International Review of the Red Cross (2017), **99** (1), 179–209.
Migration and displacement
doi:10.1017/S1816383117000637

INTERNATIONAL REVIEW of the Red Cross

Migration and data protection: Doing no harm in an age of mass displacement, mass surveillance and "big data"

Ben Hayes
Ben Hayes is a UK-based researcher and consultant working on human rights, data protection and applied ethics in counterterrorism, international security, border control, policing, humanitarian action and frameworks for research and development. He has conducted data protection impact assessments and devised data protection frameworks for the International Committee of the Red Cross, the International Federation of Red Cross and Red Crescent Societies, the Office of the United Nations High Commissioner for Refugees (UNHCR), the European Commission and other public and private sector organizations. He is a Fellow of the Transnational Institute, an Associate of the Peace Research Institute Oslo and the Human Security Collective, and a Director of Data Protection Support & Management Ltd.

Abstract
This article considers the key data protection challenges facing humanitarian organizations providing assistance to refugees, internally displaced persons and migrants. These challenges are particularly significant for several reasons: because data protection has come relatively late to the humanitarian sector; because humanitarian organizations are under pressure to innovate rapidly; because the global communications architecture on which many of these innovations depend is inherently vulnerable to State surveillance; and because States are deploying

increasingly sophisticated and coercive means to prevent irregular forms of migration and/or subjecting humanitarian organizations to surveillance and disruption. The first part of the article outlines the fundamental rights challenges presented by contemporary data-driven migration control paradigms. The second outlines concerns about "data-driven humanitarianism" and "mass surveillance" to show how humanitarian organizations risk inadvertently exacerbating these problems. The third assesses specific data protection challenges that humanitarian organizations face and the policies and practices they have developed in response. The article concludes with some brief observations on the technical and political dynamics shaping their efforts to comply with their legal and ethical obligations, and calls for the sector to work together to extend data protection norms and outlaw cyber-attacks by State actors.

Keywords: migration, border control, immigration, asylum, refugees, surveillance, vetting, big data, humanitarian action, data protection, privacy, human rights.

: : : : : : :

> You arrive at a refugee camp, hungry and desperate. To access food and basic necessities, you have to agree to provide biometric data – iris and fingerprint scans. Several years hence, you are living in a country which passes a new law asserting jurisdiction over data stored in the cloud by the organization that helped you. By taking your fingerprint, the security services can now find out not only your ethnicity or immigration status but your movements, consumer patterns and financial situation. In some instances the pressure is happening real-time, as data is collected. The fact that "humanitarian data" is picked up and used for purposes other than humanitarian, such as counter-terrorism or migration flow management (while understandable and important from one point of view), puts the individuals at risk of adverse, albeit potentially legitimate, consequences (such as arrest, denial of entry, etc).[1]

Introduction

This article considers the key data protection challenges faced by humanitarian organizations (HOs) providing assistance to refugees, internally displaced persons and migrants in need of support. These challenges are significant for many reasons, but four are particularly important in terms of framing this discussion. The first is the simple fact that concern for data protection has come relatively

1 Anja Kaspersen and Charlotte Lindsey-Curtet, "The Digital Transformation of the Humanitarian Sector", *Humanitarian Law & Policy Blog*, 5 December 2016, available at: blogs.icrc.org/law-and-policy/2016/12/05/digital-transformation-humanitarian-sector/ (all internet references were accessed in August 2017).

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

late to the humanitarian sector. This is not to say that HOs have not taken data protection-related issues such as beneficiary consent, data accuracy and confidentiality seriously in the past – clearly these practices have long been integral, if not always universally implemented – but rather that the adoption and compliance with international data protection norms is something that the sector as a whole is only just beginning to address. Though HOs were rightly singled out by privacy advocates as having failed to keep pace with developments in privacy and data protection law,[2] galvanizing some into remedial action, it is also the case that data protection (in the sense of both a set of legal standards and a community of change) has traditionally had very little to say about humanitarian action, at least relative to other sectors.[3]

This omission is critical because the features of the emergencies or conflicts to which humanitarian actors routinely respond present formidable challenges to the practical application of key tenets of data protection. Although humanitarian action often occurs in ungoverned or ill-governed spaces, where data protection may appear the lowest of priorities, these challenges are not devoid of wider social, political or legal context. On the contrary, the backdrop to humanitarian support for migrants and refugees is a global order now characterized by as yet relentless demands for ever tighter immigration and border controls – demands which have in practice resulted in ever more sophisticated techniques of data-driven "migration management", and which have in turn presented their own range of human rights and data protection challenges. This is the second overarching issue that frames this article.

HOs must contend with the consequences of these developments, primarily as defenders of the rights and best interests of their beneficiaries, but also, and increasingly, as users of the same ("interoperable") technologies and as partners of governments with multiple interests in the data. Those that are innovating and availing themselves of the opportunities presented by "data-driven humanitarianism"[4] must also contend with a global communications infrastructure that is vulnerable to surveillance and infiltration by State and non-State actors alike. With HOs as the potential targets of the intelligence agencies of friendly as well as hostile States, the risk of "aiding surveillance" is the third key challenge considered below.

This challenge is linked to a fourth: the intrinsic "double character", to borrow an expression from Marx,[5] of the applications that are shaping

2 Anna Crowe, "A Paucity of Privacy: Humanitarian, Development Organisations Need Beneficiary Data Protection Policies", *Privacy International*, 28 November 2013, available at: www.privacyinternational.org/node/240.

3 The 1990 UN General Assembly's Guidelines for the Regulation of Computerized Personal Data Files represent the most significant exception, but these were designed to apply early data protection principles to UN computer systems rather than human action *per se*. See UNGA Res. 45/95, 14 December 1990.

4 See, for example, Patrick Meier, "New Information Technologies and Their Impact on the Humanitarian Sector", *International Review of the Red Cross*, Vol. 93, No. 884, 2011.

5 This analogy is itself borrowed from Thomas Mathiesen, *On Globalisation of Control: Towards an Integrated Surveillance System in Europe*, Statewatch, London, November 1999, p. 1.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

international mobility and aid delivery in the twenty-first century. Big data promises everything from secure borders to crime prediction to efficient targeting of aid. Access to territory and humanitarian assistance is already and increasingly shaped by policies of surveillance and social sorting, and practices of inclusion, exclusion and social control.

For HOs committed to the principle of "do no harm", all of this has critical real-world consequences: for their operations and reputations, and for the fundamental rights and safety of their beneficiaries. Data breaches in developed countries can be inconvenient or costly for those affected; for refugees and their families back home, they can be life-threatening.[6] And although data protection can appear a rather toothless counterweight to the "mass surveillance" revealed by Edward Snowden[7] or the "extreme vetting" demanded by US president Donald Trump,[8] robust data protection policies and practices are among the only tangible means that HOs have to innovate responsibly, guard against the reputational damage threatened by data loss or cyber-attack, and mitigate the formidable challenges thrown up by big data and coercive government policies.[9]

This article is divided into three main parts. The first builds on this introduction by outlining some key features of contemporary international migration control and the fundamental rights challenges they present. The second part outlines concerns about "data-driven humanitarianism" and draws on the documents released by Edward Snowden to show how HOs risk inadvertently exacerbating these problems by "aiding surveillance". Finally, in the face of too many over-simplistic and sensationalist critiques of humanitarian innovation, the third part attempts to provide a more nuanced and necessarily technical assessment of the unique data protection challenges that HOs working with migrants and refugees face, and some of the policies and practices they have developed to meet those challenges. The article concludes with some brief observations on the technical and political dynamics shaping their efforts to comply with their legal and ethical obligations, and the need for HOs to work together to extend data protection norms in the sector and outlaw cyber-attacks by State actors.

6 A. Kaspersen and C. Lindsey-Curtet, above note 1.

7 Edward Snowden is a whistleblower who passed a tranche of intelligence documents to journalists at the *Guardian* and *Washington Post*. The documents revealed operational details about the global surveillance programmes of the United States and its Australian, British and Canadian partners, and the two newspapers won a Pulitzer Prize for their reporting.

8 Sabrina Siddiqui, "Trump Signs 'Extreme Vetting' Executive Order for People Entering the US", *The Guardian*, 27 January 2017, available at: www.theguardian.com/us-news/2017/jan/27/donald-trump-muslim-refugee-ban-executive-action.

9 On the challenges thrown up by big data, see Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information*, Harvard University Press, Cambridge, MA, 2015; Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Penguin, London, 2016; Gry Hasselbalch and Pernille Tranberg, *Data Ethics – The New Competitive Advantage*, Publishare, Copenhagen, 2016. On the challenges of mass surveillance and coercive State policies, see Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W. W. Norton, New York, 2015.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

The securitization of international migration

In international relations theory, critical security studies and other social science disciplines, "securitization" describes the process of transforming a subject into an issue of "security".[10] Once politicized in this way, measures that were hitherto deemed excessive or otherwise unacceptable to policy-makers may be adopted and normalized in ways that would not have been possible without the recourse to insecurity, real or imagined. Though the merits and utility of "securitization" theory are much debated,[11] it is certainly difficult to conceive of more "securitized" areas of public policy than those relating to international migration, asylum and border control. Indeed, even the most seasoned of frequent travellers may be hard-pressed to recall an actually quite recent past when immigration formalities were largely administrative in nature and the body scanners that now pervade airport checkpoints were still confined to science fiction.

While migration has long been linked to survival, legal migration has always been tied to privilege and shaped by prevailing ideologies and power structures, with visa regimes and admission policies inextricable from colonialism, racism and fascism.[12] Today, the "migrant", the "refugee" and the "illegal" are collectively objectified in the political discourse and praxis of "national security" as never before. With the obvious caveat that the brief outline which follows cannot possibly hope to do justice to such a complex and highly politicized arena,[13] this section highlights the key features of an overall policy framework in which "data" is central, yet where the key tenets of data protection have been marginalized or circumvented. These features are: the conflation of border control and counterterrorism; new technologies for identity management; the worldwide proliferation of immigration controls; outsourcing and authoritarianism; enhanced security vetting; and the limited application of relevant human rights instruments.

10 On the origins of this kind of "securitization" theory, see Barry Buzan, Ole Wæver and Jaap de Wilde, *Security: A New Framework for Analysis*, Lynne Rienner, Boulder, CO, 1998.

11 See Columba Peoples and Nick Vaughan-Williams, *Critical Security Studies: An Introduction*, Routledge, New York, 2010.

