful consent, addressing coercive consent practices. Alternatives to the current framework of informed consent should provide an opt-out for people who choose not to provide information. This should not prevent access to services. An opt out will shift the power dynamic and go some way to addressing the relationship imbalance.[73]

Of course, data protection is important across the full spectrum of humanitarian work, but it has a particular resonance when it comes to digital payments. The use of digital payments requires humanitarians to outsource part of their supply chain, which can be positive in terms of efficiency and accessing specific expertise, but also requires giving up a level of control in terms of the management of data. The very nature of digital payments requires sharing of data with a third party – the financial service provider who will facilitate the digital payment. Once transferred, the data is therefore no longer under the humanitarian organization's control.

Key concerns relating to data protection arise when using digital payments through financial service providers, who are bound by national legislation implementing FATF recommendations.[74] Concerns include the use of data by authorities for law enforcement purposes, including surveillance and profiling of individuals, and the use of personal data for commercial purposes, such as service providers offering targeted services or advertisements, or profiling customers for

72 *Ibid.*, p. 60.
73 Wilton Park, *Digital Dignity in Armed Conflict*, above note 46.
74 It is important to note that FATF recommendations do require data retention, access for law enforcement, the establishment of financial intelligence units, the submission of suspicious financial transaction reports, etc. See FATF, *The FATF Recommendations*, February 2012 (updated October 2020), available at: www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html.

creditworthiness. Data may also be used to cross-check people against master lists of customer debts, potentially leading to the financial institution directly deducting sums owed from the humanitarian assistance a person is set to receive. There are times when data protection concerns mean that digital payments are not appropriate, even if they are available. This is particularly common in conflict environments and other sensitive settings, where the choice of financial service providers is often limited and tends towards control by one particular party to the conflict.[75]

In many cases, people already have a relationship with a financial service provider, such as a bank or a mobile money operator; these individuals have already accepted and fulfilled the necessary requirements (including KYC) to access the service, and as such accept the benefits and risks that come with this. While this does not absolve humanitarians of their responsibility to undertake the necessary due diligence, there is a difference between, on the one hand, leveraging an existing financial relationship that a recipient has, and, on the other, asking someone to commence a new financial relationship for the sole purpose of receiving assistance through digital payments.

While the risks to individuals are critically important, there is a second layer of risk. We cannot ignore the fact that the personal data collected by humanitarians may be accessed by authorities, via financial service providers, and used for law enforcement purposes, which can have potential risks for wider humanitarian action. As the ICRC has observed:

> These risks are not limited to individuals. Humanitarian organizations can also face such risks. If data generated by a humanitarian organization are then used for non-humanitarian purposes, whether law enforcement or commercial, the neutrality and independence of humanitarian action could be affected. A humanitarian organization may then be perceived as supporting one party to a conflict by providing data that could lead to security risks for the organization and/or loss of access to the population of concern.[76]

Both outcomes could eventually lead to a reduction in essential humanitarian services for the affected population.

Beyond the legitimate and legal use of data, the data collected, stored, shared and analyzed by humanitarian agencies can be valuable to parties to the conflict. Data which identify people, their locations, their networks and their connections can be used with malicious intent by individuals, groups or organizations. It is not only the data that we commonly understand as personal data (e.g. name, phone number) but also the often overlooked metadata – data that provides information about other data – which is a mine of information, for those who know how to use it. General Hayden, former director of the US National Security Agency and Central Intelligence Agency, articulated this most

75 ICRC, above note 4, p. 50.
76 *Ibid.*, p. 51.

clearly when he said "[w]e kill people based on metadata",[77] highlighting how metadata is used to make life-and-death decisions. In an age of increased surveillance, the protection risks for people of concern are clear: "[e]ven though software typically can't kill people directly in the way that bullets can, the end result is often the same".[78] Metadata has always existed – for example, the information contained on the outside of a letter which says nothing of its content but still provides information on the sender and recipient. However, with digital information flows and transactions – whether financial or of any other type – the quantities of metadata generated are huge. For example, the volume of metadata generated by mobile money transactions is immense. The issue is not simply the volume of this metadata but rather what can be inferred by it, including what social groups people belong to (if a particular group was targeted for assistance), where they may have moved after the crisis, and their "network of family or friends, based on transfers received or made that didn't involve the humanitarian organisation. Information can then be inferred about these individuals in turn, even though they were not directly involved" in the programme.[79]

