International Review of the Red Cross (2021), **103** (916-917), 619–652.
Counterterrorism, sanctions and war
doi:10.1017/S1816383121000928

Biometric data flows and unintended consequences of counterterrorism

Katja Lindskov Jacobsen*
Katja Lindskov Jacobsen is a Senior Researcher at the Department of Political Science, University of Copenhagen, Denmark. Email: kj@ifs.ku.dk.

Abstract

Examining unintended consequences of the makings and processing of biometric data in counterterrorism and humanitarian contexts, this article introduces a two-fold framework through which it analyzes biometric data-makings and flows in Afghanistan and Somalia. It combines Tilley's notion of "living laboratory" and Larkin's notion of infrastructure into a framework that attends to the conditions under which biometric data is made and to subsequent flows of such data through data-sharing agreements or unplanned access. Exploring such unintended consequences, attention needs to be paid to the variety of actors using biometrics for different purposes yet with data flows across such differences. Accordingly, the article introduces the notion of digital intervention infrastructures, with biometric databases as one dimension.

Keywords: biometric data, infrastructure, humanitarian actors, counterterrorism, unintended consequences, living laboratories, data-sharing.

* Acknowledgements: This article has been underway for some time and many people have contributed in different ways, during various workshops (thanks to Lucy Suchman, Claudia Aradau, Rocco Bellanova and Linda Monsees among others) and seminars (thanks to several colleagues at the University of Copenhagen, particularly Kevin Heller and Anine Hagemann). The research was carried out as part of a Norwegian Research Council-funded project (DoNoHarm) – in the framework of which I was truly fortunate to work with amazing colleagues Kristin Sandvik (principal investigator) and Larissa Fast. Thanks also to Karl Steinacker for extremely valuable inputs and conversations over the years, to two very helpful student assistants at CMS, to three anonymous reviewers for very helpful and constructive comments, and to Editor-in-Chief Bruno Demeyere.

Digital intervention infrastructures: biometrics in counterterrorism and beyond

Biometric data – uniquely identifying biological characteristics like iris patterns or fingerprints[1] – are collected in several contexts. Particularly in the aftermath of 11 September 2001 (9/11), biometrics came to be viewed as an important counterterrorism technology. Illustrative of the imagined supremacy of biometrics as a counterterrorism technology, a former Central Intelligence Agency (CIA) officer noted, in November 2001, that "the use of biometric technologies might help make America a safer place," by protecting US citizens from terrorist attacks.[2] Today, biometrics is still seen as central to counterterrorism. A recent US program, for example, aims to develop systems capable of performing "biometric identification at long-range," in order to "recognize individuals under challenging scenarios," including from unmanned aerial vehicles.[3] Further illustrative of the imagined centrality of biometrics in US counterterrorism, a 2017 report from the Government Accountability Office (GAO) notes that between 2008 and 2017, U.S. Department of Defense (DoD) used biometrics "to capture or kill 1,700 individuals,"[4] who would allegedly otherwise represent a threat to US security.[5]

After two decades of counterterrorism biometrics, challenges have surfaced. Scholars have shown how technology-derived "accuracy" in enemy identification is problematic when mistaken for accuracy in political decisions about "who comprise legitimate targets for the use of violent force."[6] Challenges related specifically to biometrics have also become visible. Following the withdrawal of coalition forces

[1] Biometric data are "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural persons, which allow or confirm the unique identification of that natural person"; see European Union (EU), *General Data Protection Regulation, Regulation (EU) 2016/679,* 27 April 2016, OJ L 119, 4.5.2016, pp. 1–88, Art. 4(14); and EU, *Directive (EU) 2016/680*, 27 April 2016, OJ L 119, 4.5.2016, pp. 89–131, Art. 3(13). See Els Kindt, "A First Attempt at Regulating Biometric Data in the European Union", in Amba Kak (ed.), *Regulating Biometrics: Global Approaches and Urgent Questions*, AI Now Institute, September 2020, available at: https://ainowinstitute.org/regulatingbiometrics.html (all internet references were accessed in December 2021).

[2] John D. Woodward, "Biometrics: Facing up to Terrorism", Issue Paper IP-218, RAND Corporation, Santa Monica, CA, October 2001, available at: https://www.rand.org/pubs/issue_papers/IP218.html.

[3] See the BRIAR Program: Intelligence Advanced Research Projects Activity (IARPA), "Biometric Recognition and Identification at Altitude and Range", Office of the Director of National Intelligence, IARPA, available at: https://www.iarpa.gov/research-programs/briar.

[4] GAO, "DOD Biometrics and Forensics: Progress Made in Establishing Long-term Deployable Capabilities, But Further Actions are Needed", Washington, DC, 7 August 2017, available at: https://www.gao.gov/products/gao-17-580. See also Nina Toft Djanegara, *Biometrics and Counter-Terrorism. Case Study of Iraq and Afghanistan*, Privacy International, London, May 2021, available at: https://privacyinternational.org/sites/default/files/2021-06/Biometrics%20for%20Counter-Terrorism-%20Case%20study%20of%20the%20U.S.%20military%20in%20Iraq%20and%20Afghanistan%20-%20Nina%20Toft%20Djanegara%20-%20v6.pdf.

[5] For a critical assessment of how the collection of biometrics data has "been touted as uniquely suited to twenty-first century threats," see, for example, the detailed reports published by Privacy International, "Biometrics Collection Under The Pretext Of Counter-Terrorism", 28 May 2021.

[6] Lucy Suchman, Karolina Follis and Weber, "Tracking and Targeting: Sociotechnologies of (In)security," *Science, Technology & Human Values*, Vol. 42, No. 6, 2017. See also Christine Agius, "Ordering Without

from Afghanistan in August 2021, the Taliban gained access to biometric devices left by US forces, giving them access to biometric data through which persons registered by coalition forces in relation to training, salary payments or other collaboration could be identified. In this case, biometric infrastructures – as will be explained in this article – came with new forms of insecurity, thus challenging imaginaries of biometrics as straightforwardly delivering superior security. While this example is unique in many ways, additional examples appear if we consider the use of biometrics in other contexts and by other actors, including not only military but also humanitarian.

Exploring the use of biometrics in two different intervention contexts – Afghanistan and Somalia – diverse challenges and cross-cutting dynamics, logics and effects come into view. Whether resulting from biometrics falling into enemy hands, from biometrics being shared deliberately, or from real-world testing of unproven biometric modalities, both contexts illustrate how the use of biometrics may generate new risks and insecurity. Both contexts also illustrate how isolated analyses of either military or humanitarian biometrics risk overlooking the issue of data flows. In Afghanistan, not only soldiers but also humanitarian actors produced large amounts of biometric data. Also, in some contexts, data-sharing agreements enable biometric data flows between humanitarian actors and State security actors. Starting our enquiry from a perspective that attends to flows, the analysis explores different ways in which non-military biometric data flows might – intentionally or unintentionally – interrelate with counterterrorism infrastructures, e.g. at the level of data-sharing agreements (such as that between the United Nations High Commissioner for Refugees (UNHCR) and the U.S. Department of Homeland Security (DHS)).

Further, in many contexts, different actors test biometrics in ways that generate "success stories" which in turn feed into imaginaries of the accuracy and centrality of biometric data gathering and sharing. If viewed in isolation, we fail to appreciate how military and non-military actors contribute in different ways to an emerging digital intervention infrastructure. This article will more specifically focus on biometric infrastructures – as part of digital intervention infrastructures – as referring to the makings and flows of biometric data that make up an infrastructure of databases used and produced by different intervention actors, for different purposes, though sometimes with flows that enable the same data to be used across such differences. These biometric databases constitute an often-overlooked dimension of contemporary intervention infrastructures, an "infrastructure collecting, archiving and identifying digital biometrics."[7]

Bordering: Drones, The Unbordering of Late Modern Warfare and Ontological Insecurity", *Postcolonial Studies*, Vol. 20, No. 6, 2017.

[7] Following Jasanoff's definition, sociotechnical imaginaries are "collectively held and performed visions of desirable futures" that are "animated by shared understandings of forms of social life and social order attainable through, and supportive of, advances in science and technology." See Sheila Jasanoff, "Future Imperfection: Science, Technology, and the Imaginations of Modernity", in Sheila Jasanoff and Sang-Hyun Kim, *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power*, The

Following Brian Larkin, this article understands infrastructures as platforms that carry "not just water or cars" – in our case biometric data – but also desires, dreams or imaginaries[8] – in our case success stories or fear. But how and under what conditions are biometric infrastructures produced in the first place? To appreciate this, the article combines Larkin's notion of infrastructure with Helen Tilley's notion of "living laboratory" to foreground the real-world trialing of biometrics by different actors in various intervention contexts. During such trials, biometric data is produced, and so are "success stories" that potentially animate imaginaries of the presumed value to various intervention actors of biometric data (bases), thus potentially propelling quests for expanded biometric data-making and -sharing. By combining these notions of infrastructure and laboratory, the article asks under what conditions biometric intervention infrastructures are produced, and what flows they are comprised of and enable, including both biometric data flows (intentional or not) and the more invisible flows of success stories or fear.

After this introduction, the concepts of infrastructure and living laboratory are explained. Next follows an analysis of the makings and flows of biometric data, in Afghanistan and Somalia. The article concludes with a set of reflections on the broader relevance of these two cases and on the significance of exploring the making of digital intervention infrastructures – specifically, biometric databases – in a manner that attends to power relations and inequalities, including during (varyingly experimental) practices of data-making.[9]

Methodological reflections

Diverse sources were used to explore these biometric intervention infrastructures. Eleven semi-structured interviews were conducted with individuals from the International Committee of the Red Cross (ICRC), Food and Agricultural Organization (FAO), United Nations Office for Project Services (UNOPS), UNHCR and the World Food Programme (WFP), all of whom had experience with the use of biometrics in Somalia, Afghanistan or humanitarian programs more broadly. Interviewees include staff at different levels and in different locations. Given the sensitive nature of data-sharing questions and other aspects, interviews were made under conditions of anonymity. In addition, news stories, industry websites, expert reports and official documents were examined for

University of Chicago Press, Chicago and London, 2015, p. 25. On biometric data-sharing in the context of counterterror, see, for example, Privacy International, *Briefing to the UN Counter-Terrorism Executive Directorate on the Responsible Use and Sharing of Biometric Data to Tackle Terrorism*, London, June 2019, available at: https://privacyinternational.org/sites/default/files/2019-07/PI%20briefing%20on%20biometrics%20final.pdf.