12 See Liz Fekete, "The Emergence of Xeno-Racism", *Race & Class*, Vol. 43, No. 2, 2001; Steve Cohen, *Standing on the Shoulders of Fascism: From Immigration Control to the Strong State*, Trentham Books, London, 2002; Liz Fekete, *A Suitable Enemy: Racism, Migration and Islamophobia in Europe*, Pluto Press, London, 2009; Marjory Harper and Stephen Constantine, *Migration and Empire*, Oxford University Press, 2010; Lili Eskinazi, "European Immigration: A Colonial Legacy?", *Alternatives International Journal*, 31 October 2011, available at: www.alterinter.org/spip.php?article3694.

13 This article does not seek or claim to provide a theory of either surveillance or migration control. It should also be stressed that surveillance may be a byproduct of as well as a motivation within the myriad national and international policies that have been introduced in this area. Similarly, the lack of attention in this article to other factors driving developments in this area – such as migration patterns, domestic politics, technological advances and the bureaucratic impulse to enhance efficiency – does not signify any belief that they are unimportant. Lastly, immigration controls are not the same everywhere; there may be a clear direction of travel but the path is characterized by "disjointed incrementalism", a term that is credited to political scientist Charles E. Lindblom's 1959 essay "The Science of 'Muddling Through'", *Public Administration Review*, Vol. 19, No. 2, 1959.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

The migration–terror nexus

The first of these features is the conflation of immigration control with counterterrorism after the terrorist attacks in the United States on 11 September 2001. Regardless of any statistics demonstrating the "home-grown" terror threat to be more significant than that posed by migrants,[14] or the probability that in the United States one is more likely to be killed by a policeman or a toddler than a terrorist,[15] the border is now widely perceived as the first and most important line of defence against terrorism. As George W. Bush, then president of the United States, put it in 2002: "We need to know who is coming into our country, why they're coming into our country, and whether or not they're leaving our country when they say they're going to be leaving our country."[16] This assertion characterized a new orthodoxy to which all policy debates about border control could be, and inevitably were, effectively reduced.

Such discourse was by no means limited to the United States. Among the first legislative responses of the European Union (EU) to the attacks of 9/11 was a common position on combating terrorism requiring member States to vet all asylum-seekers for connections to terrorist groups before granting refugee status,[17] itself modelled on the non-binding provisions of a United Nations (UN) Security Council resolution on the same topic.[18] In the fifteen years that have followed, travellers of every stripe have been subject to ever more sophisticated attempts to vet and profile them in order to assess and mitigate the risks they are perceived to present. This has paved the way for the "extreme vetting" now demanded by the current US government (see further below).

Identity management

The second feature is a corollary to the first. Attempts to control migration through the plethora of measures that have been adopted since 9/11 have coalesced around techniques of identity management centred on the deployment of biometric identification systems. From an initial emphasis on ensuring – via a unique biometric identifier[19] – that the holder of a travel document was the person to

14 Alex Nowrasteh, *Terrorism and Immigration: A Risk Analysis*, Cato Institute, Policy Analysis No. 798, Washington, DC, 13 September 2016.

15 Gary Younge, "Trump Fears Terrorists, but more Americans are Shot Dead by Toddlers", *The Guardian*, 8 February 2017, available at: www.theguardian.com/commentisfree/2017/feb/08/trump-muslim-terrorists-gun-violence-america-deaths.

16 Adam Entous, "Bush to Seek New Powers in Homeland Security Plan", *Reuters*, 15 July 2002.

17 Council Common Position of 27 December 2001 on Combating Terrorism, *Official Journal of the European Communities*, 2001/930/CFSP, 27 December 2001 (OJ 2001 L 344/90), Art. 16.

18 UNSC Res. 1373, 28 September 2001, Art. 3(f).

19 Most biometric systems used for border and immigration controls use digitized photographs, fingerprints or iris scans, or a combination of two of these identifiers. Biometric profiles are entered into population databases and/or stored in radio-frequency identification chips attached to travel documents issued by States. Once enrolled, the identity of individuals can be checked against the database or the travel document. The only biometric mandated by the International Civil Aviation Organization, which sets global standards for air travel, is the digitized photograph.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

whom it was issued, these identity management systems are now being integrated into wider law enforcement and surveillance apparatuses. And although the mandatory fingerprinting of citizens remains a (fading) redline in some countries with a civil liberties tradition, such as the United Kingdom and United States, biometric profiling is being widely deployed across the world and has fast become the norm for "non-citizens" and "aliens", regardless of those traditions.[20]

Today, biometric profiling is part and parcel of border control worldwide, but as these systems have developed, so too have their capabilities. So-called "smart border systems" can be used to track individuals across territories,[21] while the databases that house the biometrics have been opened up to national security and law enforcement agencies.[22] Whereas authorized travellers appear to have accepted biometric profiling as a condition of their passage (of course, it is not as if they have a choice), the use of biometrics in more coercive situations – for example in respect to the determination of State responsibility for asylum and expulsion policy in the EU – has led to horrific stories of refugees and migrants mutilating their fingertips to avoid immigration enforcement measures.[23] In response, States have begun to criminalize failure to provide fingerprints to immigration officers.[24] Though the symbolism is striking, the reality is that ever tighter attempts to prevent irregular migration have long developed in symbiosis with ever more "extreme" attempts to evade them.

The global proliferation of immigration controls

This phenomenon is also reflected in the transfer of migration control techniques from destination countries to countries of origin and transit, which occurs through technical assistance, migration management deals and aid-and-trade packages. These measures take various forms, from the imposition of so-called

20 The decision to biometrically profile all asylum-seekers and irregular migrants in the EU in fact long pre-dates 9/11, with legislation proposed in 1995 and finally adopted in 2000. After 9/11, the EU decided that mandatory fingerprinting should also be introduced for all visa applicants, all visa-exempt third-country nationals entering the EU, all legally resident third-country nationals, and all EU passport holders (the UK opted out of this decision). See Kjetil Rommetveit, "Introducing Biometrics in the European Union: Practice and Imagination", in Ana Delgado (ed.), *Technoscience and Citizenship: Ethics and Governance in the Digital Society*, Springer, Cham, 2016.

21 See Ben Hayes and Mathias Vermeulen, *Borderline: The EU's New Border Surveillance Initiatives – Assessing the Costs and Fundamental Rights Implications of EUROSUR and the "Smart Borders" Proposals*, research study, Heinrich Böll Foundation, Berlin, 2012.

22 In the EU, for example, every major immigration and asylum database (including the Schengen Information System, Eurodac System, Visa Information System and proposed "smart borders" system) has seen the primary legislation later amended to provide access for security and intelligence services. See Costica Dumbrava, "European Information Systems in the Area of Justice and Home Affairs: An Overview", *European Parliamentary Research Service*, May 2017, available at: www.europarl.europa.eu/RegData/etudes/IDAN/2017/603923/EPRS_IDA(2017)603923_EN.pdf.

23 See, for example, Graeme Culliford, "I've Burned off Tips of My Fingers to Get to UK", *The Sun*, 14 June 2014, available at: www.thesun.co.uk/archives/news/900339/ive-burned-off-tips-of-my-fingers-to-get-to-uk/.

24 See EU Fundamental Rights Agency, *Fundamental Rights Implications of the Obligation to Provide Fingerprints for Eurodac*, Vienna, May 2015.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

"pre-frontier checks" and readmission obligations to policy and technology transfers, often facilitated by intergovernmental organizations.

While it might be assumed that stronger immigration controls have simply gone hand-in-hand with development and modernity, as richer countries have gradually sought to prevent or control migration from poor ones, the world's richest countries have also very deliberately exported them. Their motivation is twofold: firstly, to enlist support and build capacity in countries of origin and transit of migrants and refugees in order to prevent undocumented migrants from reaching the territories of those wealthier States which do not want them to arrive – and expeditiously returning those that do manage this feat (the EU–Turkey refugee deal being the starkest example of the pursuit of this policy[25]); and secondly, to facilitate the collection of data on inbound travellers and to gather intelligence on other persons of interest. The EU and its member States have been most active in this area, providing technical assistance to a range of countries in central and eastern Europe, North and West Africa, the Middle East and, at the height of the refugee "crises" that armed conflict always produces, countries as far afield as Sri Lanka.[26] This assistance has covered everything from immigration and asylum systems to border control infrastructure, the training of immigration officers and border guards, detention centres and information campaigns advising against unauthorized emigration. It has even – contrary to the free-movement provisions in the UN Declaration on Human Rights – encompassed the most coercive of measures to prevent "unauthorized exit".[27]

The United States has also provided a great deal of technical assistance in this area, including the technology and funding for immigration control systems in countries such as Afghanistan, Cambodia, Ethiopia, Ghana, Kenya, the Maldives, Pakistan, Tanzania and Yemen.[28] According to one government minister on the receiving end of this largesse, the rationale is to provide "a door for American influence" by allowing the United States to locate foreign nationals whenever it wishes.[29] Regardless of motivation, and as will be discussed further below, the intrinsic relationship between border control, identity management and national

25 Council of the European Union, "EU-Turkey Statement", Press Release No. 144/16, 18 March 2016.

26 See Ben Hayes, Steve Wright and April Humble, "From Refugee Protection to Militarised Exclusion: What Future for 'Climate Refugees'?", in Nick Buxton and Ben Hayes (eds), *The Secure and the Dispossessed: How the Military and Corporations Are Shaping a Climate-Changed World*, Pluto Press, London, 2015.

27 European States have, for example, supplied armed vessels to the Libyan Coastguard. See Maurizio Albahari, *Crimes of Peace: Mediterranean Migrations at the World's Deadliest Border*, University of Pennsylvania Press, Philadelphia, 2015, p. 88. See also Maggie Michael, "Backed by Italy, Libya Enlists Militias to Stop Migrants", *Associated Press*, 29 August 2017, available at: www.apnews.com/9e808574a4d04eb38fa8c688d110a23d. The Universal Declaration of Human Rights states that "[e]veryone has the right to leave any country, including his own"; see Universal Declaration of Human Rights, 217 A (III), 10 December 1948, Art. 13(2).

28 See Ben Hayes and Roch Tassé, "Control Freaks: 'Homeland Security' and 'Interoperability'", *DifferenTakes: A Publication of the Population and Development Programme at Hampshire College*, No. 45, Spring 2007.