The way in which metadata can be used for good while simultaneously eroding the privacy of the individual has been very clearly highlighted by the rapid development of contact tracing apps during the COVID-19 pandemic, many of which require users to upload personal information and to agree to their location being tracked and shared using different types of geolocation technology. As of July 2020, close to fifty countries were developing or had rolled out contact tracing apps to help fight the spread of the disease.[80] While some countries, such as South Korea, have credited the use of contact apps with "flattening the curve" of the disease, helping to bring the outbreak under control, there are real privacy concerns being raised. An analysis of COVID-related apps by Privacy International exposed some of the risks of adopting these technologies, not least that "apps are notorious for their lack of security and privacy safeguards, exploiting people's data and devices".[81] While billions of people around the world have accepted restrictions on their day-to-day life in the service of bringing the pandemic under control, there will be limits; now people are "being asked to trust governments with their proposed apps – of which there are many. These are the very same governments who have been keen to exploit data in the past."[82]

77 David Cole, "'We Kill People Based on Metadata'", *New York Review of Books*, 10 May 2014, available at: www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/. And see Johns Hopkins University, "The Price of Privacy: Re-Evaluating the NSA", Johns Hopkins Foreign Affairs Symposium, 2014, available at: www.youtube.com/watch?time_continue=1022&v=kV2HDM86XgI.

78 Ron Deibert, Citizen Lab, quoted in Stephanie Kirchgaessner, "'Cat and Mouse Game': How Citizen Lab Shone a Spotlight on Israeli Spyware Firm", *The Guardian*, 12 May 2020, available at: www.theguardian.com/world/2020/may/12/cat-and-mouse-game-how-citizen-lab-shone-a-spotlight-on-israeli-spyware-firm-nso.

79 ICRC and Privacy International, *The Humanitarian Metadata Problem: "Doing No Harm" in the Digital Era*, Geneva, October 2018, p. 74.

80 Niall McCarthy, "Which Countries Are Deploying Coronavirus Tracing Apps?", *Forbes*, 22 July 2020, available at: https://tinyurl.com/j8wse55q.

81 Privacy International, "There's an App for That: Coronavirus Apps", 20 April 2020, available at: https://privacyinternational.org/long-read/3675/theres-app-coronavirus-apps.

Reducing privacy standards in an emergency could be the start of a slippery slope; once standards have dropped, it can be difficult to raise them again.

Cyber security and the increase in cyber attacks

Digital payments also require an infrastructure, both digital and physical. Payments infrastructure requires computers and servers, which must physically be based somewhere and which require energy to run and resources to maintain. Infrastructure can break down, and it can also be damaged, particularly in situations of armed conflict.[83] If the electricity fails or the "computers are down", the economy may come to a standstill. In 2018, a massive outage of the Visa payment system left millions in Europe unable to make payments.[84] The same happened to MasterCard a few weeks later, disrupting digital payments globally.[85] A statement from Visa said the issue was not associated with any unauthorized access or cyber attack, but this is a real risk when it comes to critical infrastructure, and alongside health, water, energy and transport infrastructure, financial infrastructure is indeed critical. In 2019, financial services firms reported huge year-on-year increases in the number of cyber attacks, breaches and data thefts, with 25% of all malware attacks being made against financial services organizations, more than any of the other twenty-seven industries monitored.[86] The COVID-19 pandemic is likely to push more and more financial institutions to become fully digital, and with this increasing reliance on e-commerce and contactless payments, there should be continued investment in resilient payment systems.[87] However, humanitarian organizations are also at risk: "Humanitarian organisations collect, store, share and analyse data that is attractive to parties to armed conflict. … As a result, humanitarian organisations are exposed to a growing wave of digital attacks and cyber espionage, and have become highly prized targets."[88] In the summer of 2019, the UN was the target of a complex cyber attack: "'The attack resulted in a compromise of core infrastructure components', said UN spokesperson Stéphane Dujarric, who classified it as 'serious'. … The 'core infrastructure' affected included systems for user and password management, system controls, and security firewalls."[89] When it comes

82 *Ibid.*
83 On the protections that international humanitarian law affords against the effects of cyber operations during armed conflicts, see "Twenty Years On: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts", in this issue of the *Review*.
84 Patrick Collins, "Visa Card Payments System Returns to Full Capacity after Crash", *The Guardian*, 2 June 2018.
85 Martin Arnold, "MasterCard Customers Suffer Outages around the World", *Financial Times*, 12 July 2018.
86 Hadar Rosenberg, *Banking and Financial Services: Cyber Threat Landscape Report*, IntSights, April 2019, p. 3.
87 World Economic Forum, *Impact of COVID-19 on the Global Financial System: Recommendations for Policy-Makers Based on Industry Practitioner Perspectives*, Geneva, April 2020, available at: www3.weforum.org/docs/WEF_Impact_of_COVID_19_on_the_Global_Financial_System_2020.pdf.
88 ICRC, above note 20, p. 12.

to digital payments, data collected to make payments to recipients can be at risk of "hacks" while held with the humanitarian organization, and again when held by the financial service provider.