[8] Brian Larkin, "The Politics and Poetics of Infrastructure", *Annual Review of Anthropology*, Vol. 42, No. 1, October 2013. See also Jana Hönke and Ivan Cuesta-Fernandez, "Mobilising Security and Logistics Through an African Port: A Controversies Approach to Infrastructure", *Mobilities*, Vol. 13, No. 2, January 2018.

[9] Rocco Bellanova, Kristina Irion, Katja Lindskov Jacobsen, Francesco Ragazzi, Rune Saugmann and Lucy Suchman, "Toward a Critique of Algorithmic Violence", *International Politics Sociology*, Vol. 15, No. 1, March 2021.

accounts of how biometric data is made and may subsequently flow. Sources cover the period from early uses in the aftermath of 9/11, to current examples from Afghanistan, recent data protection policies and data-sharing agreements. Neither Afghanistan nor Somalia are in-depth case studies. Rather, the article draws on examples from both contexts to illustrate trends of broader relevance, for example regarding how biometric data flows may generate insecurity.

Little information is available, and secrecy surrounds not just counterterrorism biometrics but also data-sharing agreements between donors and humanitarian agencies. In cases where the content of data-sharing agreements is not known, it is impossible to determine whether and what type of biometric data might be exchanged, which may not always be the case. For example, in Jordan biometric data is not shared with the UNHCR, whereas in the case of the U.S. DHS, such data is being shared.[10] It is certainly difficult, and not the aim here, to irrefutably prove direct links between non-military biometric data and counterterrorism uses of such data. Yet, simply disregarding the possible place of non-military biometrics in ongoing counterterrorism efforts risks contributing to the continued invisibility of such potential interconnections and the risks and insecurities that may result. Adding to the invisibility relating to biometric data flows, is of course also the invisibility of many of the people who suffer harm from the unintended consequences of such biometric data flows and from other unintended consequences of contemporary uses of biometrics in various intervention contexts.[11] Importantly, in addition to unpacking biometric data-makings and flows, it is crucial to unpack and remedy this type of invisibility, as some have indeed begun to do.[12]

Analytical framework: infrastructures and living laboratories

Infrastructural makings and flows: data and dreams

In exploring biometrics as part of broader digital intervention infrastructures, the analysis operationalizes two elements of Larkin's notion of infrastructure. First is

[10] Anonymous interview, November 2021.

[11] Keren Weitzberg, *Biometrics and Counter-Terrorism: Case Study of Somalia*, Report, Privacy International, 28 May 2021; Karen Fog Olwig, Kristina Grünenberg, Perle Møhl and Anja Simonsen, *The Biometric Border World: Technology, Bodies and Identities on the Move*, 1st ed., Routledge, Oxon and New York, 2020; Katja Lindskov Jacobsen and Larissa Fast, "Rethinking Access: How Humanitarian Technology Governance Blurs Control and Care", *Disasters*, Vol. 43, No. 2, 2019; Mirca Madianou, "The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies", *Television & New Media*, Vol. 20, No. 6, 2021.

[12] Gus Hosein and Carly Nyst, *Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives are Enabling Surveillance in Developing Countries*, Report, Privacy International, 2013; Human Rights Watch, "UN Shared Rohingya Data Without Informed Consent", 15 June 2021, available at: https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-08/2021-guidelines-for-authors-irrc.pdf; Adam Moe Fejerskov, Maria-Louise Clausen and Sarah Seddig, *Risks of Technology Use in Humanitarian Settings. Avoiding Harm, Delivering Impact*, Policy Brief, Danish Institute for International Studies, 17 August 2021; Elise Thomas, "Tagged, Tracked and in Danger: How the Rohingya Got Caught in the UN's Risky Biometric Database", *WIRED*, 12 March 2018, available at: https://www.wired. co.uk/article/united-nations-refugees-biometric-database-rohingya-myanmar-bangladesh.

Larkin's focus on flows. A crucial element of Larkin's approach is his definition of infrastructure as "socio-technical platforms for mobility," not simply mobility of people but more broadly of material and immaterial flows like cars and dreams, data and rumours, for example. Indeed, Larkin's approach invites us to study infrastructures with attention to their functions in terms of flows. Infrastructure, understood in this way, is not only to be studied with attention to processes that go into the makings – e.g. of biometric databases – but also with attention to flows enabled by these infrastructures. Second, is Larkin's emphasis on immaterial elements like imaginaries and desires. As Larkin writes, infrastructures "emerge out of and store within them forms of desire."[13] In our analysis, this for example translates into a focus on success stories as something, which dreams are made of, and thus as a type of "flow" which feeds into and animates broader biometrics accuracy imaginaries.

Accordingly, this article suggests a two-fold approach, attending to makings and flows of both biometric data and biometric success stories. Attending to flows encourages us to explore – rather than assume – how the emergence of biometric infrastructures affects relations between actors, e.g. by following how biometric data produced by one type of actor may flow into the realm of a very different type of actor. From this perspective, the article calls attention to various flows: between different humanitarian databases (with Somalia as the laboratory for interoperability[14]), between humanitarian and corporate actors, between humanitarian and counterterrorism actors, or unintended flows between coalition and "enemy" forces.

Living laboratory

Bringing Tilley's notion of "living laboratory" into the analysis of infrastructures enables us to pose questions that precede the focus on data flows, questions about the conditions under which biometric data was produced in the first place.[15] "Living laboratory" foregrounds the varyingly experimental character of many biometric uses through which data has been made. It also foregrounds the

[13] B. Larkin, above note 8. As opposed to a narrower focus on material dimensions only (roads, pipes, cables, etc.), Larkin suggests with his attention to dreams and imaginaries, that immaterial components are also important. In our case, success stories and imaginaries, that biometric infrastructures produce and carry, for example affect the future rollout (or not) of biometric databases.

[14] "The SCC [Somalia Cash Consortium] piloted biometric interoperability with WFP's SCOPE in 2018"; see Boniface Owino, *Harmonizing Registrations and Identification in Emergencies in Somalia*, Development Initiatives, Nairobi, 29 August 2019, available at: https://devinit.org/documents/67/Report_Harmonising-registrations-and-identification-in-emergencies-in-Somalia.pdf.

[15] Regarding the conditions under which biometric data is produced, several contexts deserve attention. Scholars have for example explored how force is experienced by Somali individuals in their encounters with biometrics in European asylum systems beyond Somalia: "Forced to have his fingerprints registered, Mukhtaar experienced first-hand what European humanitarian care could entail for asylum-seekers"; see Anja Simonsen, "Fleeting (Biometric) Encounters: Care and Control at Italian Border Sites", in Karen Fog Olwig, Kristina Grünenberg, Perle Møhl and Anja Simonsen (eds), *The Biometric Border World: Technology, Bodies and Identities on the Move*, 1st ed., Routledge, Oxon and New York, 2019, p. 135.

significance of attending to wider implications of more or less explicitly experimental technology uses and underlying rationales, like the risk of implicitly making certain locations into temporary laboratories considering the seeming acceptance of biometric technology testing in various intervention contexts.[16] Importantly, "living laboratories" are not spaces or conditions that simply exist in that capacity. Rather, Tilley invites us to explore how such spaces are created by external actors via particular assumptions and analogies that in turn legitimize specific practices.[17] While Tilley developed her analysis with reference to colonial Africa, living laboratory foregrounds dynamics of relevance to contemporary biometric experiments. Tilley for example notes that, when shifting to settings in Africa, this often meant that informed consent was then "rarely an explicit concern" – a silencing, which contributed to making Africa a seemingly appealing "living laboratory."[18] The issue of consent – often the absence of genuine consent – and arguably of the subsequent international legal obligation is an important consideration in relation to the making of biometric data in contemporary intervention contexts.[19] Thus, Tilley's analysis highlights the importance of adding questions about the makings of laboratory conditions to our analysis of biometric data flows. As such, "living laboratory" becomes an analytical lens through which to explore questions about various tensions and misfortunes of temporary real-world laboratories.

Combining the two, Tilley invites important considerations, including questions that precede the Larkin-inspired focus on flows of biometric data and immaterial components like success stories or fear: prior to exploring such flows, we should ask how biometric data is made in the first place, by whom and under what conditions? Thus, combining Tilley and Larkin, a two-fold analytical framework is developed. Accordingly, the subsequent analysis first attends to questions about "data-makings" (before data flows) by asking (a) by whom and (b) under what conditions, and second, explores the issue of "data flows," with attention to both (a) intended and (b) unintended biometric data flows.

[16] Tilley focuses on colonial Africa and how global power inequalities are (re)made in non-Western laboratories. She unpacks the entanglements of "fact-gathering" (p. 8) research and colonial-time "intelligence" (p. 4) to show how scientific endeavours were linked to broader colonial aims: Helen Tilley, *Africa as a Living Laboratory: Empire, Development, and the Problem of Scientific Knowledge, 1870–1950*, The University of Chicago Press, Chicago and London, 2011.

[17] H. Tilley, above note 16, p. 2.

[18] *Ibid.*, pp. 1–2.