29 Former Maldives Minister of State for Defence and National Security Ilyas Hussain Ibrahim, cited in Gus Hosein and Carly Nyst, *Aiding Surveillance*, Privacy International, London, 2013, p. 55, available at: www.privacyinternational.org/node/310.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

INTERNATIONAL REVIEW of the Red Cross

security means that this kind of technical assistance frequently raises human rights concerns that are rarely discussed by donors or recipients.

Responsibilization, privatization and authoritarianism

In addition to the thinly veiled attempts by rich countries to outsource their responsibility for refugees and asylum-seekers to poorer ones, contemporary immigration controls are characterized by the growing involvement of the private sector in their domestic and international enforcement.[30] EU States, for example, have imposed legal obligations on transport companies that make them responsible for preventing the arrival of undocumented or inadequately documented passengers. From airlines to lorry drivers, the failure to prevent the passage of unauthorized travellers frequently results in hefty fines known as "carrier sanctions".[31] Scandalously, the predilection for private actors to go to the aid of migrant boats in distress has been similarly restricted by threats and prosecutions for those electing to rescue anyone other than those at an immediate risk of drowning.[32]

More generally, as States have come to depend more heavily on large-scale computer systems and surveillance technology, the private sector has become more invested in the development and implementation of immigration and border control policy. The defence and technology sectors have profited most from these arrangements, with the major defence contractors now earning significant parts of their revenue from their diversification into all things "homeland security".[33] In addition to the massive contracts on offer for border fortification and wide-area surveillance, privatization in the field of criminal justice has seen the private sector gain an increasing foothold in areas such as immigration detention and the enforcement of expulsion policy.[34] Inevitably, the corporatization of border control and immigration enforcement puts efficiency and profit ahead of other values and interests, such as accountability and human rights protection.

Finally, the obligations that have been imposed on the transport sector have been steadily expanded into other areas of public and private life, with landlords, employers, banks, universities, schools and health service workers increasingly subject to statutory obligations to police their clientele by checking their immigration status – again with heavy penalties for dereliction of duty. The growing instrumentalization of public and private actors in the "fight" against illegal

30 See Thomas Gammeltoft, "The Migration Control Industry", in Rita Abrahamsen and Anna Leander (eds), *Routledge Handbook of Private Security Studies*, Routledge, London, 2016.

31 See Sophie Scholten, *The Privatisation of Immigration Control through Carrier Sanctions*, Brill, Leiden, 2015.

32 See Maarten den Heijer, "Frontex and the Shifting Approaches to Boat Migration in the European Union: A Legal Analysis", in Ruben Zaiotti (ed.), *Externalizing Migration Management: Europe, North America and the Spread of "Remote Control" Practices*, Routledge, London, 2016. See also Irini Papanicolopulu, "The Duty to Rescue at Sea, in Peacetime and in War: A General Overview", *International Review of the Red Cross*, Vol. 98, No. 902, 2016.

33 See Mark Akkerman, *Border Wars: The Arms Dealers Profiting from Europe's Refugee Tragedy*, Transnational Institute, Amsterdam, 2016, available at: www.tni.org/en/publication/border-wars.

34 See reports and website of the Global Detention Project, available at: www.globaldetentionproject.org/.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

immigration, which has not been accepted uncritically,[35] has important implications for organizations committed to non-discrimination and universal human rights.

Extreme vetting

The four features outlined above all feed into an overarching fifth: the agglomeration of personal data in order to vet, profile and ultimately categorize travellers and migrants into the legitimate and the suspicious, the deserving and the undeserving, the entitled and the excluded, and so on. As noted above, 9/11 was very much the catalyst for this drive, as the rules were tightened first for refugees and asylum-seekers, then for visa applicants, then for visa-exempt travellers.

The means through which all of this has been achieved include the introduction of biometric visas, where applicants are enrolled and vetted at the time of their application;[36] the introduction of passenger name record (PNR) disclosure regimes and advance passenger information (API) systems, under which law enforcement and security agencies receive detailed information on travellers before their journeys have begun;[37] and Electronic Systems for Travel Authorization, developed to pre-screen travellers before they are allowed to board an inbound carrier.[38] The vetting that takes place occurs largely in secret but is known to include checks to ensure that travellers meet entry criteria and have not previously fallen foul of immigration laws, and screening against national security and counterterrorism databases such as "no-fly" lists, "watch lists", sanctions lists and foreign policy lists.[39] Data is also routinely shared with other States, for example through the Schengen, "Five Eyes" and other bilateral and multilateral security cooperation frameworks.[40]

While the European tabloid press has struggled to come to terms with the idea that one could both own a smartphone and be in need of refugee protection,[41]

35 Medical professionals and university staff are among those who have resisted or refused to engage in such checks where they have been legislated for. See, for example, Miranda Wilson, "Academics Refuse to Police Immigration", *Institute of Race Relations News*, 13 May 2009, available at: www.irr.org.uk/news/academics-refuse-to-police-immigration/.

36 For instance, this is the case with the EU Visa Information System.

37 Australia pioneered the use of API systems, while under EU law the security and intelligence agencies have access to the passenger data (PNR) held in European airline reservations databases.

38 The United States operates a travel authorization system, while the EU plans to introduce one.

39 For an explanation of how these systems are supposed to work, see UK House of Commons, Committee of Public Accounts, "E-Borders and Successor Programmes", 27th Report of Session 2015–16, London, 2016. See also Julien Jeandesboz, Didier Bigo, Ben Hayes and Stephanie Simon, *The Commission's Legislative Proposals on Smart Borders: Their Feasibility and Costs*, PE 462.613, European Parliament, Brussels, 2013.

40 States party to the Schengen Convention pool data on persons to be refused entry or subject to surveillance checks via the Schengen information system, and exchange supplementary data through the "Sirene network". "Five Eyes" refers to a post-war intelligence alliance comprising Australia, Canada, New Zealand, the UK and the United States. In 2009, these countries adopted a "Five Country Conference Data-Sharing Protocol" for biometrics (unpublished). Interpol, the International Police Office, also facilitates the exchange of data used in border control.

41 See James O'Malley, "Surprised that Syrian Refugees Have Smartphones? Sorry to Break this to You, but You're an Idiot", *The Independent*, 7 September 2015, available at: www.independent.co.uk/voices/comment/surprised-that-syrian-refugees-have-smartphones-well-sorry-to-break-this-to-you-but-youre-an-idiot-10489719.html.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

European governments have seized upon the opportunity to introduce some "extreme vetting" of their own by aping the seizures of such devices by US and Israeli border guards.[42] In early 2017, Denmark and Norway produced draft proposals to confiscate smartphones from refugees at the point of registration and to use the data they contain to assess both the security threat that the asylum-seeker poses and the credibility of their asylum claims.[43] The proposals, which raise substantial concerns about asylum procedures, represent an unparalleled intrusion into the private lives of persons seeking asylum.

Privacy and data protection: Dissolving at the border

What, then, of the rights to privacy and data protection that should temper States' predilection for untrammelled surveillance? The short answer is that the right to privacy has proved relatively ineffective due to overbroad interpretations of what constitutes a "necessary and proportionate" restriction.[44] This is due in no small part to a discriminatory approach on the part of States which views foreigners as being less entitled to privacy rights than citizens.[45] As for data protection, which regulates the processing of personal data by public and private bodies and gives rights to data subjects to assert control over data that concerns them and to seek redress if it is misused, security and public policy derogations are compounded by limited geographical reach.[46] Although more than 100 countries now have

42 On the United States, see Olivia Solon, "US Border Agents are Doing 'Digital Strip Searches'. Here's How to Protect Yourself", *The Guardian*, 31 March 2017, available at: www.theguardian.com/us-news/2017/mar/31/us-border-phone-computer-searches-how-to-protect; on Israel, see "Israel Approves Email Checks at the Border", *Times of Israel*, 24 April 2013, available at: www.timesofisrael.com/israel-approves-email-checks-at-the-border/.

43 For Denmark, see unpublished proposal dated 10 February 2017 to amend the Danish Aliens Act, on file with author. For Norway, see proposal (in Norwegian) dated 11 January 2017, available at: www.regjeringen.no/contentassets/8c99986c9bd444b6a00d56fe8afca077/visitasjon-horingsnotat-januar-2017.pdf.

44 Article 8(2) of the European Convention for the Protection of Human Rights and Fundamental Freedoms, ETS 5, 4 November 1950 (entered into force 3 September 1953), on the right to private and family life, holds that "[t]here shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." On what makes communications surveillance "necessary and proportionate", see Necessary and Proportionate Coalition, "Necessary & Proportionate: International Principles on the Application of Human Rights to Communications Surveillance", May 2014, available at: www.necessaryandproportionate.org/principles. On the recent judgments of the Court of Justice of the European Union that are beginning to limit the broad scope of the permissible exceptions, see the judgments *Tele2* and *Watson*, Joined Cases Nos C-203/15, C-698/15; *Schrems v. DPC Irl*, Case No. C-362/14; and *Digital Rights Ireland* and *Seitlinger*, Joined Cases Nos C-293/12, C-594/12.

45 See Marko Milanovic, "Foreign Surveillance and Human Rights, Part 1: Do Foreigners Deserve Privacy?", *EJIL: Talk! Blog of the European Journal of International Law*, 2013, available at: www.ejiltalk.org/foreign-surveillance-and-human-rights-part-1-do-foreigners-deserve-privacy/.

46 Although data protection is often seen as corollary to the right to privacy related to the information that is held about individuals, it is increasingly recognized as a fundamental and constitutional right. See, for example, Charter of Fundamental Rights of the European Union, 2012/C 326/02, 26 October 2012, Art. 8.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

some form of data protection law or provision,[47] many of these do not yet amount to comprehensive data protection regimes and/or fall far short of the highest standards that have been developed in Europe (first by the Council of Europe (CoE), then the EU).[48]

Crucially, even where these high standards do prevail, if data is processed on a statutory basis, or for the purposes of national security, the key data protection principles of individual consent and choice either do not or cannot apply, while the right to assert control over one's data is restricted in fundamental ways (for example in respect to access, correction and deletion of data).[49] These substantial carve-outs are underscored by a now widely held perception that travel and immigration data is "fair game" for national security agencies. As the EU's data protection supervisor put it in 2008, in a critical response to a raft of EU border control proposals that fell largely on deaf ears, the "underlying assumption" is that "all travellers" should be "considered a priori as potential law breakers" and "put under surveillance".[50]

Aiding surveillance?