Risk cannot be entirely eliminated

As noted above, the risks in using digital payments can never be entirely avoided, only mitigated. Critical risks including exacerbating the digital divide, increased cyber attacks and data breaches, unknown implications of the creation and use of digital identities, and wider concerns around data protection which must be weighed against the benefits of digital payments. Decisions must be taken mindfully and based on each country or population group, as the severity of impact can change for different groups in different situations. Affected people must have the option to opt out of providing personal data (biometric or otherwise) without it prejudicing their access to essential assistance. Risk analysis – a weighing of the cost–benefit parameters – should be done in consultation with affected people themselves. While the risk may be the same for different groups, the impact of that risk on people's daily lives can vary wildly, and we should listen to their perspectives when taking decisions. A Ground Truth Solutions study which found that "users want cash transfers delivered through mechanisms that are flexible, trustworthy and reliable"[90] dovetails with other evidence – both researched and anecdotal – that people prefer payment mechanisms with which they are familiar, whether those are digital or not. Expecting people in crisis situations to absorb new risk or trust unfamiliar systems is a big ask and must not be undertaken unless it is in their best interest and with their agreement. It is not only today's risks that are a concern; technology is developing much faster than we can keep pace with, and it is obvious that humanitarians cannot accurately imagine all possible future risks. Despite this, we must continue to examine the risks and benefits of digital solutions, including digital payments, while respecting the principle of "do no digital harm".

How to mitigate the risks of digital payments

While we have focused on some of the main risks of digital payments, it is worth remembering all the evidenced benefits that have led the humanitarian sector to embrace their use, particularly as the risks and potential pitfalls of digital payments described above can all be mitigated to a certain extent. The question that must be asked every time humanitarians choose digital payments is whether

89 Ben Parker, "The Cyber Attack the UN Tried to Keep under Wraps", *The New Humanitarian*, 29 January 2020, available at: www.thenewhumanitarian.org/investigation/2020/01/29/united-nations-cyber-attack.

90 Ground Truth Solutions, *Improving User Journeys for Humanitarian Cash Transfers*, December 2018, available at: https://groundtruthsolutions.org/wp-content/uploads/2018/12/User_Journeys_Summary-Report_2018.pdf.

those mitigation measures are sufficient to balance the advantages with the risks. We have noted that there is no such thing as risk-free action, and this is especially true in conflict settings. In weighing the risks and benefits of any action, we touch on one of central dilemmas of humanitarian action in crisis: the risk of acting versus the risk of doing nothing.

Closing the digital divide

If digital payments are not accessible to all, there are several measures that humanitarians can take, depending on the cause. Sometimes the issue is simply that people have never used digital payments before. In this case, basic financial literacy classes can be provided to ensure that people are comfortable with the payment instrument being used. For example, Mercy Corps "embraces a broad definition of financial inclusion, seeking to improve access [and] ensure quality and actual usage of financial products and services", and one of its key strategies is increased client-level financial capability.[91] Organizations such as the Center for Financial Inclusion[92] and the Consultative Group to Assist the Poor[93] were founded with the very objective of promoting financial inclusion and advocating for inclusive, responsible finance. The ICRC, where possible, tries to use financial service providers that people already hold personal accounts with, so that they are familiar and comfortable with the services, have already met the KYC requirements and are not being asked to trust unfamiliar systems. If the issue is that people cannot meet the KYC requirements, this can be harder to resolve. The ICRC can refer people to legal services to help them obtain missing documentation such as identity papers, and even cover the costs of these documents if needed. Humanitarian agencies such as the Danish Refugee Council, Norwegian Refugee Council, UNHCR and a host of local actors include legal advice and the provision of, or advocacy for, key documentation as part of their services. If people cannot access digital payments services, humanitarians must be ready to offer alternatives such as cash payments or in-kind assistance. It can be challenging to offer different options; for example, if digital payments are not a solution for many people, making cash payments to large numbers of people can be logistically complicated, and setting up a new pipeline to procure and deliver in-kind assistance instead will take time. Humanitarian organizations must ensure that they have the infrastructure and procedures in place for in-kind assistance, cash, vouchers or digital payments where appropriate, enabling them to switch if needed.