[19] See, for example, Naomi Cohen, "'Do No Digital Harm': A Conversation on Handling Sensitive Data", October 2018, *The New Humanitarian*, where panelists discuss this issue of consent noting for example how: (a) "We deal with people that sometimes have a very low level of education or data literacy. How can we pass all these messages about new technology or even more basic messages? And from a data protection point of view, it is, how can we say that consent is informed and valid?" (panelist Maria-Elena Ciccolini); and (b) "The humanitarian space is probably home to what must be the biggest power asymmetry between the people who are gathering the data versus the people from whom the data is being gathered … I think the way in which we see the power asymmetry playing out is in ownership of the data." (panelist Zara Rahman)

Afghanistan and Somalia: analyzing biometric data-makings and data flows

Data-makings: (a) by whom

Afghanistan

Several sources indicate that by November 2019, the US military had gathered biometric data from "7.4 million identities," including several terror suspects.[20] During the first half of 2019, this data helped identify persons on the battlefield "thousands of times."[21] Indicative of the focus on biometric data collection, a US military document on *Employment of Biometrics in Support of Operations* has a section on "collectors," which notes that: "Almost every operation provides the opportunity to collect biometrics."[22] Specifically in Afghanistan, already by 2011, biometric data of "about more than 1.5 million Afghans" had been collected and stored in "databases operated by American, NATO [North Atlantic Treaty Organization] and local forces."[23] Considering the composition of this data, it becomes evident that this biometric data collection effort has a specific focus, namely on "males of fighting age, ages 15 to 64," of which "roughly one of every six" had been registered biometrically in this database.[24] But how was biometric data produced in the first place? Who was collecting it and how? Given the connection to intelligence gathering, it should be noted that such biometric data collection constitutes only a small part of the data-gathering practices of a much larger US intelligence infrastructure.[25] That of course applies to humanitarian actors too as they collect large amounts of data, with digital biometric data being just one type of data – but a particularly sensitive one given for example that one cannot easily get a new iris pattern, voice or fingerprint, combined with the ease

[20] Observers note that the DoD's goal was to register 80% of the Afghan population: see Annie Jacobsen, *First Platoon A Story of Modern War in the Age of Identity Dominance*, Penguin, Dutton, 2021. Others note that the DoD "stores biometric data on more than seven million people, mostly from war zones"; see Matthias Monroy, "NATO Establishes Biometric Database, US Military has it Already", *Matthias Monroy*, 8 November 2019, available at: https://digit.site36.net/2019/11/08/nato-establishes-biometric-database-us-military-has-it-already/; Thales, "Automated Fingerprint Identification System (AFIS) Overview – A Short History", *Thales*, 18 June 2021, available at: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/afis-history; Delores M. Etter, Jeniffer Webb and John Howard, "Collecting Large Biometric Datasets: A Case Study in Applying Software Best Practices", *CrossTalk*, May/June 2014, available at: http://jjhoward.org/pubs/collecting-large-biometric-datasets.pdf. It remains unknown to what extent the DoD reached its 80% goal.

[21] Dave Gershgorn, "Exclusive: This is How the U.S. Military's Massive Facial Recognition System Works", *OneZero Medium*, 6 November 2019, available at: https://onezero.medium.com/exclusive-this-is-how-the-u-s-militarys-massive-facial-recognition-system-works-bb764291b96d.

[22] Army, Marine Corps, Navy and Air Force, "Biometrics: Multi-Service Tactics, Techniques, and Procedures for Tactical Employment of Biometrics in Support of Operations", Air Land Sea Application (ALSA), April 2014, p. 7, available at: https://www.marines.mil/Portals/1/MCRP%203-33.1J%20BIOMETRICS%201.pdf.

[23] Thom Shanker, "To Track Militants, U.S. has System that Never Forgets a Face", *New York Times*, 13 July 2011, available at: https://www.nytimes.com/2011/07/14/world/asia/14identity.html.

[24] *Ibid.*

[25] Thanks to an anonymous reviewer for highlighting this important point.

with which large amounts of digital biometric data can be shared, which is not the case for paper files.

As alluded to above, US soldiers in Afghanistan have been collecting "fingerprints and iris patterns" from several individuals encountered in the field, assuming this would allow the US military to accurately "identify enemy combatants,"[26] for example by matching fingerprints of individuals in the field against templates stored in biometric databases including "watch lists of known or suspected terrorists."[27] Besides field encounters, "soldiers and police officers" have also collected biometrics (notably fingerprint and iris scans) from detainees, or from "local residents who apply for a government job, in particular those with the security forces and the police and at American installations."[28] At a more subtle level, biometrics have been collected by lifting off fingerprints "from a defused bomb or from remnants after a blast." Such fingerprint data was then subsequently used when checking the fingerprints of individuals encountered in the field or persons applying for jobs. According to General Petraeus, this practice was "very helpful in identifying who was responsible for a particular device in a particular attack, enabling subsequent targeting."[29] Biometrics was also used to control who was given access to US military bases.

Not only US soldiers but also various groups of Afghan officials have been collecting biometric data. At the Sarposa Prison in southern Afghanistan, for example, Afghan officials (using technology provided by the US) collected iris scans and fingerprints from militants and detainees.[30] Represented as displaying the usefulness of this data, the database was for example used to identify some of the 475 inmates who escaped this prison following an incident where the Taliban dug a tunnel system "right into the prison's political section where hundreds of Taliban were held."[31] Now, according to various sources, biometric data was important in identifying these individuals and getting them back into the prison: "Within days of the breakout, about 35 escapees were recaptured at internal checkpoints and border crossings; they were returned to prison after their identities were confirmed by biometric files."[32] Various other Afghan officials

[26] United States Government Accountability Office, "Defense Biometrics: Additional Training for Leaders and More Timely Transmission of Data Could Enhance the Use of Biometrics in Afghanistan", GAO Report Number GAO-12-442, 23 April 2012, available at: https://www.gao.gov/assets/600/590318.txt; see also Noah Schactman, "Army Reveals Afghan Biometric ID Plan; Millions Scanned, Carded by May", *WIRED*, 24 September 2010, available at: https://www.wired.com/2010/09/afghan-biometric-dragnet-could-snag-millions/.

[27] U.S. DHS, "Enhancing Security Through Biometric Identification", available at: https://www.dhs.gov/xlibrary/assets/usvisit/usvisit_edu_biometrics_brochure_english.pdf.

[28] T. Shanker, above note 23.

[29] *Ibid.*

[30] Spencer Ackerman, "Biometrics Help Nab Afghan Prison Escapees", *WIRED*, 14 July 2011, available at: https://www.wired.com/2011/07/biometrics-help-nab-afghan-prison-escapees/; T'ash Spenser, "Afghanistan Using Biometrics on Wide Scale for Security", *BiometricUpdate*, 9 July 2012, available at: https://www.biometricupdate.com/201207/afghanistan-using-biometrics-on-wide-scale-for-security.

[31] Jon Boone, "Afghanistan's Great Escape: How 480 Taliban Prisoners Broke out of Jail", *The Guardian*, 25 April 2011, available at: https://www.theguardian.com/world/2011/apr/25/afghanistan-great-escape-taliban.

[32] T. Shanker, above note 23.

also collected biometric data. Indeed, two main biometric projects were active in Afghanistan: one focusing on collecting biometrics from detainees "and what NATO calls 'other persons of interest',"[33] another focused on collecting biometrics from army and police applicants. Developed by the U.S. DHS and NATO, the "Afghan Automated Biometric Identification System" (AABIS)[34] was "administered by about 50 Afghans at the Ministry of Interior in Kabul,"[35] who collected "biometric data from army and police applicants,"[36] in order to "keep Taliban infiltrators out of the Afghan army."[37] Also focusing on army and police staff, the Afghan Personnel and Pay System (APPS), which was used by the Afghan Ministry of the Interior and the Ministry of Defense to pay the national army and police, also had a biometric component.[38]

Biometric data was also collected by various other actors. For example, Afghanistan's National Statistics and Information Authority collected fingerprints and iris scans when implementing the "e-Tazkira" ID-card system[39] with support from the World Bank.[40] The Independent Election Commission implemented biometrics in "an attempt to prevent voter fraud during the 2019 parliamentary elections."[41] Other actors also collected biometrics. In a 2019 report, the WFP notes that since initiating its biometric SCOPE system in Afghanistan, "more than 2.5 million beneficiaries have been registered."[42] Even earlier, the UNHCR started collecting biometrics from beneficiaries. In 2002, the UNHCR introduced mandatory iris recognition for millions of Afghans whom the refugee agency assisted in repatriating to Afghanistan from refugee camps in neighbouring

[33] Steve Gold, "Military Biometrics on the Frontline", *Biometric Technology Today*, Vol. 2010, No. 10, 2010.

[34] According to NATO, the aim of AABIS is "to monitor movements of militants around Afghanistan, as well as keep Taliban infiltrators out of the Afghan army" (*ibid.*). "[T]he data captured in the field is collated and used in real time and in the field then batch processed and relayed to Kabul where it is stored centrally and replicated to other databases across Afghanistan and back in the U.S." (*ibid.*).

[35] The database is maintained at the Ministry of the Interior; see Afghan War News, "Afghan Automated Biometrics Information System (AABIS)", available at: https://afghanwarnews.info/intelligence/aabis.htm.

[36] Federal Bureau of Investigation (FBI), "Mission Afghanistan: Biometrics. A Measure of Progress", 29 April 2011, available at: https://www.fbi.gov/news/stories/mission-afghanistan-biometrics.

[37] S. Gold, above note 33.

[38] Eileen Guo and Hikmat Noori, "This is the Real Story of the Afghan Biometric Databases Abandoned to the Taliban", *MIT Technology Review*, 30 August 2021, available at: https://www.technologyreview.com/2021/08/30/1033941/afghanistan-biometric-databases-us-military-40-data-points/. Critics have argued that this biometric system was, however, not very successful: Zack Kopplin, "Afghanistan Collapsed Because Corruption had Hollowed Out the State", *The Guardian*, 30 August 2021, available at: https://www.theguardian.com/commentisfree/2021/aug/30/afghanistan-us-corruption-taliban.

[39] "Even the national digital ID, the tazkira, championed by the World Bank since 2018 and required to access public services and jobs and to vote, can expose vulnerable ethnic groups"; see Rina Chandran, "Analysis – Afghan Panic Over Digital Footprints Spurs Call for Data Collection Rethink", *Reuters*, 20 August 2021, available at: https://www.reuters.com/article/afghanistan-conflict-tech-idUSL5N2OI06Y.

[40] Frank Hersey, "25K Afghan Biometric Passports Ready to be Issued, 100K More to Follow", *BiometricUpdate*, 7 October 2021, available at: https://www.biometricupdate.com/202110/25k-afghan-biometric-passports-ready-to-be-issued-100k-more-to-follow.

[41] E. Guo and H. Noori, above note 38.

[42] WFP, "Afghanistan Annual Country Report 2019. Country Strategic Plan 2018–2022", July 2020, p. 19, available at: https://docs.wfp.org/api/documents/WFP-0000113807/download/.