As suggested in the introduction, the coercive State practices described above have significant implications for HOs, whose activities and innovations – if not subject to robust data protection safeguards – risk exacerbating the fundamental rights problems posed by mass surveillance and data-driven migration management. These concerns were spelt out in a 2013 report by the advocacy group Privacy International entitled *Aiding Surveillance*, which examined the way in which "development and humanitarian aid initiatives are enabling surveillance in developing countries".[51] The report focused on four areas of innovation in the development and humanitarian sectors: (i) the information systems underlying cash transfer programmes; (ii) biometric identification and voter registration systems; (iii) the use of mobile phones and the data collected and generated by them for purposes such as mobile money, health services and crisis management; and (iv) border surveillance and security technologies.

47 See DLA Piper, "Data Protection Laws of the World", available at: www.dlapiperdataprotection.com/.

48 See, for example, CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108, 28 January 1981 (entered into force 1 October 1985); Regulation of the European Parliament on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC, 2016/679/EU, 27 April 2016 (GDPR).

49 For an overview of key principles of data protection see European Union Agency for Fundamental Rights and Council of Europe – European Court of Human Rights, *Handbook on European Data Protection Law,* 2014, available at: www.fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf.

50 European Data Protection Supervisor, *Preliminary Comments of the European Data Protection Supervisor*, Brussels, 3 March 2008, p. 5, available at: https://edps.europa.eu/sites/edp/files/publication/08-03-03_comments_border_package_en.pdf.

51 G. Hosein and C. Nyst, above note 29.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

Supported by dozens of examples, the report observed that whereas the underlying technologies "have been the subject of extensive debate in advanced Western democracies in recent years",[52] there has been a "systematic failure to critically contemplate the potential ill effects of deploying technologies in development and humanitarian initiatives, and in turn, to consider the legal and technical safeguards required in order to uphold the rights of individuals living in the developing world".[53] Justified criticism was levelled at UN agencies, donors, international non-governmental organizations, development actors and HOs, while seminal strategy documents such as the UN Office for the Coordination of Humanitarian Affairs' (OCHA) *Humanitarianism in a Networked Age*[54] and the UN's Post-2015 High-Level Panel's *A New Global Partnership*[55] were chastised for having paid "scant attention to the potential impact of the adoption of new technologies or data analysis techniques on individuals' privacy".[56] In conclusion, the report warned that the "do no harm" approach beloved of the aid sector risked setting too low a bar for human rights protection. The aim, it suggested, should not be to simply avoid imperilling beneficiary human rights, but to actively promote and protect them.[57]

In addition to innovating responsibly, HOs face another challenge thrown up by disclosures about surveillance. The rapid growth first in mobile telephony and then in smartphones[58] has opened up tremendous possibilities not just for communication but for protection and assistance of migrants and refugees in need of support from HOs. However, as noted in the introduction to this article, it has also opened up tremendous possibilities for government surveillance, which has important consequences for how information and communications technologies (ICTs) are perceived and used by people whose situations render them vulnerable to detection or abuse. Oblivious to such concerns, some HOs appear to assume that persons in need of assistance are happy to hand over their personal data to whoever requests it, or that privacy is essentially a Western construct with little appeal in other cultures or contexts. However, in-depth research into the use of smartphones and social media networks by migrants and refugees *en route* to Europe conducted by The Open University and France

52 *Ibid.*, p. 8.
53 *Ibid.*, p. 7.
54 OCHA, *Humanitarianism in the Network Age*, OCHA Policy and Study Series, Geneva, 2013.
55 UN, *A New Global Partnership: Eradicate Poverty and Transform Economies through Sustainable Development: The Report of the High-Level Panel of Eminent Persons on the Post-2015 Development Agenda, 2013*, New York, 2013.
56 G. Hosein and C. Nyst, above note 29, p. 9.
57 *Ibid.*, pp. 56–58. Also see Kristin Bergtora Sandvik, Katja Lindskov Jacobsen and Sean Martin McDonald, "Do No Harm: A Taxonomy of the Challenges of Humanitarian Experimentation", in this issue of the *Review*.
58 According to research by the Open University and France Médias Monde, "98% of the population in the Middle East and North Africa use a mobile phone, 84% use a smartphone, 81% use internet connections, [and] 51% use a 'high-end' device (i.e. over $500)". See Marie Gillespie *et al.*, *Mapping Refugee Media Journeys: Smartphones and Social Media Networks: Research Report*, Open University and France Médias Monde, 13 May 2016, available at: www.open.ac.uk/ccig/research/projects/mapping-refugee-media-journeys.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

Médias Monde suggests this position is wrong.[59] It found, *inter alia*, that "fear both of surveillance by traditional institutions such as governments and soussurveillance [sic] by other group members among refugees" resulted in them "shrouding their identities on social media and online via use of avatars and pseudonyms";[60] that "refugees will not share personal information online, preferring to remain anonymous for fear of reprisals, surveillance, detention and/or deportation";[61] and that communication with family and friends was conducted "mainly on Whatsapp as they trust that it is not under surveillance as are Twitter and Facebook accounts".[62] Their lack of trust in both governments and State-funded institutions and organizations drove them "towards unofficial, potentially dangerous and exploitative resources".[63] Beneficiary communities far from the militarized borders of "Fortress Europe" and unfamiliar with the concept of data protection have also demonstrated significant concern about the capacity for different actors to use information in ways that may not be in their best interests.[64]

The risks of "aiding surveillance" do not end there. Among the documents released to journalists in 2013 by the whistleblower Edward Snowden were some which showed that the National Security Agency and Government Communications Headquarters, the key US and UK surveillance and intelligence agencies, had targeted HOs for surveillance. Those whose communications were intercepted included the United Nations Children's Fund, the United Nations Development Programme and Médecins du Monde.[65] It is safe to assume that if the United Kingdom and United States are doing this, other capable domestic and foreign intelligence agencies are also targeting HOs. This too has significant implications for

59 *Ibid.*

60 *Ibid.*, p. 13. The research stressed: "It is important to underline that, during the interviews with refugees, issues of trust and confidentiality were of paramount importance. Fear of being under surveillance and exposure – even by other refugees and not just the French authorities – was a key stumbling block when refugees were answering interview questions as well as in the more informal conversations that took place around the interviews." *Ibid.*, p. 43.

61 *Ibid.*, p. 17.

62 *Ibid.*, p. 48.

63 *Ibid.*, pp. 13–18. Consider also proposals by FRONTEX, the EU's Border Management agency, to develop a smartphone app to ensure the safety of people crossing the Mediterranean. Migrants' rights groups and privacy organizations pointed out that refugees were obviously unlikely to embrace an application that would make it easier for European governments to follow and intercept them. See Diane Taylor and Emma Graham-Harrison, "EU Asks Tech Firms to Pitch Refugee-Tracking Systems", *The Guardian*, 18 February 2016, available at: www.theguardian.com/world/2016/feb/18/eu-asks-tech-firms-to-pitch-refugee-tracking-systems.

64 Unpublished research conducted in Gaza by the author in 2015 (on file with author) found strong concerns about data protection in the form of frustration about international non-governmental organizations and international organizations conducting surveys and collecting personal information, including names and identity documents, never to return. This in turn led to suspicion on the part of local communities, who are increasingly distrusting of the motives of such organizations.

65 See James Ball and Nick Hopkins, "GCHQ and NSA Targeted Charities, Germans, Israeli PM and EU Chief", *The Guardian*, 20 December 2013, available at: www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner. See also Joan Tilouine and Simon Piel, "British Tapped UN and NGO Phones and Emails in Nigeria and Congo", *Le Monde*, 8 December 2016, available at: www.lemonde.fr/afrique/article/2016/12/08/british-tapped-un-and-ngo-phones-and-emails-in-nigeria-and-congo_5045681_3212.html.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

the operations and beneficiaries of those HOs. And although people who passively accept mass surveillance as "the way of the world" tend to comfort themselves with the naive assumption that it is largely passive – surveillance for surveillance's sake, as it were – it is also clear that various forces are quite prepared to disrupt the activities of HOs in pursuit of a political or military advantage. This could include locating or gathering intelligence on targets or adversaries, influencing civilian populations or undermining the distribution of aid, for example. Moreover, although people may be aware of the risks involved in sharing personal information, the risks involved in "metadata" collection and surveillance are much less well understood.[66] This in turn raises important questions as to the extent to which HOs must acknowledge the inherent risks in using new technologies to provide assistance and advise their beneficiaries accordingly as part of their protection mandate.

International Committee of the Red Cross (ICRC) staff members are among those now calling for concerted action to address these threats. Warning of the dangers of hacking by malevolent State and non-State actors, a 2016 post on the ICRC's blog cites the hypothetical yet by now familiar example of an online platform established by an HO to "crowdsource" real-time data about humanitarian needs and evidence of human rights abuses, and asks us to imagine such a platform being hacked or spoofed to create a false picture about who is attacking whom.[67] "A successful hack could rapidly reshape perceptions and change the course of conflict", the post observes.[68] The post also suggests that in the light of growing physical attacks on HOs, from medical convoys to facilities to staff, "norms are shifting, and agencies' reputation for neutrality is no longer guaranteed to offer protection".[69] As such, it may be "increasingly desirable to attack an agency's reputation directly" in order "to spread misinformation about the mandate, impact and purpose of its operations or the intentions of its staff".[70] Needless to say, this could have devastating consequences for the HO's staff, security, reputation and beneficiaries.

In February 2017, Brad Smith, the president of Microsoft, issued a call for a fifth "Digital Geneva Convention" to protect civilians on the internet and address the alarming growth of State-sponsored cyber-attacks, peacetime nation-State hacking, offensive "cyber-war" capabilities and the "weaponization" of software to achieve national security objectives.[71] While the idea has gained some traction in humanitarian circles, the failure to achieve anything but piecemeal reforms to the mass surveillance programmes revealed by Edward Snowden coupled with the

66 "Metadata" means data about data. Telecommunications metadata includes data such as the time, duration, origin and destination of phone calls, electronic messages, instant messages and other modes of telecommunication. This information can be used to build up a detailed picture about an individual's location, movements and contacts.