While many humanitarian organizations are using technologies to improve digital proximity to populations, such as harnessing different means of (two-way) digital communications, monitoring population movements remotely, or making digital payments so that people can pay for essential goods and services, they

91 Mercy Corps, *Financial Inclusion: Approach and Principles*, 2019, available at: https://tinyurl.com/1f9ejhfq.
92 See the Center for Financial Inclusion website, available at: www.centerforfinancialinclusion.org.
93 See the Consultative Group to Assist the Poor website, available at: http://cgap.org/.

must continue to balance both physical and digital proximity. The ICRC will continue to negotiate for unimpeded access to people affected by armed conflict. Being accountable to people affected by armed conflict is a key element of the organization's identity and the essence of its operational model, which is based on proximity to affected people.

Digital identities and personal data: protecting data "by design"

When it comes to digital identity, humanitarian organizations should take a measured approach to their engagement. If humanitarian organizations use biometrics, thus creating digital identities, steps must be taken to ensure that those digital identities are used only for the specified purposes and are securely managed. Affected people must have the information they need to make an informed decision and to have agency over their digital identity and digital anonymity, and must have the ability to opt out of having a digital identity created on their behalf, without it prejudicing their access to assistance. A middle-ground option may be provided by the development of different forms of "self-sovereign identities", such as blockchain-based identities where the data subject has a digital identity but has ultimate control over who can access it.

In discussing how to mitigate risks related to data protection, it is imperative to analyze the situation of affected people. Some people may be at greater risk of negative consequences due to their individual characteristics, such as their legal status, their socio-economic situation, their race, or their religious or political affiliations. This can be exacerbated in situations of armed conflict, which often fall along ethnic or socio-political fault lines. It is also important to understand how the financial service provider will both store and use the data that it receives from humanitarian organizations to facilitate the digital payments. This is influenced both by the financial service provider's own company practice and by national legislation. For example, the ICRC has checklists that highlight data protection "red flags" and issues of concern which it would wish to discuss or negotiate with the provider. However, the humanitarian sector must be realistic; while it should be possible to negotiate that the service provider only uses the data provided to facilitate the digital payment and not for marketing or analyzing creditworthiness, obligations such as mandatory reporting under national legislation cannot be negotiated. Significant investment is being made by humanitarian organizations in tools and guidance to support analyzing data protection concerns with digital payments. A new short course hosted by CaLP focuses on e-transfers and operationalizing beneficiary data protection.[94] The ELAN Data Starter Kit[95] is designed to help humanitarians plan and improve data management practices, while the Mercy Corps *E-Transfer Implementation*

94 CaLP, "E-Transfers and Operationalizing Beneficiary Data Protection", available at: www.calpnetwork.org/blog/new-calp-online-training-course-e-transfers-and-operationalizing-beneficiary-data-protection/.

95 ELAN, *A Data Starter Kit for Humanitarian Field Staff*, available at: www.mercycorps.org/sites/default/files/2019-11/DataStarterKitforFieldStaffELAN.pdf

Guide[96] provides a step-by-step walkthrough on implementing e-transfers and includes support on analyzing the regulatory environment, KYC requirements and including data protection in its contracting. Many organizations, including UN agencies and NGOs, have their own internal data protection policies and guidance.

In short, every humanitarian organization must complete its due diligence. For the ICRC, this means firstly determining the likelihood of the risk – how likely is the data to be compromised? – and secondly determining the impact of the risk on the individual – how severe would the consequences be for the individual, as well as for the perception and acceptance of the ICRC by the population and the parties to the conflict? In practical terms, this entails ICRC teams completing a Data Protection Impact Assessment, which will help to identify the privacy risks to individuals, identify data protection compliance liabilities for the ICRC, protect the ICRC's reputation, and ensure that the organization does not compromise on the neutrality of its humanitarian action.[97] Similarly, CaLP has shared guidance on data protection in CVA, including model privacy impact assessments,[98] and this work is being built on by multiple humanitarian organizations.