Pakistan. Upon returning to Afghanistan, each returnee had to undergo iris registration with the UNHCR.[43]

Though this list of actors who gather biometrics from various segments of the Afghan population is already long, it is not, however, an exhaustive list. Rather, the point is to illustrate the plethora of actors that for different purposes collect and store biometric data from Afghan individuals – whether from subjects that US soldiers suspect of being terrorists, or subjects who collaborate with US forces, whether in prison, or former UNHCR-registered refugees. Whilst these actors are indeed very different – sometimes opposed – what they share is a strong faith in biometrics as a tool to more effectively achieve diverse aims. But how does the collection and storing of biometric data potentially link these diverse actors in different ways? What happens when biometric data "travels" from one actor (with one purpose) to a different actor (and purpose)? When may such flows occur in contravention of data protection principles? What do biometric data exchanges or flows mean for the underlying contrasting security priorities – which one is eventually prioritized? How does biometric data collected by humanitarian actors flow once collected? Such questions were relevant even twenty years ago as the UNHCR was conducting biometric registration in the Afghan–Pakistan borderlands, which, for the UNHCR was a repatriation location, but for others, like the US military, a location of intense counterterrorism efforts with biometric identification as one of its central components. These are some of the questions that we return to later, after having explored another characteristic of these biometric data-makings, which is shared across various data-making actors: degrees of experimentation.

Somalia

In Somalia, US drone strikes intensified in 2019[44] and the US military remains focused on preventing "the use of Somalia as a safe haven for international terrorism."[45] Yet, in contrast to Afghanistan, Somalia is a counterterrorism location with few – at times no – US ground troops.[46] Appreciating this,

[43] The UNHCR sub-contracted the Pakistan National Database & Registration Authority (NADRA) to register the refugees, which means that the data was with the Pakistani Government and shared with the UNHCR. This is standard procedure until today. See UNHCR, "Government Delivered First New Proof of Registration Smartcards to Afghan Refugees", *UNHCR*, 25 May 2021, available at: https://www.unhcr.org/pk/12999-government-to-deliver-first-new-por-smartcards-to-afghan-refugees.html.

[44] Kim Helfrich, "Top Islamic State Official Dies in Airstrike", defenceWeb, 15 April 2019, available at: https://www.defenceweb.co.za/security/national-security/top-islamic-state-official-dies-in-airstrike/.

[45] Karl Wiest, "Commander of United States Africa Command Visits Somalia", *United States Africa Command*, 27 November 2018, available at: https://www.africom.mil/article/31366/commander-of-united-states-africa-command-visits-somalia.

[46] In 2017, US troops returned to Somalia for the first time since 1993, where eighteen US Special Forces died in a combat encounter. US troops were recently withdrawn, but US military engagements in Somalia continue by other means including drone strikes; see The Bureau of Investigative Journalism, "Drone Strikes in Somalia", *The Bureau of Investigative Journalism*, available at: https://www.thebureauinvestigates.com/projects/drone-war/somalia; Amnesty International, "Somalia: US Must Not Abandon Civilian Victims of its Air Strikes After Troop Withdrawal", *Amnesty International*,

important questions emerge concerning our analysis of biometrics in US counterterrorism interventions. Without soldiers on the ground in Somalia, how and by whom is biometric data then collected? Is biometrics even a significant component of US counterterrorism efforts in Somalia? Indeed, and again in contrast to Afghanistan, little information is available on how and to what extent the US military uses biometrics in Somalia. Yet, few accounts indicate that biometrics do play a role. For example, the practice of lifting off fingerprints from improvised explosive devices does not seem unique to Afghanistan. In May 2010, biometrics-enabled intelligence indicated: "a suspected member of a *Somali* Al Qaeda terrorist organization was trying to enter the US from Mexico."[47] Border control agents apprehended a person whose fingerprints flagged him as being "of extreme interest to the U.S. government,"[48] given that his "live" fingerprints, presented to scanners at this border crossing, "matched those of a suspected Al Qaeda bomb-maker that had been lifted during an improvised explosives device investigation and entered into BEWL [DoD's Biometric-Enabled Watchlist]."[49] Thus, even with no or very few US soldiers in Somalia, biometric data from members of Somalia-based Al Qaeda were still collected and stored in US databases. Examples like this indicate that biometrics may not be altogether unimportant to US targeting of terror suspects in/from Somalia.

Concerning US military actors, little information exists about their potential use of biometrics in Somalia. Yet, concerning Al Shabaab, a former US Navy SEAL noted, in 2017, "once militants are off the battlefield and in custody, program stakeholders collect defectors' biometric data."[50] It has also been noted how US military contractors biometrically register recruits.[51] Such accounts tentatively suggest that military actors and contractors produce biometrics from individuals in Somalia. Yet, as for the case of Afghanistan, looking only at biometrics collected for military purposes neglects the diversity of actors who for different purposes produce biometric data. Somalia, for example, hosts numerous humanitarian and development agencies who gather biometrics from various beneficiaries. Indicative of the extent of biometric data-making in Somalia, the WFP conducted a European Union (EU)-funded study to map "Somalia Databases," including biometric databases.[52] Thus, not only do military actors

7 December 2020, available at: https://www.amnesty.org/en/latest/news/2020/12/somalia-us-must-not-abandon-civilian-victims-of-its-air-strikes-after-troop-withdrawal/.

[47] Anthony Kimery, "Biometrics Play Significant Role in New US Army Intelligence Doctrine", *BiometricUpdate*, 22 September 2018, available at: https://www.biometricupdate.com/201809/biometrics-play-significant-role-in-new-us-army-intelligence-doctrine.

[48] *Ibid.*

[49] *Ibid.*

[50] Home Office, "Country Policy and Information Note. Somalia: Al Shabaab", UK Home Office, November 2020, p. 35, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/933800/Somalia-_Al_Shabaab_-_CPIN_-_V3.0e.pdf.

[51] Kyle Rempfer, "US Troops, Non-Profit Trainers and a 'Lightning Brigade' Battle for Somalia", *Military Times*, 21 May 2019, available at: https://www.militarytimes.com/news/your-army/2019/05/21/us-troops-nonprofit-trainers-and-a-lightning-brigade-battle-for-somalia/.

[52] WFP Somalia, "Somalia Databases and Beneficiary Registries for Cash Transfer Programming", *World Food Programme*, October 2018, available at: https://reliefweb.int/sites/reliefweb.int/files/resources/

collect biometrics (in little-known ways), various humanitarian actors also produce ("ideally interoperable" – see below) databases with biometrics from different parts of the Somali population. The UNHCR collects and stores biometrics from Somali refugees that they assist. By 2018, the WFP had conducted biometric registration of 1.6 million Somali beneficiaries.[53]

Other UN agencies also collect and store biometric data. The UN FAO runs "a biometrics-based fishermen database system in Puntland."[54] The UNOPS has biometrically registered frontline soldiers of Somalia's National Army. Interestingly, some UN agencies use contractors for the making of biometric data(bases) – notably to register populations in areas of Somalia that are difficult to access. As an interviewee noted, those carrying out biometric registration for a UNOPS program were contractors. This enabled them to bypass strict UN security regulations. In this sense, the making of biometric data simultaneously generated an implicit "risk-outsourcing." Besides contractors, the making of non-military biometric databases also involved local Somali staff: "we were training Somalis to use the [biometric] equipment since in some locations it was too dangerous for UN staff to do the registration ourselves."[55] Moreover, the African Union Mission to Somalia (AMISOM) has trained the Somali Police Force in biometric registration. The International Organization for Migration (IOM) has installed biometric scanners to collect fingerprints at eight border crossings in Somalia.[56] And in addition to – sometimes in collaboration with – various UN projects, researchers have produced biometric data, for example, whilst testing new biometric voter registration tools during the 2017 election in Somaliland. These examples are not an exhaustive list, but are meant to illustrate the breadth of military and non-military actors engaged in making databases with biometrics from individuals of Somali origin, including fishermen, border-crossers, refugees and frontline soldiers.

1555331373.Somalia%20Databases%20and%20Beneficiary%20Registries%20for%20Cash%20Transfer%20Programming.pdf.

[53] More recent data is not easy to get. Even interview persons working on biometrics with the WFP did not have updated numbers ready to hand.

[54] FAO of the UN, "Biometrics Information Transfer System", *Food and Agriculture Organization of the United Nations*, available at: https://www.itu.int/net4/wsis/archive/stocktaking/Project/Details?projectId=1386768611. A UN Security Council Resolution (UNSCR) describes this "biometrics-based fishermen database system in Puntland" as one of many counter-piracy initiatives, alongside "support Kenyan prisons." See UNSCR, Report of the Secretary-General on the Situation with Respect to Piracy and Armed Robbery at Sea off the Coast of Somalia, UN Doc. S/2013/623, 21 October 2013, p. 8. Adding to this is INTERPOL's database of Somali piracy suspects.

[55] Anonymous interview, December 2019.

[56] The IOM has deployed MIDAS "IOM Upgrades Biometric Fingerprint Scanners to Enhance Somalia's Border Management", *Reliefweb*, 6 June 2018, available at: https://reliefweb.int/report/somalia/iom-upgrades-biometric-fingerprint-scanners-enhance-somalia-s-border-management, which was developed for the Sahel. It has also supported for years the government in the issuance of ID cards; see Canada: Immigration and Refugee Board of Canada, "Somalia: Identification Documents, Including National Identity Cards, Passports, Driver's Licenses, and Any Other Document Required to Access Government Services; Information on the Issuing Agencies and the Requirements to Obtain Documents (2013–July 2015)", SOM105248.E, 17 March 2016, available at: https://www.refworld.org/docid/571f16dc4.html; FindBiometrics, "US-Backed NGO Project Enhances Biometric Border Screening in Mogadishu", *FindBiometrics*, 13 June 2018, available at: https://findbiometrics.com/us-backed-ngo-project-enhances-biometric-border-screening-mogadishu-506133/.