67 A. Kaspersen and C. Lindsey-Curtet, above note 1.

68 *Ibid.*

69 *Ibid.*

70 *Ibid.*

71 Brad Smith, "The Need for a Digital Geneva Convention", *Microsoft Blog*, 14 February 2017, available at: blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

troubling role of many technology companies in actually facilitating those programmes suggests that there will be no "quick wins" in this area.[72]

Data protection in humanitarian action

Building on its earlier work on privacy, aid and development, Privacy International's *Aiding Surveillance* provided a sharp corrective to the technological evangelism that was, quite understandably, sweeping the aid and development sectors at the time,[73] and made a foundational contribution to a wider discourse about the importance of data protection in humanitarian action. Between 2013 and 2016, Médecins Sans Frontières, the Cash Assistance Learning Partnership, OCHA, Oxfam, the UN Office of the High Commissioner for Refugees (UNHCR), the UN World Food Programme, UN Global Pulse and the ICRC all adopted data protection policies, rules governing data sharing, or responsible data use statements.[74] In 2015, the International Conference of Data Protection and Privacy Commissioners (ICDPPC) adopted a Resolution on Privacy and International Humanitarian Action (ICDPPC Resolution) – another first – reiterating that while data processing is an integral part of the performance of the mission of humanitarian actors, the adoption of data protection frameworks "by the overall humanitarian community is still scarce".[75] The ICDPPC Resolution spelt out some of the key challenges facing HOs seeking to comply with data protection law and principle. This included the collection of "sensitive data" (defined recently in the EU General Data Protection Regulation (GDPR) as personal data that reveal "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data"), whose collection is prohibited unless strict conditions and requirements are fulfilled.[76] The ICDPPC also suggested that monitoring and information management systems, electronic data transfers, ID systems and biometrics, mobile phone apps and drones – essentially the entire spectrum of humanitarian innovation – posed "specific privacy and security risks".[77] The ICDPPC Resolution warned that "humanitarian organizations not benefiting from privileges and immunities may

72 See Ian Brown, Mort Halperin, Ben Hayes, Ben Scott and Mathias Vermeulen, "Towards Multilateral Standards for Surveillance Reform", in Russell Miller (ed.), *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair*, Cambridge University Press, Cambridge, 2017.

73 See, Kristin Bergtora Sandvik and Maria Gabrielsen Jumbert (eds), *The Good Drone*, Routledge, London, 2017.

74 See Jos Berens, Ulrich Mans and Stefaan Verhulst, *Mapping and Comparing Responsible Data Approaches*, GovLab and Leiden University Centre for Innovation, June 2016, pp. 5–6.

75 37th International Conference of Data Protection and Privacy Commissioners, "Resolution on Privacy and International Humanitarian Action", Amsterdam, 27 October 2015 (ICDPPC Resolution).

76 GDPR, above note 48, Art. 9. The ICDPPC Resolution, above note 75, also notes that "data that would normally not be considered as sensitive under data protection laws may be very sensitive in [a] humanitarian emergenc[y] context". The GDPR is a binding EU law, while the ICDPPC Resolution is an advisory, "soft-law" measure.

77 ICDPPC Resolution, above note 75.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

come under pressure to provide data collected for humanitarian purposes to authorities wishing to use such data for other purposes (for example control of migration flows and the fight against terrorism)".[78] However, although the Resolution stressed numerous risks arising from data processing by HOs, and called for compliance with international data protection laws, it provided little in the way of guidance as to how specific challenges, including those unique to the sector, might be mitigated in practice. The same is true of many of the data protection provisions adopted by HOs. While the key principles of data protection have been transposed into formal policies, they often fail to provide clear guidance on how implementation can be achieved in the testing circumstances in which humanitarian action occurs. In July 2017, the ICRC and Brussels Privacy Hub made a huge leap in terms of filling this void with the publication of a *Handbook on Data Protection in Humanitarian Action* (ICRC Handbook).[79]

The remainder of this article considers some of the key data protection challenges facing the sector, drawing on the main topics raised in the ICRC Handbook. For illustrative and comparative purposes, the analysis draws on the data protection rules set out in the EU GDPR. Where the analysis refers more generally to "data protection laws", it is referring to common principles found in relevant national and international frameworks.[80]

There are several reasons for the focus on the GDPR. First, to compare data protection challenges with legal norms for data protection requires a baseline: in the absence of any wider and comparable international law or convention, EU law is chosen because it is widely regarded as the "gold standard". Moreover, as data protection laws continue to spread steadily across the world, it is highly likely that the EU will continue to set the standard. Second, the GDPR is the first data protection law to make any specific reference, albeit only in passing, to humanitarian action.[81] Third, even where HOs are working in countries with

78 *Ibid.*

79 Christopher Kuner and Massimo Marelli (eds), *Handbook on Data Protection in Humanitarian Action*, ICRC, Geneva, 2017 (ICRC Handbook).

80 This includes frameworks developed by the UN (UNGA Res. A/Res/45/95, "Guidelines for the Regulation of Computerized Personal Data Files", 14 December 1990), the CoE (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108, 28 January 1981 (entered into force 1 October 1985; Committee of Ministers, Recommendation No. R (99) 5 for the Protection of Privacy on the Internet: Guidelines for the Protection of Individuals with Regards to the Collection and Processing of Personal Data on Information Highways, 23 February 1999; Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Transborder Data Flows, ETS 181, 28 November 2001; Consultative Committee of the Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data, *Guidelines on the Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data*, 23 January 2017), the EU (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data), the Organisation for Economic Co-operation and Development (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 September 1980), Asia-Pacific Economic Cooperation (APEC Privacy Framework, 2004), and the Economic Community of West African States (ECOWAS Supplementary Act on Personal Data Protection 2010).

81 See GDPR, above note 48, recitals 46, 73, 112.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

weaker data protection laws, those that are headquartered in the EU, wishing to operate in the EU or transferring data into the EU will have to comply with the GDPR. Even organizations with privileges and immunities, which had hitherto considered their activities and records beyond the reach of these laws, can increasingly expect to have to demonstrate that they have adequate data protection policies if they wish to receive data from governments or HOs in EU member States.[82] Fourth, because data protection is so central to fundamental rights protection in the information age, it is suggested that as a community of actors committed to respect for human rights, HOs should aspire to the highest standards of human rights protection.

Legality of processing

Data protection laws set out "legitimate bases" or permissible "conditions for processing"; it is by definition illegal for HOs or any other data controller to process personal information in the absence of such a legal basis.[83] Top of the list of grounds is consent, which HOs have traditionally relied on as the basis for their own data collection activities. However, for many HOs, it is questionable whether the conditions under which that consent is obtained always meet the norm of "freely given", "unambiguous" and "informed consent".[84] This is because beneficiaries of humanitarian assistance programmes will often (though not always) have no real choice but to register and provide data should they wish to avail themselves of assistance. Moreover, data subjects should be informed as to how their data is being used, with whom it will be shared and for what purposes, and the consent should be recorded. But with multiple HOs frequently involved in aid distribution to displaced or besieged populations, and the tremendous practical challenges that may be posed by the novelty or scale of the emergency to which HOs are responding, providing this information to people in order to obtain their consent becomes quite a feat.

Therefore, HOs may wish to process data according to an alternative legal basis. Those international organizations with humanitarian mandates derived from international law may elect to process personal data in accordance with their

82 The GDPR only permits the transfer of data outside of the EU if the recipient State is the subject of an "adequacy decision" (meaning that it has been deemed to offer comparison-standard data protection) or is subject to binding data protection rules in the form of either standard contractual clauses drawn up by the European Commission or binding corporate rules approved by a data protection supervisory authority. *Ibid.*, Arts 44–48.

83 Within the EU framework, for example, data processing is only lawful if it is based on the consent of the data subject, a contractual requirement or a legal obligation; is necessary to protect the vital interests of the data subject or of another natural person; is necessary for the performance of a task carried out in the public interest or in the exercise of official authority; or is within the scope of the legitimate interests of the controller or a third party, unless such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data. On the lawfulness of data processing, see *ibid.*, Art. 6.

84 The EU defines consent as a clear affirmative act establishing a "freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her". *Ibid.*, recital 32.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

mandate functions, but for NGOs this is not an option. The EU GDPR tacitly advises HOs to use the "vital interests" of the data subject as a basis for processing,[85] but also states that this should only be done in cases "where the processing cannot be manifestly based on another legal basis".[86] Moreover, "sensitive data" – which may well be needed to provide vital services – may only be processed without consent where the data subject is physically or legally incapable of providing it, or in connection with public health laws or emergencies.[87] These inconsistencies leave HOs facing difficult decisions about when it is appropriate to seek consent and when it is not, and how to implement a sufficiently (and legally) robust process for obtaining and documenting such consent. HOs that do elect to process data in the "vital interests" of their beneficiaries – defined as things that are "essential for life" – will also have to ensure that such processing is necessary and proportionate (i.e., not excessive) to this purpose.[88] Those relying on consent will also have to implement enhanced procedures for children, with parental consent to data processing of children being the norm, while making practical provision for the withdrawal of consent, which should be as simple a process as giving it. And all HOs will have to facilitate the right of data subjects to object to the processing of their personal data and, where appropriate, to have their data corrected or deleted.

Transparency to beneficiaries

Transparency is fundamental to data protection and should be second nature to HOs committed to providing accountability to affected populations. Regardless of the legal basis for data processing, data protection laws require data controllers to render their data processing operations transparent to data subjects.[89] This is not only about informing consent; data protection laws grant data subjects the right to this information.[90] Under the GDPR, they "should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing", with "the specific purposes for which personal data are processed … explicit and legitimate and determined at the time of the collection".[91] The difficulties of providing such information to the beneficiaries of humanitarian action are obvious, and

85 *Ibid.*, recital 46.
86 *Ibid.*
87 In a humanitarian context, circumstances in which the data subject may not be able to provide consent may include situations when it is not possible to provide the requisite information about data processing to the data subject, circumstances in which the complexity of the processing may not be compatible with a free determination by the data subject, and situations where there is a significant power imbalance between data controller and data subject, with the latter offered no meaningful choice as to whether to provide their data. See ICRC Handbook, above note 79, Ch. 3.
88 The EU defines "vital interests" as those that are "essential for the life of the data subject or that of another natural person": GDPR, above note 48, recital 46. The ICRC Handbook, above note 79, offers a broader interpretation in its subsection 3.3.
89 See, for example, GDPR, above note 48, Arts 12–22, 34.
90 *Ibid.*
91 *Ibid.*, recital 39.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

compliance with even minimum standards may be difficult to achieve in practice.[92] While it is entirely legitimate for HOs to point to circumstances which make it difficult or impossible to provide beneficiaries with information about data processing at the point of collection, they cannot rely on the exigencies of a particular situation to disregard these obligations altogether. Instead, they will have to look to novel means to provide information to individual beneficiaries and beneficiary communities, including *post hoc* information campaigns, the revision and incorporation of data protection issues into individual counselling procedures and outreach programmes, and the use of helpdesks and ICTs to make information available to those who seek it.