It is critical that any risk assessment – whether for data protection or any other area of risk – includes consulting the affected population themselves. In Afghanistan, the ICRC considered using mobile money transfers to make digital payments. People living in Taliban-controlled communities were well aware of the possibility of geolocalization through mobile phones, and while they said that they trusted the ICRC to protect their data – and often gave the organization their phone numbers so that its teams could be in contact with them – they were concerned about how the mobile money companies would use their data, or which groups their data might be passed to. In direct contrast to this, in Ukraine, where ICRC teams discussed digital payments and technologies, the local communities – somewhat fatalistically – told the organization that the authorities already had all their data (through passport records, mobile phone and banking records, and even through Facebook), and as such, they didn't see any additional risk in the ICRC collecting and sharing their data. These two examples show how different people's perspectives of the likelihood and impact of risk can be, and why it is essential to take affected people's views into account when analyzing risk.

From a pure data protection perspective,

> one possible option in programmes using cash and voucher assistance is for the Humanitarian Organization to transfer, when feasible, a unique identifier (from which the receiving entity cannot identify the final beneficiary) and the amount

96 Mercy Corps, *E-Transfer Implementation Guide*, 2018, available at: www.mercycorps.org/sites/default/files/2020-01/EtransferGuide2018%2C%20Final.pdf.
97 C. Kuner and M. Marelli (eds), above note 71, Chap. 5.
98 CaLP, *Protection Beneficiary Privacy: Principles and Operational Standards for the Secure Use of Personal Data in Cash and e-Transfer Programmes*, 2013, available at: www.calpnetwork.org/wp-content/uploads/2020/01/calp-beneficiary-privacy-web.pdf.

of cash to be distributed to the commercial service provider (e.g. bank or mobile network operator), so as to limit the risks to the individuals concerned.[99]

This can be particularly useful for people who have no formal identity document, or where the risk of their data being shared with the financial service provider is deemed too high. Of course, this approach does not allow for financial inclusion, as the person does not have access to a personal account.[100]

Assessing critical infrastructure

In terms of financial infrastructure, it is much easier to assess its availability than its security. Humanitarian organizations can assess several issues, including the provider's liquidity, its geographical coverage, including the number of points of sale (locations and capacity of those places where recipients can make onward digital payments or "cash out"), and the availability of customer support services. With the growing risk of cyber attacks on financial infrastructure, it becomes more complex and difficult to analyze the security of that infrastructure. Beyond analyzing past incidents in the country and which providers they have affected – likely only from publicly available sources, as financial service providers do not disclose all hacks – there is a limit to what a humanitarian organization can do to be sure of the stability and safety of financial infrastructure. Humanitarians can, however, ensure that they implement appropriate technical and operational security standards in their own operations, and processes should be put in place for the protection of people's personal data from loss, theft, damage or destruction; this includes back-up systems and effective means to respond to security breaches and prevent unauthorized access, disclosure or loss of data that humanitarians store. The *Handbook on Data Protection in Humanitarian Action* also recommends that humanitarian organizations "protect 'by design' the Personal Data they obtain from beneficiaries …. Encryption or compartmentalization of information can be viable solutions to meet this need."[101]

Data responsibility: From theory to practice

All of these mitigation measures fall under the broad category of data responsibility. The OCHA Centre for Humanitarian Data has attempted to address gaps in guidance through its series on data responsibility, providing guidance on a wide range of issues including data incident management.[102] However, this remains a critical area for investment.

99 C. Kuner and M. Marelli (eds), above note 71, p. 154.
100 ICRC, above note 4, p. 26.
101 C. Kuner and M. Marelli (eds), above note 71, p. 155.
102 OCHA, Centre for Humanitarian Data, "Guidance Note: Data Incident Management", August 2019, available at: https://centre.humdata.org/wp-content/uploads/2019/08/guidanceNote2_dataincidentmanagement.pdf.

Of course, humanitarians can't predict the future; we cannot know all the myriad ways in which the data we collect today could be used for different purposes tomorrow, employing technologies that may not even exist today. However, all humanitarian agencies need to ensure data minimization – i.e., that only the personal data necessary for the identification of individuals should be collected and processed for the explicit humanitarian purpose of making the digital payments. Any "excess" information should not be collected, or if collected, should be deleted. We must ensure that the technologies we use to create digital ID, to store, process and share data and to communicate with affected people are secure. While it is vital to uphold clear standards on data protection, the humanitarian sector must also accept that it is impossible to fully protect data from every possible breach or misuse. More fundamentally, we should start from the fact that access to humanitarian assistance should not depend upon people being forced to disclose their personal information.[103] With robust data responsibility policies and practices, and thoughtful decision-making, we can do our due diligence, taking measures to analyze the risks that the method of assistance – and in the case of CVA, the payment instrument – exposes people to, and mitigate them.