Data-makings: (b) under what conditions

Afghanistan

The first real-world "laboratory" in which the US military was testing counterterrorism biometrics was in Iraq. Specifically, the idea of "expanding biometrics for wholesale application on the battlefield was first tested in 2004 by Marine Corps units in Falluja."[57] Prior to that smaller trials had taken place, like testing biometric prototypes "in Iraqi detention centers in 2003."[58] While Iraq is not the focus of this article, it is important since "success stories" coming out of these biometric trials circulated beyond Iraq in ways that affected the use of counterterrorism biometrics in Afghanistan. As General Petraeus noted: "based on our experience in Iraq, I pushed this hard here in Afghanistan, too."[59] Though field tested before, various accounts suggest that also in Afghanistan, the use of biometrics was in some sense experimental, testing, for example, how biometric devices developed elsewhere would perform when used in the rough conditions of Afghanistan. It was, for instance, discovered that: "The hand-held [biometric] devices fail in the awesome heat of the Afghan summer."[60] Another dimension being tested was interoperability: "military officials acknowledge that the new systems fielded by American, coalition and Afghan units do not all speak to one another."[61]

Experimental dimensions underwriting these trials of biometric prototypes, application scale and other unproven aspects like interoperability were not exclusively conditions that characterized specific uses of biometrics by the US military. The World Bank, for example, provided "technical support to the [Afghan] Government on MSP [mobile salary payments] pilots"[62] where "biometric and biographic information of MoE employees receiving salary payments" was being registered.[63] Further, the UNHCR was testing biometrics.[64] In 2002, the UNHCR initiated a "first-of-its-kind UNHCR biometrics program

[57] Regarding this "trial": "The insurgent safe haven was walled off, and only those who submitted to biometrics were allowed in and out"; see T. Shanker, above note 23.

[58] N. Toft Djanegara, above note 4, p. 6.

[59] T. Shanker, above note 23.

[60] *Ibid.*

[61] *Ibid.* Further, it was observed that "the US military has made some mistakes with its biometrics technology, such as in Iraq, where soldiers collated a vast amount of data on civilians they encountered, but then discovered that one data-base does not work with another": S. Gold, above note 33.

[62] Concerning this pilot, the World Bank notes: "The existing legal and regulatory framework would need to be strengthened to fill existing gaps in terms of data privacy and consumer protection." The World Bank, "Combined Project Information Documents/Integrated Safeguards Datasheet (PID/ISDS)", The World Bank, 18 February 2019, p. 8, available at: https://documents1.worldbank.org/curated/en/591601550669552595/pdf/Project-Information-Document-Integrated-Safeguards-Data-Sheet-Payments-Automation-and-Integration-of-Salaries-in-Afghanistan-PAISA-P168266.pdf.

[63] The World Bank, *ibid.*, p. 8.

[64] Katja Lindskov Jacobsen and Karl Steinacker, "Contingency Planning in the Digital Age. Biometric Data of Afghans Must Be Reconsidered", *PRIO Blogpost*, 26 August 2021, available at: https://blogs.prio.org/2021/08/contingency-planning-in-the-digital-age-biometric-data-of-afghans-must-be-reconsidered/.

for Afghan refugees in Pakistan."[65] The system used anonymously stored iris scans to decide whether returning Afghan refugees had already received aid from the UNHCR once. Thus, "false positives" – where a person's iris is mistakenly matched against existing templates in the UNHCR's database – could mean that biometric failures would imply that the UNHCR erroneously denied aid to eligible but falsely matched returnees.[66] Beyond the case of Afghanistan, others have similarly noted with reference to biometrics how "deploying such sophisticated technologies in difficult environments has a high failure rate."[67]

Not only the UNHCR but also the WFP have been testing biometrics in Afghanistan: "WFP is currently trialing a ground-breaking initiative to take advantage of new technology in its food assistance efforts," running "6 e-voucher pilots," starting in May 2014.[68] Specifically, the WFP tested e-vouchers as "a new model of food assistance."[69] This e-voucher model had an important biometric component: "Biometric registration captures the fingerprint of the beneficiary to ensure verification of the intended beneficiary. […] which allows them to verify and accept payments for the food items purchased by the e-voucher recipient."[70] One challenge that was discovered during this US-funded e-voucher pilot was that in a few cases, "involving about 5% of beneficiaries," their "fingerprints could not be read by the biometric function of the POS [point of sale] machine because the recipients were elderly or had sent a representative who was not previously registered to redeem the e-voucher."[71] Despite – or rather alongside – discovering new knowledge about this and other challenges, the WFP pilot produced biometric data on approximately "70,000 food assistance recipients." For the WFP, the advantages of this new system were described with reference to accountability and inclusion benefits. Yet, as an interviewee noted about informed consent in another context: "what can be guaranteed to these recipients about where their data may potentially end up once collected?" Yet, international legal frameworks of course exist that are meant to guide use of biometrics, namely, through international human rights law and requirements such as consent and collection for specific purposes. We get back to the issue of risks stemming from potential biometric data flows in the next section.

[65] Irwin Loy, "Biometric Data and the Taliban: What are the Risks?" *The New Humanitarian*, 2 September 2021, available at: https://www.thenewhumanitarian.org/interview/2021/2/9/the-risks-of-biometric-data-and-the-taliban.

[66] Katja Lindskov Jacobsen, "Experimentation in Humanitarian Locations: UNHCR and Biometric Registration of Afghan Refugees", *Security Dialogue*, Vol. 46, No. 2, 2015.

[67] G. Hosein and C. Nyst, above note 12, p. 81.

[68] Katrin Fakiri, "Building a Gateway to Digital Payments in Afghanistan: The World Food Programme's E-Voucher Initiative", Case Study, Better Than Cash Alliance, New York, May 2016, available at: https://btca-production-site.s3.amazonaws.com/documents/185/english_attachments/Afghanistan_Case_Study_May2016.pdf?1463507198.

[69] See also, WFP SCOPE, "WFP's Beneficiary and Management System", WFP SCOPE, 16 January 2018, available at: https://www.globalinnovationexchange.org/innovation/scope-wfp-s-beneficiary-and-management-system.

[70] K. Fakiri, above note 68.

[71] *Ibid.*

Not only do biometric technology trials produce data that may subsequently circulate via (un)intentional paths. Moreover, attending to the conditions under which biometric data-making takes place will render visible another set of risks, including risks of technology failures as well as a more subtle production of subjects whose exposure to biometric failures is made to seem more acceptable than for other subjects.[72] Yet, despite accounts of risks and insecurity during two decades of biometric data production – and as others have also noted – there has, however, often been "minimal acknowledgement of the attendant risks,"[73] and limited attention to questions about how biometric data, once collected, can be deleted or otherwise secured from unwanted access, and to how meaningful consent can be obtained in the absence of answers to such questions. What are subjects consenting to when enrolled in humanitarian or other biometric databases? To indefinite retention of their data? To the sharing of their biometric data? As an interview explained (with reference to biometrics beyond Afghanistan): "we decided to remove the part about data deletion in our consent form. We cannot guarantee this."[74] So once registered with humanitarian actors like the UNHCR or WFP, do refugees know and consent to having their data stored indefinitely? What does that "laboratory" condition mean – not only during trial phases but also in subsequent implementation?

Somalia

Of these multiple actors, many use biometrics in Somalia in more or less experimental programs. For example, iris recognition for biometric voter registration in Somaliland was tested in a setup involving experts from the University of Notre Dame.[75] In previous trials, fingerprint registration was unable to solve the problem of "double-registration" – which refers to the same individual using a "system" twice, in this case to cast more than one vote. One aim of this new iris recognition trial was to generate knowledge about this double-registration problem whilst collecting biometric data as part of this trial, including the aim of developing a fraud-free voter registration checklist.[76] Trials conducted in Somaliland and elsewhere in Somalia not "only" produced knowledge about the reliability of iris technology for voter registration. Implicitly, Somalia risks being turned into as a "living laboratory," with increasingly larger parts of the Somali population produced as "test subjects." Trialing biometrics

[72] Katja Lindskov Jacobsen, "Making Design Safe for Citizens: A Hidden History of Humanitarian Experimentation", *Citizenship Studies*, Vol. 14, No. 1, 2010.

[73] Keren Weitzberg, Margie Cheesman, Aaron Martin and Emrys Schoemaker, "Between Surveillance and Recognition: Rethinking Digital Identity in Aid", *Big Data & Society*, Vol. 8, No. 1, 2021.

[74] Anonymous interview, September 2021.

[75] ACE, "Iris Biometric Voter Registration in Somaliland", *ACE Electoral Knowledge Network*, 3 December 2014, available at: https://aceproject.org/electoral-advice/archive/questions/replies/413937370.

[76] Stephen Mayhew, "Notre Dame Researchers Using Iris Recognition to Improve Accuracy of Somaliland Election Process", *BiometricUpdate*, 21 August 2014, available at: https://www.biometricupdate.com/201408/notre-dame-researchers-using-iris-recognition-to-improve-accuracy-of-somaliland-election-process.

under challenging conditions puts the technology "to test" but also poses challenges, for example, to ensuring informed consent. This challenge is not exclusive to the iris trial but applies to a broad range of varyingly experimental uses of biometrics in Somalia. As an interviewee noted with regard to non-military use of biometrics: "it's like dangling a lollipop," highlighting critical challenges to obtaining meaningful informed consent in contexts (refugee assistance, voting, etc.) where biometrics are trialed. Indeed, considering the position of vulnerability and lack of alternatives, one wonders whether consent in such circumstances can ever truly be genuine. As this interviewee explained: "giving consent is extremely complex: consent to having one's data stored? Shared? For what purposes?" Thus, biometrics trials not only produce new knowledge. They also produce beneficiaries (aid recipients, fishers, etc.) and other enrolled subjects (infants, voters, etc.) as seemingly acceptable test subjects.