These methodologies are particularly applicable to scenarios in which HOs collect data without knowing exactly how it will be used or shared, for example during population and vulnerability assessment surveys implemented at the outset of an emergency response. As noted above, and in order to guard against "function creep" (the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended), data protection law generally requires data controllers to specify the purpose(s) for which data will be used at the point of collection.[93] The challenge for HOs is to be as specific as possible, while retaining the flexibility to use the data for purposes that may only be determined as humanitarian responses unfold and develop. Where the purposes and/or partners change significantly, it could be necessary for HOs to inform beneficiaries, and depending on their consent procedures, to seek fresh or additional consent from data subjects. HOs therefore face another difficult judgement call as to where to draw the line. A single consent giving HOs *carte blanche* to use beneficiary data however they see fit, with no further consultation of the data subject, clearly breaches fundamental data protection principles, but obtaining additional consent for new data processing operations will inevitably have significant logistical, operational and resource implications. The key legal test is whether the processing is "compatible with the purposes for which the personal data were initially collected",[94] but if the purpose is deemed to be providing "humanitarian assistance", HOs may have wider scope in this area than other data controllers.[95]

Information security

The multiple risks that refugees, asylum-seekers and internally displaced persons face come from countries of origin, host States, transit and destination States (where those States enforce repressive exclusion policies), and malevolent third parties such as non-State armed groups, criminals and even "hacktivists" (those

92 According to the GDPR, "[i]t should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed".

93 See, for example, *ibid.*, Art. 13.

94 *Ibid.*, Art. 6(4).

95 See ICRC Handbook, above note 79, subsection 2.6.3.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

who engage in the subversive use of ICTs to promote a political cause or social change), among others. All of these adversaries could potentially use their personal data in ways that prejudice their best interests, expose specific groups or individual data subjects and their families to serious harm, or severely undermine the capacity of HOs to implement their mandates. Once beneficiary data has been collected, robust information security policies and practices are effectively the only thing that stands between HOs and vulnerable people and their potential adversaries.

Security in the field is trying enough, but the transition from physical files to digitized records via ICTs has created a new set of challenges for the humanitarian sector. Typically, a lack of technical expertise in the field has meant that local databases, solutions and innovations – which have been invaluable in delivering protection and assistance – have not always been developed or managed with information security in mind (to put it mildly). While central databases should offer much stronger data security, the breadth of access that it may be necessary to provide creates other vulnerabilities. In this respect, like all large organizations, HO's ICT users are their weakest link. Many lack basic information security training and, like a majority of ICT users, routinely engage in practices which undermine both their personal and organizational security.[96] This matters because the vast majority of successful ICT hacks do not exploit technical, "back-end" vulnerabilities (breaching firewalls, breaking into databases, etc.) but rely instead on some form of "social engineering" or psychological manipulation, such as tricking users or employees into handing over confidential or sensitive data by getting them to click on a bogus link or open an email attachment containing "malware" (software which is specifically designed to disrupt, damage or gain authorized access to a computer system). With the frequency and sophistication of these attacks increasing,[97] HOs should be making information security an integral part of field security and training their staff accordingly. While information security is already second nature to businesses with assets and reputations to protect, a cultural shift is still required in the humanitarian sector.[98]

It is something of a cliché, but the simplest way to achieve data protection is not to collect the data in the first place, or at least to collect only what you need. The next best option is to make sure the data is accurate and relevant, and to delete it as soon as it is no longer necessary. These principles are embodied in the concepts of

96 See Fran Howarth, "The Role of Human Error in Successful Security Attacks", *IBM SecurityIntelligence*, 2 September 2014, available at: securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/.

97 Symantec, "Extraordinary Attacks, High-Dollar Heists, Electoral Disruption", *2017 Internet Security Threat Report*, ISTR 22, April 2017.

98 A recent report on how international humanitarian actors manage risk states: "In terms of staff time and attention, the management of safety/security risk receives the most emphasis, with fiduciary risk management (prevention of fraud and diversion) ranking a close second. … The study found less overall emphasis and understanding of risk management in the areas of information security and legal (e.g., counter-terror legislation) compliance." See Abby Stoddard, Katherine Haver and Monica Czwarno, *NGOs and Risk: How International Humanitarian Actors Manage Uncertainty*, Humanitarian Outcomes and InterAction, February 2016, available at: www.humanitarianoutcomes.org/sites/default/files/ngo-risk_report.pdf.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

"purpose specification", "necessity and proportionality" and "data minimization",[99] yet various imperatives in the humanitarian sector are pushing in the opposite direction. Many HOs seem to be starting from the default position that personal data must be retained for long, indeterminate or even indefinite periods to satisfy auditing requirements.[100] Inflated claims about the power of big data (see further below) are also encouraging HOs to collect and retain more personal information than they should, and many have poor "digital hygiene" practices, leaving data trails that amplify risks to beneficiaries, instead of minimizing and restricting access to data that is legitimately needed for archiving purposes. Another cultural shift is needed to address these problems.

The maintenance of humanitarian archives poses a different set of data protection challenges. For certain HOs, there are numerous and compelling reasons, some set out in their mandates, to maintain detailed archives of their activities, not least that the information may be of critical importance to data subjects such as refugees, as well as their families, long into the future. The difficulty comes in balancing the importance of maintaining a "humanitarian memory" with the fundamental principles of data protection law. UNHCR, for example, has a long-standing Records and Archives Policy which states that individual case files should be kept indefinitely, and a new data protection policy which states that personal data should be deleted as soon as it is no longer needed.[101] To date, however, all personal data relating to UNHCR's beneficiaries has been considered part of their case files, so the working assumption is – contrary to the organization's data protection provisions – that everything should be kept forever. The public and private interest in keeping historical records about refugees is clear, but do the archives need to contain every last scrap of data about a person's time in a refugee camp, particularly when more and more data is collected? And what if someone later objects to the retention of particular records in their case file, and requests deletion in accordance with their fundamental rights? Autonomy is fundamental to data protection, but paternalism is endemic to humanitarianism; a suitable balance must be found.

Sharing and caring

Many HOs share personal data with third parties, including host governments, operational/implementing partners and commercial service providers, in order to facilitate or enhance the provision of protection and assistance. Though it is counter-intuitive for privacy and data protection advocates, it is important to stress that the pooling of data among HOs assisting displaced persons is not only

99 These principles are found in many data protection laws. See, for example GDPR, above note 48, Art. 5(1)(b) on purpose specification and Art. 5(1)(c) on necessity, proportionality and data minimization.

100 With the prospect of internal and external audit by States and other donors facing their programmes, many HOs appear fearful of deleting data, while deciding what to keep, what to throw out and securely destroying data can be costly.

101 See retention provisions in UNHCR, Policy on the Protection of Personal Data of Persons of Concern to UNHCR, May 2015, Art. 4(6).

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

a vital part of emergency response but can actually lower data protection risks by significantly reducing the amount of data that is collected and stored – and with it the "survey fatigue" that is often reported by those in need of assistance as a result of unnecessarily repetitious vulnerability assessments. However, in the absence of commonly applied data protection standards across the sector, such cooperation brings with it a raft of practical problems, while competition among HOs for funding, overlapping mandates and the politics of data ownership add a substantial layer of complexity. HOs also need to take more responsibility in their role as "gatekeepers" of sensitive information in response to increasing interest from the media, research institutes and private companies. In their desire to put a positive spin on refugee stories, or facilitate research that promises better understanding of refugees and their needs, HOs may not always take into account their legal obligations or the ethical implications of their actions.[102]

Data protection laws require that data subjects should provide explicit consent to the transfer of their data to another organization.[103] Data controllers must also ensure that all third-party recipients will properly protect the data, will only use it for specified purposes and will only receive the data they need to meet those purposes. Transfers should be regulated by legal or contractual agreement, and executed using secure communications channels – all of which is a far cry from how HOs have typically exchanged data in the past.[104] Data subjects must also be able to exercise their rights, and to obtain and seek redress in the event that things go wrong. Although the formalization of data-sharing arrangements to meet basic data protection standards has required a sea change in practice on the ground, these problems are not insurmountable. UNHCR's cash assistance programmes, for example, were the subject of a detailed data protection impact assessment resulting in innovative procedures for mapping data-sharing arrangements, assessing the adequacy of third-party data protection regimes, minimizing the amount of data that is shared, and concluding data-sharing agreements with a wide range of partners.[105]

102 See European Commission, "Guidance Note – Research on Refugees, Asylum Seekers & Migrants", Directorate-General for Research and Innovation, available at: ec.europa.eu/research/participants/data/ref/h2020/other/hi/guide_research-refugees-migrants_en.pdf.

103 Such provisions only generally apply if the recipient of the data will have control over how it is used. Organizations may transfer data to "sub-processors" to perform tasks on their behalf or under their direction, subject to appropriate safeguards. See, for example, GDPR, above note 48, Arts 6(1), 7, 28.

104 See, for example, the findings of a data protection impact assessment conducted for UNHCR which recommended that "[t]he transfer of refugees' personally identifiable data in unencrypted files and on media susceptible to loss or theft should be restricted to an absolute minimum. Where possible, the practice of e-mailing such files should be replaced with secure FTP channels or VPNs. If files are to be e-mailed, the practice of transmitting encrypted files and the passwords for those files in successive e-mails should also cease in favour of a more secure procedure. The medium-term objective should be the implementation of secure ICT solutions that allow partners to access and use UNHCR data (and correct or augment where necessary), but through which UNHCR retains much greater control". See UNHCR and Trilateral Research & Consulting, *Privacy Impact Assessment of UNHCR Cash Based Interventions*, Geneva, December 2015, p. 23, available at: www.globalprotectioncluster.org/_assets/files/tools_and_guidance/cash-based-interventions/erc-privacy-impact-assessment-of-unhcr-cbi_en.pdf.