Conclusion

The digitalization of cash is happening, with or without the humanitarian sector. Digital payments in humanitarian responses have been proven to have numerous benefits, primarily for recipients but also for humanitarian agencies delivering services, and these benefits are not being questioned *per se*. Rather, we need to ensure that these benefits outweigh the risks, and that as humanitarians we do our due diligence, on behalf of the people we serve, while recognizing that we do not live in a risk-free world. This is not a one-time deal; the analysis of risks and benefits should be done every time we choose whether to use digital payments, and should be done in collaboration with affected people, in order to take on board their views and their own analysis of risk.

Despite the rise in digital payments, it does not follow that cash will cease to exist. Cash (physical currency) is not linked to the person, and as such does not discriminate or identify; cash remains here to stay, at least in the coming years. The humanitarian sector must continue to work with both cash payments and digital payments – as well as offering in-kind assistance and services – based on what is most appropriate to meet the needs of populations affected by armed conflict and other situations of violence. We must always offer alternatives.

103 It is important when providing humanitarian services to collect the minimum amount of data possible, or even none at all. This process of data minimization is separate from the question of identifying the appropriate legal basis for data collection and processing, a principle which is supported by the ICRC's *Handbook on Data Protection in Humanitarian Action* and the "do no harm" principle and is one of the core principles of data protection.

Humanitarians are often accused of embracing change too slowly, particularly with regard to new technologies. Technology is moving faster than any of us – as private individuals or within our organizations – can keep pace with. Humanitarians are not financial service providers, and we are not technologists; we need to find avenues for working with the private sector to harness opportunities, but in ways that are in the best interests of crisis-affected people. At the ICRC's 2018 symposium on "Digital Risks in Situations of Armed Conflict", Professor Nathaniel Raymond, whose research interests have focused on the human rights and human security implications of information communication technologies for vulnerable populations, particularly in the context of armed conflict, challenged the audience by stating: "We are undermining the 'values of Geneva' through a relatively blind embrace of the potential 'promises of Silicon Valley'."[104] Banknotes and coins are a public utility, and companies make no profit from their use, only from the goods and services purchased with them. Hence the drive for "cashlessness", as digital payments generate revenue for financial service providers – and with it, greater surveillance and greater risks of misuse of data. Seen in this context, the approach taken by organizations like the ICRC and Oxfam, of taking time to analyze the opportunities and risks of solutions, should be understood as a measured and appropriate level of caution rather than a reluctance to embrace change. Humanitarians should "experiment in labs, and not on people".[105]

The ICRC will continue to be defined and led by our principled approach to humanitarian action, putting people at the centre of our work. To harness the opportunities that digitalization brings – for digital payments, but also beyond – we will continue to keep the people we serve at the centre of our analysis.

I would finish with a call to action for the humanitarian sector to do two key things.

Firstly, humanitarians must define what "do no digital harm" looks like in reality. "This requires that we understand the risks, protection issues, ethical concerns and challenges before building digital solutions and having a valid and important humanitarian purpose for developing a certain digital capability or using certain data."[106] Digitalization is changing the way our world works in fundamental ways, and this "digital disruption" has both positive and negative impacts on humanitarian action. Organizations must consider not only the way they provide humanitarian protection and assistance in a digital world, but how they transform themselves as digital agencies. We must translate our principled approach to humanitarian action into this brave new digital world.

Secondly, and most importantly, as we have reflected throughout this paper, we must keep people affected by conflict and other situations of violence at the centre of our action. Humanitarians must base both the strategic and day-to-day decisions that we make on conversations with the affected people that we

104 ICRC, above note 20, p. 5.
105 *Ibid.*, p. 2.
106 *Ibid.*, p. 2.

are here to serve, always keeping their interests at the forefront. This does not simply involve providing feedback mechanisms; it requires us to actively listen to, and reflect upon, what people affected by conflict and other situations of violence have to say, and to adapt our approaches to their preferences, needs and capacities. We must ensure a person-centred approach to the analysis of the risks and benefits of any action – including the use of digital payments.

Fundamentally, humanitarians must be more mindful in their decision-making around digital payments and their interactions in the digital world, always putting affected people at the centre of their decision-making.