Another example is infant fingerprinting. "Despite years of effort, reliable biometric identification of newborns and young children has remained elusive."[77] Yet, although critics note, among other things of concerns *vis-à-vis* infant biometrics, that they "would be surprised if the concept of toddler fingerprinting would be acceptable – or even attempted – in wealthy countries,"[78] infant biometrics trials were conducted in India: "This is the first time anybody has collected a longitudinal database of fingerprints for such a young population," said biometric expert Jain, from Michigan State University. Following this trial, Jain talked to the UN "about trialing the system with the World Food Programme."[79] Later, the WFP announced their decision to partner with experts from Michigan State University to set up a "proof of concept" trial to test whether child biometrics could solve what the WFP saw as a problem of different families "presenting the same children as their own, with the goal of getting more supplementary food rations."[80] The trial involved "taking the thumbprints of 150 children in three locations in Somalia over seven months."[81] During this trial, "evidence" of the reliability of child biometrics was produced. According to the WFP, the trial had demonstrated the feasibility of using biometrics to identify children under 5 years old, thus producing a "proof of concept" that animates visions of ever-expanding enrolment populations, now including children down to 5 years. The WFP trial also produced a call for "more research" to test the

[77] Steven Saggese, Yunting Zhao, Tom Kalisky, Courtney Avery, Deborah Forster, Lilia Edith Duarte-Vera, Lucila Alejandra Almada-Salazar, Daniel Perales-Gonzalez, Alexandra Hubenko, Michael Kleeman, Enrique Chacon-Cruz and Eliah Aronoff-Spencer, "Biometric Recognition of Newborns and Infants by Non-Contact Fingerprinting: Lessons Learned", *Gates Open Research*, Vol. 3, 2019.

[78] Ben Parker, "Betting on Biometrics to Boost Child Vaccination Rates", *The New Humanitarian*, 18 July 2019, available at: https://www.thenewhumanitarian.org/news-feature/2019/07/18/betting-biometrics-boost-child-vaccination-rates.

[79] Aviva Rutkin, "We Now Have the Tech to Fingerprint Babies – But Should We?", *New Scientist*,, 15 June 2016, available at: https://www.newscientist.com/article/mg23030782-200-we-now-have-the-tech-to-fingerprint-babies-but-should-we/.

[80] The New Humanitarian, "Syria Cash Aid Freeze, Somali Biometrics, and Poverty Porn: The Cheat Sheet", *The New Humanitarian*, 26 April 2019, available at: https://www.thenewhumanitarian.org/cheat-sheet/2019/04/26/syria-cash-aid-freeze-somali-biometrics-and-poverty-porn-cheat-sheet.

[81] *Ibid*.

reliability of biometrics for children under 5 years: "while biometric technologies have some application in children above 5 years of age, solutions at younger ages are largely experimental and require more research."[82] This call for further research echoes a broader logic where failures and limitations are countered by adding more of the same: more biometrics trials, more biometric data collection, more interoperability, more data-sharing. Both the proof of concept and the call for further research echo the U.S. DoD's vision of a future of ubiquitous biometrics, and in that way nourishes the vision of expanding biometrics as key to successful and presumably more ethical counterterrorism efforts.

As with "success stories" from Iraq feeding broader "dreams" and affecting the introduction of biometrics in Afghanistan, the case of Somalia is illustrative of somewhat similar dynamics. To explain how the idea of using biometrics in a specific UN project came about, an interviewee for example explained how UN Mine Action[83] had been using biometrics and that "success stories" from that had inspired other UN programs.[84] Various interviewees alluded to similar dynamics of biometric success stories circulating: "biometrics wasn't so popular when I worked on it. However, because of the success of this project, many other UN agencies jumped onto the bandwagon so to speak," adding that knowledge about the success of biometrics in a specific UN project "was for example shared during meeting amongst Heads of Programmes (FAO, UNODC [UN Office on Drugs and Crime], etc.), that is, within UN circles."

As an example of immaterial aspect of biometrics infrastructures, attending to such "success stories" is important for several reasons. They have effects as they, for example, animate a sense of confidence, in different UN projects, about the value of using this technology and encourage the use of biometrics in an increasing number of programs. Moreover, such UN-labelled success stories not only animate expectations in other UN programs but also beyond. They travel to industry websites to display the value and reliability of biometrics. As an interviewee, for example, explains: "our automated biometric identification system (ABIS) has been deployed by UNSOM [UN Assistance Mission in Somalia],"[85] showing how the technology helped the Somali Federal Government. Such biometric success stories may also animate existing faith in biometrics for counterterrorism. This vendor not only deployed its systems with UNOPS, but has also "won a Home Office [prize] for its work on a project to help counter terrorism," as a company with "close liaison" with the Ministry of Defence and NATO.[86] In these ways, "success stories" and other "knowledge" generated

[82] Unicef, "Biometrics: UNICEF Guidance on the Use of Biometrics in Children-Focused Services", *Unicef*, October 2019, available at: https://data.unicef.org/resources/biometrics/.

[83] An anonymous interviewee described how UN Mine Action "came into Somalia very early due to the nature of their work."

[84] Interview, December 2019. See also U.S. Department of State, *Country Reports on Human Rights Practices for 2011*, Washington, DC, 2012, p. 538.

[85] Human Recognition Systems, "Case Study UN Somalia", available at: https://www.hrsid.com/case-study-un-somalia?__hstc=90097796.566aa022561b6cdf11fa359f1b3a830f.1579511311374.1579511311374.1579511311374.1&__hssc=90097796.1.1579511311374&__hsfp=2488122038.

[86] S. Gold, above note 33.

during varyingly experimental uses of biometrics in Somalia animate visions of biometrics for counterterrorism. Yet, at the same time, critics have pointed out how "biometric initiatives in Somalia by various international actors have had dubious benefits and detrimental effects on local populations."[87] One lens through which to unpack certain dimensions of such "detrimental effects" is to look at what happens to the biometric data once it has been collected.

Data flows and after

Once all of the concerned actors have collected biometrics, how is this biometric intervention infrastructure then being used? While these actors share a common faith in the importance of biometrics for advancing their specific aim (refugee protections, emergency aid, counterpiracy, counterterrorism, etc.), Larkin's invitation to focus on flows – e.g. of biometric data – becomes an entry point for exploring what happens to the biometric data that these different actors have produced. Shifting from exploring the makings of biometric databases to exploring subsequent data flows, examples of intended and unintended data flows are presented below (with crucial difference in terms of the whom and how of such data-sharing).

Data flows and after: (a) intended – data-sharing agreements

Afghanistan

One example of deliberate exchanges of biometric data is the above-mentioned AABIS where data flows between the Federal Bureau of Investigation (FBI) and Afghanistan's Ministry of the Interior was an intended part of the system set-up. As described by the FBI, information sharing with partners like the FBI, was a "key component of the program [AABIS]," enabling critical data flows.[88] As such, AABIS represents an example of biometric data-sharing by design: "AABIS … is designed to be compatible with the U.S. DoD ABIS and the FBI Integrated Automated Fingerprint Identification System."[89] With the withdrawal of US troops and other coalition forces from Afghanistan in August 2021, several questions emerge. For example, will this biometric database, which one source tentatively put at approximately "8.1 million records," be retained or deleted?[90] If retained, what does this mean for the potential of biometric counterterrorism intervention infrastructures to alter frontiers by calling into question where

[87] K. Weitzberg, above note 11.

[88] FBI, "Mission Afghanistan: Biometrics. Part 4: A Measure of Progress", *FBI*, 29 April 2011, available at: https://www.fbi.gov/news/stories/mission-afghanistan-biometrics.

[89] AABIS: Afghan War News, above note 35. The centrality of such "data sharing with DoD and the Federal Bureau of Investigation" is also described by other sources, including a DoD report; see Office of the Secretary of Defense, "Justification for FY 2022 Afghanistan Security Forces Fund (ASFF)", May 2021, p. 42, available at: https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2022/FY2022_ASFF_Justification_Book.pdf.

[90] E. Guo and H. Noori, above note 38.

intervention ends, considering the potential for external actors' continued access to biometric data of millions of Afghan citizens. Crucially, this and other examples of biometric data-sharing in the context of counterterrorism must be understood against a wider backdrop of actors and initiatives that in different ways encourage biometric data-sharing, including UNSCR 2396 (2017), which requires States to "develop and implement systems to collect biometric data" in order to "responsibly and properly identify terrorists."[91]

Concerning Afghanistan specifically, highlighting the potentially fatal consequences of biometric data falling into the hands of the Taliban (see below) is important for several reasons. It may for example help accentuate the urgency of discussing how best to prevent further risks emerging for biometrically registered subjects in Afghanistan, including risks of retribution. However, at the same time, these discussions should not make us forget that intended data-sharing "by design" may also come with challenges, though sometimes more subtle. For example, the diverse actors who have collected and stored biometric data for different purposes may have a shared faith in the usefulness of biometrics. Yet, besides that shared faith are often crucial differences in logics and security priorities, for example (but not exclusively) between military and humanitarian actors. Acknowledging how logics, mandates and protection priorities of different biometric data-making actors do not always align, it becomes crucial to ask how their biometric data may flow – by intentional or unintentional paths. Importantly, how may such data flows affect these potentially un-align-able security priorities and, ultimately, the security of individuals whose biometric data may be accessed by agencies without the consent, let alone awareness, of the concerned individual? On that note it is interesting to observe how, in their annual country report on Afghanistan, the WFP notes about data-sharing agreements signed with four partners – the UNHCR,[92] International Rescue Committee, Norwegian Refugee Council (NRC) and Shelter Now International – that these agreements on the sharing of beneficiaries' data do not include biometric data.[93] The sensitivity of this data as well as the difficulty of ensuring that it remains in safe hands, despite data-sharing agreements that deliberately exclude biometrics, become evident from the following examples of unintended flows.

[91] Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, *Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?*, Human Rights Center at the University of Minnesota, July 2020; UN S/RES/2396(2017), 21 December 2017.

[92] Since 1985 the UNHCR has concluded and renewed memoranda of understanding (MoUs) at a global level; the last version is of 2018. See UNHCR and WFP, "Addendum on Data Sharing to the January 2011 Memorandum of Understanding between the Office of the United Nations High Commissioner for Refugees (UNHCR) and the World Food Programme (WFP)", 17 September 2018, available at: https://www.refworld.org/docid/5bbcac014.html. It includes, for the first time, provisions on data-sharing and states that both parties may give each other "access to biometric data of head of household and alternative assistance collector, and in exceptional cases, transfer of biometrics"; see UNHCR and WFP, "Annex 1: Matrix of Personal Data, Non-Personal Data and Information", 17 September 2018, available at: https://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=5bbcac204.

[93] WFP, above note 42.