105 *Ibid.* See also UNHCR, *Operational Guidelines on the Protection of Personal Data of Persons of Concern*, forthcoming 2018.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

The nature and extent of data protection risks related to data sharing does of course very much depend upon the type of data being shared and who the recipient is. Thus, sharing data with operational partners or service providers that have established solid data protection policies of their own may appear relatively low-risk, whereas cooperation with governments – whose policies toward migrants and refugees (or specific religious or ethnic groups) may change over time – is often perceived as higher-risk.[106] To navigate this landscape, it is crucial for HOs to properly assess the legal framework to which they and their local partners and service providers are subject, and analyze those laws through the prism of whether they could harm their beneficiaries. Such assessment often reveals the kinds of "positive disclosure" obligations discussed above, which are now found the world over and routinely risk undermining or prejudicing the fundamental rights of beneficiaries of humanitarian programmes. Some of the risks are obvious, like States requiring health service providers to inform public authorities about "conditions" such as HIV, TB or even homosexuality. Although HOs can and often do adopt a principled stance with regard to compliance with such laws, their local partners may not be in a position to do so. Other risks are far from obvious, such as those posed by international counterterrorism and anti-money-laundering regimes, which oblige all financial service providers to conduct "due diligence" on financial transfers and account holders.[107] This includes checking individual customers against hundreds of national and international sanctions lists – an activity that is frequently outsourced to "compliance" service providers and subject to the scrutiny of State financial intelligence units and national security agencies. Despite a growing awareness of the importance of data protection in the cash sector, it is far from clear that HOs, which have turned to cash assistance programmes in increasing numbers, are cognisant of the need to address this issue head-on with their service providers.[108] Because many sanctions lists are established by States that are party to a conflict or otherwise concerned with a situation of violence, the use of banks to deliver cash payments could inadvertently compromise the neutrality of HOs by embroiling them in sanctions enforcement.

A similar problem is posed by telecommunications registration and data retention regimes, which frequently oblige service providers to retain information about users, their communications traffic and even their content data, and make it available to law enforcement and security agencies. Prior to the advent of mobile telephony, obtaining these kinds of records often required a judge to serve a warrant on a phone company; today, all that may be needed is a mobile phone

106 UNHCR, for example, is often obliged to share basic biographical information about refugees registered in a host State, leaving little scope for data protection beyond seeking to minimize what is actually shared.

107 See Gavin Sullivan and Ben Hayes, *Blacklisted: Targeted Sanctions, Pre-emptive Security and Fundamental Rights*, European Centre for Constitutional and Human Rights, Berlin, 2011. Also see Ben Hayes *et al.*, *"De-risking": From Financial Surveillance to Financial Exclusion? Banking Problems and Solutions for the Non-Profit Sector*, Human Security Collective and Open Society Foundations, forthcoming 2018.

108 See Jessica Burniske, Naz Modirzadeh and Dustin Lewis, "Counter-Terrorism Laws: What Aid Agencies Need to Know", Overseas Development Institute, Humanitarian Practice Network Briefing Paper No. 79, November 2014.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

number. That surveillance is widespread and increasingly difficult to avoid does not, however, absolve HOs of their data protection responsibilities. On the contrary, the imperative is for them to recognize that beneficiary communications tools like bulk SMS messaging are particularly vulnerable to interception by State and non-State actors alike, to seek more secure alternatives where possible, and to ensure that their use does not compromise the neutrality of humanitarian action or the safety or security of their beneficiaries.[109]

As noted above, governments may also request data directly from HOs, or even assert jurisdiction or seize it against their wishes. Organizations that benefit from privileges and immunities have well-established rules for dealing with requests from governments and can assert various legitimate interests, including the fundamental rights of their beneficiaries, as a reason to refuse unwarranted requests.[110] Those HOs that do not benefit from such protections, and which have not made provision to mitigate against such eventualities, risk compromising not just the privacy but also the safety and security of their beneficiaries. In August 2017, it emerged that the Combined Homelessness and Information Network database, used by UK charities and government agencies to pool data and target interventions to support people sleeping rough, had been accessed by the Home Office to target foreign nationals for deportation.[111] The database, which is run by a homelessness charity, includes the location, nationality, mental health status and gender of rough sleepers.[112] Examples such as this – and there are others[113] – should serve as a cautionary tale for other initiatives that map vulnerability or provide "open data" sets that could be used for purposes other than those for which they were designed.

109 "Data collection on refugees should balance security and public safety with the need to preserve human dignity and rights. Governments and refugee agencies need to establish trust when collecting data from refugees. Technology companies should acknowledge their platforms are used by refugees and smugglers alike and improve user safety measures, and we should ask what it means for companies to have such politically charged data". Mark Latonero, "For Refugees, a Digital Passage to Europe", *Responsible Data Forum*, 8 February 2016, available at: responsibledata.io/for-refugees-a-digital-passage-to-europe/.

110 See, for example, UNHCR, *Guidelines on the Sharing of Information on Individual Cases: "Confidentiality Guidelines"*, Geneva, August 2001. Also see Els Debuf, "Tools to Do the Job: The ICRC's Legal Status, Privileges and Immunities", *International Review of the Red Cross*, Vol. 97, No. 897/898, 2016.

111 Mark Townsend, "Home Office Used Charity Data Map to Deport Rough Sleepers", *The Guardian*, 19 August 2017, available at: www.theguardian.com/uk-news/2017/aug/19/home-office-secret-emails-data-homeless-eu-nationals.

112 St Mungo's, "CHAIN – Combined Homelessness and Information Network", available at: www.mungos.org/work-with-us/chain/.

113 Further examples include publishing real-time data on the conditions, routes and profiles of asylum-seekers in the Horn of Africa region, which can inadvertently provide resources from which smugglers and human traffickers can benefit; mapping refugee movements during armed conflict, which may have been used to the advantage of parties to the conflict; failing to consider the risks involved in the publication of maps showing the geographical location of religious minorities or victims of sexual violence, which may render those groups or individuals vulnerable to further harm; and publishing statistics that demonstrate the provision of assistance to different ethnic, religious or national groups, which have given rise to accusations of preferential treatment. The first example cited here is described in Joseph Guay and Lisa Rudnick, "What the Digital Geneva Convention Means for the Future of Humanitarian Action", *UNHCR Innovation Service*, 25 June 2017, available at: www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/. Subsequent examples are derived from the author's work experience and are not publicly documented.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

Big data

In a landmark 2013 report, OCHA suggested that "[f]inding ways to make big data useful to humanitarian decision makers is one of the great challenges, and opportunities, of the network age".[114] The arguments martialled in support of big data-led innovation in the humanitarian sector are persuasive, particularly when underscored by the demonstrably poor information management that has hampered effective action and cost lives. But while there can be no doubt that this kind of innovation offers HOs the chance to remedy some basic failings and enhance effectiveness, OCHA's unfettered enthusiasm for correlating and analyzing "vast pools of information, generating surprising insights into the places [HOs] operate", was accompanied by a total blind spot when it came to data protection.[115]

Admittedly, data protection norms, with their relatively simple demands, are not easily accommodated by this brave new world, at least at first sight. Data protection demands purpose specification and limitation; big data wants to find new uses for data by turning it into "actionable intelligence". Data itself becomes the rationale for the collection and processing of personal data, and "function creep" is in-built as the *raison d'être* is to develop uses for data that were not foreseen at the point of collection. In turn, HOs are encouraged to use ever more complex targeting and eligibility assessments to identify and better serve the most vulnerable aid recipients, even though this inevitably increases the amount of data (including sensitive data) collected by HOs in order to profile individuals, families or households. Complexity makes it harder for beneficiaries to understand (and hence makes them unable to provide meaningful consent to) their involvement in big-data programmes, and specifically how their information is collected, used, stored, shared and analyzed. Crucially, layering and modelling dimensions of vulnerability to the *n*th degree may not be in their "vital interests" either. Using big-data analytics for eligibility decisions can also produce discriminatory effects that persons of concern may not be able to appeal. And it is not only individual rights that are at stake: big data can undermine their collective dimension by impacting whole groups of beneficiaries in negative or unforeseen ways.

These challenges are by no means limited to HOs: they are present wherever personal data is "mined" for insight and are particularly acute when accompanied by machine learning, profiling and automated decision-making. And though it appears that data protection legislation has been struggling to keep up, the GDPR introduces requirements with far-reaching implications for HOs developing these tools.[116] It states that "[e]very data subject should therefore have the right to know … the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing"; each

114 OCHA, above note 54, p. 26.
115 The phrase "data protection" did not appear anywhere in OCHA's 112-page document.
116 GDPR, above note 48, recitals 63, 71, Arts 4, 13, 14, 15, 22.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

subject also has "the right to obtain human intervention [and] an explanation of the decision reached after such assessment and to challenge the decision".[117]

Moreover, "[w]here possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data".[118] This set the tone for the *Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data* (Big Data Guidelines) issued by the CoE in January 2017, which urge data controllers to look beyond straightforward data protection to "preventive policies and risk assessments" that "consider the legal, social and ethical impact of the use of Big Data, including with regard to the right to equal treatment and to non-discrimination".[119] Mechanisms for HOs to achieve these objectives are considered further below.

Biometrics

Biometric ID systems are increasingly popular with HOs working with migrants and refugees because these organizations' beneficiaries often lack identity documents. By obtaining a unique identifier such as a digitized photograph, iris scan or fingerprint, biometric systems provide for more efficient registration procedures and, by speeding up entitlement checks and reducing fraudulent claims, faster and more equitable distribution of assistance. But as noted above, the GDPR explicitly defines biometrics as "sensitive data", and privacy and civil liberty campaigners have repeatedly expressed concerns about the development and implementation of biometric ID systems. This is due to both the scale of the data protection and security challenges that arise once personal data is linked to a biometric profile, and because biometrics are increasingly used as a tool of policing and immigration enforcement. Nevertheless, the demonstrable efficiency and accuracy of biometric profiling has taken precedence. Providing legal identity to the estimated 2.4 billion people who lack recognized identity documents is now a UN Sustainable Development Goal, providing additional impetus for the adoption of biometrics by States.[120] Crucially, although critics of biometric ID systems tend to focus instinctively on the implications of including individuals in a database, in development and humanitarian contexts, biometric registration drives may also engender social exclusion and even statelessness, as those identified as not entitled to citizenship or protection may be disenfranchised.