Somalia

Some biometric infrastructures are set up to enable data flows within the humanitarian sector, for example to enable various humanitarian actors in Somalia to share biometric data internally.[94] Indeed, improved interoperability between various databases of humanitarian actors in Somalia was the focus of a report, which also describes the piloting of "biometric interoperability" between the WFP and the Somalia Cash Consortium. A specific focus of the aforementioned mapping of "Somalia Databases," including biometric ones, was to assess the "potential for data sharing and interoperability" and the making not just of biometric data, but on "making biometric collection standards."[95]

Another type of intended data flow occurs where data-sharing agreements are made. One example of data-sharing agreements enabling biometric data flows was the decision made by the EU in 2010 to share data on "suspected maritime pirates," including fingerprint data collected by EU Naval Force Somalia, with INTERPOL, allowing that biometric data "to be checked against INTERPOL's global databases."[96] More specifically on data-sharing agreements that enable biometric data collected by humanitarian actors to flow beyond humanitarian databases, a Privacy Impact Assessment highlights how the U.S. DHS "has been discreetly gathering the biometric information of tens of thousands of refugees, many of whom may never make it to America."[97] The biometric data was made available to the U.S. DHS "through a sharing arrangement with the United Nations High Commissioner for Refugees (UNHCR), which sends profiles to federal agencies when referring refugees for resettlement."[98] However, out of the almost 85,000 UNHCR referrals in 2018, less than a quarter of these referrals were accepted for resettlement.[99] Through data-sharing agreements like these, biometric data from "tens of thousands of refugees who are not admitted to the country" flows into DHS databases, stored "on Homeland Security's IDENT [Automated Biometric Identification System] database" and shared with various

[94] B. Owino, above note 14.

[95] K. Fakiri, above note 68.

[96] K. Weitzberg, above note 11.

[97] FindBiometrics, "The DHS and UNHCR are Sharing Biometric Data of Refugees", *FindBiometrics*, 23 August 2019, available at: https://findbiometrics.com/dhs-unhcr-sharing-biometric-data-refugees-082304/. "Under the 2019 MOU, UNHCR is now directly sharing biometric and associated biographic information with DHS Office of Biometric Identity Management (OBIM) Automated Biometric Identification System (IDENT) (soon to be replaced by Homeland Advanced Recognition Technology (HART))."; see U.S. DHS, *Privacy Impact Assessment for the United Nations High Commissioner for Refugees (UNHCR) Information Data Share DHS/USCIS/PIA-081*, 13 August 2019, p. 1, available at https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis081-unhcr-august2019.pdf.

[98] U.S. DHS, *Privacy Impact Assessment for the United Nations High Commissioner for Refugees (UNHCR) Information Data Share DHS/USCIS/PIA-081*, 13 August 2019, available at: https://www.dhs.gov/publication/dhsuscispia-081-united-nations-high-commissioner-refugees-unhcr-information-data-share.

[99] Eric Weiss, "DHS and UNHCR are Sharing Biometric Data of Refugees", *Find Biometrics*, 23 August 2019, available at: https://findbiometrics.com/dhs-unhcr-sharing-biometric-data-refugees-082304/. Qualifying this, an interviewee noted that "The Trump years were somewhat different. During the Obama years, 90% or more of the referred cases were accepted." (Interview, November 2021)

federal agencies.[100] IDENT is "a continually growing database that holds biometric information and other personal data on over 200 million people who have entered, attempted to enter, and exited the United States of America."[101] Also, critically, considering the aforementioned data-sharing agreement with the UNHCR, IDENT holds information of people who have never set a foot in the US.

Considering data flows in view of such data-sharing agreements invites a range of important questions, including questions about the reach of biometric counterterrorism infrastructures: to what extent might biometric counterterrorism infrastructures interconnect with biometric data stored by non-military agencies? Non-military biometric databases may not only be valued by donors who feel ensured that, with biometric registration, "assistance reaches the right people,"[102] but possibly also by counterterrorism actors.[103] As the ICRC notes in their Biometric Processing Policy, the agency is "aware of the value of biometric data in locating and identifying persons of concern to States and security," adding that the ICRC is conscious that State authorities have a significant interest in obtaining such data from organisations operating in humanitarian emergencies. This interest can extend to using biometric data for purposes that … may be incompatible with the neutrality, impartiality and independence of the ICRC, [including] counter-terrorism activities.[104]

Similarly, Privacy International argues that the value of biometrics gathered in aid programs "is not lost on intelligence agencies."[105] Further to this point, McDonald argues: "international intelligence operations realise the uniqueness of the data that humanitarian organisations collect."[106] While such concerns are not specific to Somalia but apply more broadly to humanitarian biometrics, the extent of non-military biometric data-making in Somalia, coupled with ongoing

[100] *Ibid.*

[101] Thales Group, "DHS's Automated Biometric Identification System IDENT – The Heart of Biometric Visitor Identification in the USA", *Thales Group*, 19 January 2021, available at: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/ident-automated-biometric-identification-system.

[102] National Independent Electoral Commission, Federal Republic of Somalia. "Voter Registration Feasibility Study Report", UNSOM, UNDP, Mogadishu, Somalia, November 2017, p. 31, available from: https://www.ec-undp-electoralassistance.org/wp-content/uploads/sites/24/2019/03/VR-Feasibility-Study-Report-Eng.pdf.

[103] The New Humanitarian, "Head to Head: Biometrics and Aid. One Timely Topic, Two Opinionated Views", *The New Humanitarian*, 17 July 2019, available at: https://www.thenewhumanitarian.org/opinion/2019/07/17/head-head-biometrics-and-aid. In this opinion piece, for example, note the following: "In 2019 the WFP's partnership with Palantir (a US company working with anti-terrorism efforts, the CIA, the police, and the US Immigration and Customs Enforcement) raised serious questions. Many believe that aid agencies are being naïve when entering into data partnerships with corporations and do not fully understand the implications."

[104] ICRC, "Policy on the Processing of Biometric Data by the ICRC", 28 August 2019, available at: https://www.icrc.org/en/download/file/106620/icrc_biometrics_policy_adopted_29_august_2019_.pdf.

[105] Kevin P. Donovan and Carly Nyst "Privacy for the Other 5 Billion: Western-Backed Biometrics Programs for the Developing World Could Put Data in the Wrong Hands", *Slate*, 17 May 2013, available at: https://slate.com/technology/2013/05/aadhaar-and-other-developing-world-biometrics-programs-must-protect-users-privacy.html.

[106] Sean McDonald, "From Space to Supply Chains: A Plan for Humanitarian Data Governance", *SSRN*, 12 August 2019, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3436179.

US counterterrorism efforts in Somalia, makes Somalia a particularly interesting context to explore not only the makings of biometric data, but also subsequent flows – and implications thereof. Indeed, other scholars have also, in analyses of humanitarian actors' use of biometric registration, highlighted various "concerns regarding data-sharing practices with states."[107]

Though difficult to prove, the significance of enquiring about potential infrastructural interconnections emerge when considering not only the role of donors (e.g. data-sharing agreements and requests) but also the role of corporations like Palantir.[108] Palantir is widely known for its role in US counterterrorism: its software has been "used by the CIA to identify terrorist and insurgent threats."[109] As Palantir explains, their technology "allows the military to have a more targeted response to threats."[110] Meanwhile, Palantir notes in a philanthropy report, how in three trial projects – one in Somalia – its data-analyzing tool "Foundry" helped the WFP automate data flows and "make precise, data-driven decisions to ensure its beneficiaries are reached."[111] Correspondingly, the WFP announced, in February 2019, that they had entered into a five-year partnership with Palantir.[112] Thus, not only warfighting but also humanitarian data in Somalia is on the radar of Palantir's top-level leadership. Besides criticism that this WFP–Palantir partnership could lead to "exploitation of the data in WFP's 'data lake'," including "beneficiary biometric data,"[113] the partnership also illustrates the significance of exploring the potential role of non-military biometrics in military counterterrorism. The WFP is the only humanitarian actor in Somalia with known partnerships with Palantir. Yet, the WFP is not the only non-military actor collecting biometrics from various parts of the Somali population.

Though the case of Palantir is exceptional (the WFP being the only humanitarian actor with known partnerships with corporations working with the US military on counterterrorism), the role of corporations in relation to the issue of control over biometric data is relevant beyond the WFP–Palantir partnership.

[107] Mirca Madianou, "The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies", *Television & New Media*, Vol. 20, No. 6, 2019, available at: https://journals.sagepub.com/doi/full/10.1177/1527476419857682.

[108] Privacy International, "One of the UN's Largest Aid Programmes Just Signed a Deal with the CIA-Backed Data Monolith Palantir", *Privacy International*, 12 February 2019, available at: https://privacyinternational.org/news-analysis/2712/one-uns-largest-aid-programmes-just-signed-deal-cia-backed-data-monolith.

[109] Charles W. Mahoney, "United States Defence Contractors and the Future of Military Operations", *Defense & Security Analysis*, Vol. 36, No. 2, 2020, p. 192.

[110] Steven Overly, "Peter Thiel's Company Palantir Defense Could Win Contracts Under Donald Trump", *Financial Review*, 9 November 2016, available at: https://www.afr.com/technology/peter-thiels-company-palantir-defense-could-win-contracts-under-donald-trump-20161109-gskz92.

[111] For the Palantir project in Somalia, see https://www.palantir.com/philanthropy-engineering/learn-more/wfp.html. The other two projects were in South Sudan and Uganda.

[112] WFP, "Palantir and WFP Partner to Help Transform Global Humanitarian Delivery", *World Food Programme*, 5 February 2019, available at: https://www.wfp.org/news/palantir-and-wfp-partner-help-transform-global-humanitarian-delivery.

[113] Linda Raftree, "A Discussion on WFP-Palantir and the Ethics of Humanitarian Data Sharing", *Medium*, 5 March 2019, available at: https://medium.com/data-stewards-network/a-discussion-on-wfp-palantir-and-the-ethics-of-humanitarian-data-sharing-4fc1499f81d8.