HOs deploying biometrics cannot ignore these wider concerns. UNHCR, for example, is currently rolling out its global Biometric Information Management System (BIMS) across its operations, providing an enduring digital identity that offers recognition to the excluded. UNHCR has also used the profiles it has collected to

117 *Ibid*., recital 63.
118 *Ibid*.
119 CoE, *Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data*, T-PD (2017) 01, Strasbourg, 23 January 2017 (Big Data Guidelines), p. 5.
120 UN Sustainable Development Goals, "Goal 16: Promote Just, Peaceful and Inclusive Societies", adopted 25 September 2015, para. 9.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

verify identity and entitlement in order to streamline food and cash assistance, and is rightly lauded for developing innovative and complex data-sharing arrangements with operational partners and the Jordanian banking sector. But as more and more of its stakeholders and partners implement or contemplate the introduction or use of biometrics, UNHCR has inevitably faced increased pressure to share or provide access to BIMS for more purposes than were initially foreseen – for example, for joint registration activities with host governments, or in the security vetting of successful resettlement candidates. Consequently, links between UNHCR's policies of inclusion and States' policies of exclusion are beginning to intersect, creating data protection and fundamental rights challenges that were not foreseen when BIMS was established. These challenges include the development of a biometrics policy that can reconcile the competing demands of different stakeholders, explaining the data flows and attendant risks to refugees and dealing with beneficiary and government claims over the data.[121]

Perception is crucial. Any suggestion that biometrics collected for humanitarian purposes could ultimately be used against the interest of their beneficiaries risks severely undermining the credibility, reputation and viability of entire programmes.[122] Even ostensibly "low-tech" biometric databases containing digitized photographs carry inherent risks due to the rapid development of facial recognition technology.[123]

Managing risk

Despite the myriad risks for HOs processing personal data and the evident difficulty that HOs have in terms of responsible innovation, it is by no means the case that these challenges are insurmountable. All data processing carries inherent data protection risks; the key thing is for data controllers to properly assess these risks from the outset and develop appropriate safeguards.[124] More than a means for

121 In 2017, the *Economist* magazine was moved to ask: "Will a refugee, who does not enjoy the protections of citizenship, be granted privacy rights to data stored in a cloud service?" See "Phones are Now Indispensable for Refugees", *The Economist*, 11 February 2017, available at: www.economist.com/news/international/21716637-technology-has-made-migrating-europe-easier-over-time-it-will-also-make-migration.

122 In 2016, *TakePart* magazine reported that "[c]ity officials in Calais announced in January that they would be clearing the Jungle [refugee camp] that month …. As an alternative, the city unveiled a new, official refugee camp, located on the Jungle's edge. … But few took the city up on the offer. The palm scanners spooked some of the residents, who worried their biometrics would be given to police and used against them if they managed to get to England." See Marc Herman, "Unwelcome Refugees", *TakePart*, 5 February 2016, available at: www.takepart.com/feature/2016/02/05/jungle-calais-france-demolition/.

123 According to the EU Fundamental Rights Agency, "[d]uring the latest period of arrivals of high numbers of refugees, private initiatives started to offer tracing services – particularly in big train stations in Austria, Germany and Hungary – using photos without considering data protection risks". See EU Fundamental Rights Agency, "Thematic Focus: Family Tracing and Family Reunification", available at: fra.europa.eu/en/theme/asylum-migration-borders/overviews/focus-family.

124 As Kaspersen and Lindsey-Curtet, above note 1, explain, "[b]eneficiaries need the best of both worlds: for more nimble and efficient ways of meeting their needs to be embraced by agencies with a history that inspires trust. For those agencies, that implies a willingness to self-disrupt in partnership with willing innovators – to constantly question the value of their ways of working, and think hard about the potential opportunities presented by technology to connect people, things, processes and data in new ways. But in seeking to harness the immense opportunities of technology to improve humanitarian aid, they also need to be conscious of some very real risks".

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

HOs to "do no harm", such assessment is becoming a legal obligation. The GDPR requires data controllers to conduct an assessment of the impact of envisaged processing operations on the protection of personal data where "new technologies" are involved and are "likely to result in a high risk to the rights and freedoms of natural persons".[125] Data protection impact assessments (DPIAs) must comprise "measures, safeguards and mechanisms" for risk mitigation and compliance with data protection law, and data subjects should be consulted.[126] DPIAs will be mandatory where data controllers intend to process sensitive data "on a large scale" (e.g. biometrics or health data). They will also be mandatory where processing is "systematic, extensive and automated", involving profiling that could "significantly affect the natural person".[127] Furthermore, where a DPIA "indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk", data controllers are obliged to seek prior approval for the processing from their data protection supervisory authority.[128] The more recent CoE Big Data Guidelines place a similar onus on data controllers to "[i]dentify and evaluate the risks of each processing activity" and assess their "potential negative outcome on individuals' rights and fundamental freedoms",[129] further encouraging ethical impact assessment with a view to preventing discrimination and social exclusion.

By conducting such assessments, HOs can mitigate risks in the design of their ICTs and devise forward-facing policies that offer meaningful privacy and fundamental rights protection to their beneficiaries. It must be hoped that they will also learn that it is much easier to do this at the design stage than to retro-fit data protection safeguards to systems that are already operational.[130] This is why the most recent EU and CoE legislation mandates privacy and data protection by design. Fortunately, these obligations are being imposed at a time when extensive innovation and research and development (R&D) has transformed these once aspirational concepts into highly effective models for information security and data protection. Anonymization techniques,[131]

125 GDPR, above note 48, Art. 35(1).

126 DPIAs must include a systematic description of the envisaged processing operations and their purposes of the processing; an assessment of the necessity and proportionality of the processing operations in relation to the purposes; an assessment of the risks to the rights and freedoms of data subjects; and the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with data protection law. *Ibid.*, Art. 35.

127 *Ibid.*, Art. 35.

128 *Ibid.*, Art. 36.

129 Big Data Guidelines, above note 119, p. 5.

130 DPIAs can still be very helpful in remedying data protection gaps in existing systems and programmes.

131 By stripping datasets of personally identifiable information (PII), or replacing PII with codes (pseudonymization), HOs can render their data much less vulnerable to misuse. While these techniques are by no means infallible – individuals can be "re-identified" from multiple anonymized datasets using data matching or similar techniques, posing a potential risk to individuals included in large aggregate datasets – used correctly they can significantly reduce risk. However, as noted above, anonymizing data in order to produce aggregate or statistical information that may be published, or at least shared more widely than personal data, may in certain circumstances entail acute protection risks for beneficiary populations: see above note 113.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

applied cryptography,[132] "zero knowledge" architecture[133] and new possibilities to put data under the meaningful and effective control of data subjects[134] now offer HOs the chance to develop ICTs that that are both highly effective and highly secure.

Conclusion: What kind of disruption?

While significant strides have been taken by the humanitarian sector in the four years since Privacy International pointed out the "paucity of privacy" in the aid and development sectors,[135] many HOs still have a great deal of work to do to meet the minimum standards for beneficiary data protection, information security and responsible innovation that are now embodied in not just the spirit but the letter of data protection law. Even those organizations that have led by example and adopted strong data protection policies still have a long way to go to ensure that these commitments are properly implemented across their operations. Building on the new ICRC *Handbook on Data Protection in Humanitarian Action*, which remains the only detailed guidance available to HOs, it is also vitally important that proactive discussions on global standards for collecting, sharing and storing personal data in times of crisis continue, and that data protection authorities assume greater responsibility for the development and implementation of workable standards. And while HOs, like all organizations, are understandably reluctant to discuss attempts to penetrate their information systems by State and non-State actors alike, they will have to find a way of collectively addressing this problem if they are to garner support for the zero-tolerance approach that international humanitarian law demands and the neutrality and effectiveness of humanitarian action requires. It remains to be seen if a "Digital Geneva Convention" is a viable response to these problems; in the meantime it is imperative that HOs take responsibility for properly securing their information systems and ensuring that their data cannot be used to undermine their neutrality or the rights and interests of their beneficiaries.

This fundamental challenge is at the heart of innovation and the embrace of new technologies in the humanitarian sector. It is a challenge that is both highly technical – requiring resources to be allocated to serious risk assessment and genuinely responsible innovation in tandem with R&D – and highly political, with the discourse around technological disruption in humanitarian action still very much characterized by a technological determinism that too often portrays or perceives data protection as a hindrance. Humanitarians are now expected to be in the "lab" as well as the "field", are told to ignore the new digital

132 Applied cryptography allows for the encryption of data at rest and in transit.
133 "Zero knowledge" architecture involves storage platforms which prevent the platform owner and unauthorized third parties from reading information stored in a database.
134 For example, personal information management systems and data autonomy and portability initiatives.
135 G. Hosein and C. Nyst, above note 29.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press

humanitarianism "at their peril",[136] and are threatened with a "drift into irrelevance" if they fail to "self-disrupt".[137] They are also cautioned that "[o]verly prescriptive and rigid frameworks derived from entirely different circumstances … have the potential to stifle discoveries" and advised to adopt "minimalistic" approaches in devising regulatory schemes.[138]

Of course, technology is nothing more than a solution looking for a problem, and it is clear that many tech providers are attracted to the humanitarian sector not simply because they want to do good, but because it provides a great opportunity to test their solutions in the real world. If responsible innovators within the humanitarian sector set the agenda, for example by seeking out highly secure communication and data storage solutions, this collaboration is invaluable. But when the agenda is set by other prevailing interests, there is a significant risk of policy incoherence, unintended consequences and negative externalities. The palpable desperation on the part of some tech companies to develop a blockchain-based identity management system for refugees,[139] for example, promises agencies like UNHCR more robust and versatile ID systems, but may also seriously risk exacerbating or entrenching the exclusion and disenfranchisement caused by the State policies described in the introduction to this article. Donors also play a fundamental role here: data protection is at last beginning to feature in financing agreements, but may be fundamentally compromised in practice by the over-prioritization of data-intensive initiatives such as cash transfer programming, biometrics and transparency and accountability mechanisms.

Until technological disruption and data protection in the humanitarian sector are framed as mutually reinforcing (rather than mutually exclusive), HOs will inevitably continue to be bounced into hasty procurement or deployment decisions that needlessly undermine or jeopardize the fundamental rights of their beneficiaries. Those who control the purse strings – both outside and inside HOs – could have the greatest impact by meaningfully prioritizing data protection and information security. If not, what is known in the trade as a "catastrophic data breach" may one day make them sit up and listen.

136 See, for instance, the book endorsements for Patrick Meier, *Digital Humanitarians: How Big Data is Changing the Face of Humanitarian Response*, Routledge, 2015, available at: www.digital-humanitarians.com/.

137 A. Kaspersen and C. Lindsey-Curtet, above note 1.

138 J. Berens, U. Mans and S. Verhulst, above note 74, p. 8.

139 "Microsoft and Accenture's Blockchain ID System for Refugees Highlights Data Privacy Needs", *ITU News*, 20 June 2017, available at: news.itu.int/blockchain-refugees/.

https://doi.org/10.1017/S1816383117000637 Published online by Cambridge University Press