For example, the other issue is the data used through commercial service providers – cash programmes in particular. Were they cash programmes for very specific vulnerable groups who might be targeted by the Taliban, because they were war veterans, or sexual minorities – whatever it is.[114]

As a more general point, an interviewee from the aid sector raises the following question: "How to effectively implement data deletion when shared with so many different actors?" Importantly, even if large amounts of data may not have "flowed," the potential for such flows may have had negative implications. Besides data, immaterial things like rumours and fear (rather than dreams) also emerged and circulated, potentially affecting personnel on the ground who risk being "seen as collaborating with a CIA contractor," when gathering biometrics from beneficiaries, and to individuals in Somalia for whom "knowledge of this partnership" may deter them from seeking WFP assistance.[115]

If we consider flows of biometric data not just among aid agencies but within Afghanistan and Somalia more broadly, an additional type of potential flow emerges – the possibility, and the associated risk, of involuntary flows of humanitarian biometric data falling into the hands of armed groups.

Data flows and after: (b) unintended – in enemy hands

Afghanistan

A particularly noteworthy case of unintentional biometric data flows emerged as coalition forces left Afghanistan, in August 2021. Following their withdrawal, "the Taliban seized US military biometric devices that might help uncover people who worked with international forces, The Intercept reported."[116] "On August 27th, the Taliban boasted of using US digital identity technology to hunt down Afghans who had worked with the international coalition,"[117] specifically, the US military's Handheld Interagency Identity Detection Equipment (biometrics devices). This scenario entails significant risks to the many Afghan individuals who have had their biometrics data captured and stored in these biometric identification systems. For these Afghans, it means that "the Taliban have sensitive personally identifiable information that they have said they will use to target those they deem enemies or threats."[118] According to various sources, the Taliban regime "mobilized a special unit, called Al Isha, to hunt down Afghans who helped US and allied forces," and following the revelation of biometric

[114] I. Loy, above note 65.

[115] Andrew Young, "A Discussion on WFP-Palantir and the Ethics of Humanitarian Data Sharing", *MEDIUM*, 5 March 2019, available at: https://medium.com/data-stewards-network/a-discussion-on-wfp-palantir-and-the-ethics-of-humanitarian-data-sharing-4fc1499f81d8.

[116] I. Loy, above note 65.

[117] Emrys Schoemaker, "Digital Identity for Development – and Protection", *Global Policy*, 14 September 2021, available at: https://www.globalpolicyjournal.com/blog/14/09/2021/digital-identity-development-and-protection.

[118] *Ibid.*

devices left behind by coalition forces having fallen into the hands of the Taliban, one of the commanders of that unit emphasized in an interview "that his unit is using US-made hand-held scanners to tap into a massive US-built biometric database and positively identify any person who helped the NATO allies."[119]

Others have highlighted the dangers confronting Afghans whose biometric data may have become accessible to the Taliban regime in whose eyes they are traitors, for which they may be punished. With biometrics, "erasing" such traits in order to remain safe in a Taliban-ruled Afghanistan is impossible: you cannot change the pattern of your iris. It remains to be seen what the Taliban will do with this data and with these devices. How and where, if at all, might they for example "use it to check whether an individual has collaborated with coalition forces?"[120] While this story first broke in the August of 2021, concerns had been raised ten years earlier: "Some Afghans are concerned that in the future the growing biometric database could be abused as a weapon."[121] Importantly, concerns about unintended consequences of data flows on civilians have been highlighted in a report by the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Professor Fionnuala Ní Aoláin. Specifically the report mentions how "Aside from the threat of misuse, in particular by oppressive and/or authoritative governments, concerns have also been raised regarding the collection of biometric data on vulnerable populations and persons in vulnerable situations, in diverse contexts." Specifically concerning Afghanistan, the Special Rapporteur noted not only how "the United States and some of its allies proceeded to collect biometric data of populations in conflict zones, such as Iraq and Afghanistan," but also that since 2007, human rights organizations have cautioned that these biometric databases "could become a 'hit list' in the wrong hands,"[122] posing risks to "millions of Afghan and Iraqi citizens who have never been accused of any wrongdoing."[123]

As Larkin reminds us, we should not only attend to material flows but also to immaterial elements. Even if massive amounts of biometric data may not have been flowing to, let alone actively used by the Taliban, the potential infrastructural interconnection that became visible with stories circulating of the Taliban having access to coalition biometrics may indeed have generated immaterial "flows," notably in the form of "rumours" and "fear" (rather than desires and dreams).[124] Indeed, it is crucial to take seriously how not only data

[119] Siddharthya Roy and Richard Miniter, "Exclusive: First-Ever Interview With Terror Leader who's Hunting Americans and Allies in Afghanistan", *Zenger News*, 28 August 2021, available at: https://www.zenger.news/2021/08/28/taliban-team-is-using-us-made-biometric-database-and-scanners-to-hunt-american-and-afghan-enemies/.

[120] K. L. Jacobsen and K. Steinacker, above note 64.

[121] T. Shanker, above note 23.

[122] K. Huszti-Orbán and F. Ní Aoláin, above note 91, pp. 6–7.

[123] K. Huszti-Orbán and F. Ní Aoláin, above note 91.

[124] Thomas Macaulay, "Fears Grow Over Taliban Using Biometric Systems to Identify US Collaborators", *TNW News*, 18 August 2021, available at: https://thenextweb.com/news/fears-taliban-has-seized-us-biometric-systems-will-target-vulnerable-people-afghanistan.

flows but also fear can have potentially negative consequences, like if a person decides not to go to hospital out of fear that the Taliban may require that person to undergo biometric screening. In such cases, even if potential biometric data flows and subsequent uses may not all materialize, the emergence and flow of fear need to be taken seriously as potentially affecting biometrically registered persons' security negatively. Such questions are relevant for all actors who collect biometrics in Afghanistan (and elsewhere). Once collected, can it be guaranteed that this sensitive data (you can never get a new iris) will not fall into "enemy hands" or otherwise into the hands of actors who may use it for other purposes than originally intended?

Summarizing these examples from Afghanistan, looking across military, humanitarian and other actors – as an infrastructure perspective invites us to do – highlights important challenges. For example, how neither storing of identifiable biometric data by coalition forces, nor anonymized data in UNHCR databases, offer an easy solution to difficult questions about what "safe" biometrics may look like. For the UNHCR, anonymized data generated different risks (of failures translating into humanitarian failures to assist). Asking new questions like how do (intentional or unintentional) biometric data flows alter the security aims guiding the use of such data? Interoperability is not simply a technical issue, not just a matter of infrastructural platforms that enable data flows, but also a question of how such flows carry and constitute imaginaries, including hierarchies of whose lives are important/unimportant from different security perspectives. What diverse, sometimes diametrically opposed, security perspectives does the flow of biometrics "erase" or what hierarchies do these flows reinforce or constitute or reshape? Moreover, how do success stories travel, and with what implications for the rollout of biometrics in new contexts or expansion of biometrics in existing contexts?

Somalia

Concerning flows of biometric data within Somalia there are also risks of involuntary flows of humanitarian biometric data falling into the hands of actors who may use this data not to enhance but to jeopardize the security of the individuals whose links to Western actors may be perceived negatively. As an interviewee, working for a UN agency in Somalia, notes: "Al Shabaab could misuse it if they were able to identify someone e.g. as a beneficiary of aid from western organizations (whom they see as their enemy)." A risk, which meant that this UN agency decided to reconsider the kind of biometric device that they were using: "We had these big bulky registration machines. But they looked too suspicious, so we found another type of registration device that looks more low-key and less suspicious, if our staff got stopped by Al Shabaab when carrying one of these devices."

Besides data-sharing and partnership agreements, data flows from humanitarian to State security actors may emerge from a very different type of involuntary interconnection. Though impossible to verify, interviewees and news stories claim that defense agents may be among those who carry out cyber-attacks against UN database to enable involuntary flows of data. According to McDonald, humanitarian organizations are not only limited in their ability to safeguard the biometric data they store. They are also "a target for a range of digitally savvy groups," including "international intelligence services."[125] As noted by an interviewee, highly placed within a central humanitarian organization: "it would not surprise me if those involved in doing counter-terror were the same people as those involved in hacking into our [humanitarian] database. Attacks on our database is an ongoing challenge, and we are really struggling to have some minimum cybersecurity."[126] Accentuating this, a journalist revealed how, in 2019, UN networks in Geneva experienced a "major hacking attack."[127] According to a cybersecurity expert, the attack had "the hallmark of a sophisticated threat actor," adding that "nation-states are frequently the most sophisticated threat actors."[128] This incident illustrates how humanitarian actors' biometric databases are vulnerable to unauthorized access,[129] with hacking incidents resulting in unintended data flows. Whilst cases of unauthorized access to humanitarian databases are not unfamiliar to technology providers or to humanitarian actors,[130] the extent of this vulnerability remains elusive. Aid agencies, "like any business with a reputation to protect, have the incentive not to admit when they have been hacked."[131] These different data flows – to Al Shabaab, the DHS, or hackers – remain largely invisible for various reasons, like the nature of these being confidential programs, the embarrassment associated with acknowledging to have been hacked, and possible difficulties in contradicting a widespread imaginary of biometrics as valued in counterterrorism, refugee assistance and many other intervention contexts.

Importantly, several actors have highlighted how these challenges and crucial unintended consequences are not unique to Afghanistan and Somalia, but indicative of much wider challenges. A UN Special Rapporteur thus stresses how "sharing data with governments that have lower rule of law or human rights standards would risk contributing to human rights violations, going against States' obligations under international human rights [and domestic] law."[132]

[125] Sean McDonald, "From Space to Supply Chains: A Plan for Humanitarian Data Governance," *SSRN*, 12 August 2019, available at https://ssrn.com/abstract=3436179.

[126] Anonymous interview, August 2020.

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

[128] *Ibid.*

[129] Katja Lindskov Jacobsen and Larissa Fast, "Rethinking Access: How Humanitarian Technology Governance Blurs Control and Care," *Disasters*, Vol. 43, No. 2, 2019.

[130] Ben Parker, "Security Lapses at Aid Agency Leave Beneficiary Data at Risk", *The New Humanitarian*, 27 November 2017, available at: https://www.thenewhumanitarian.org/investigations/2017/11/27/security-lapses-aid-agency-leave-beneficiary-data-risk.

[131] Anja Kaspersen and Charlotte Lindsey-Curtet, "The Digital Transformation of the Humanitarian Sector," *Humanitarian Law & Policy*, 5 December 2016, available at: https://blogs.icrc.org/law-and-policy/2016/12/05/digital-transformation-humanitarian-sector/.

[132] K. Huszti-Orbán and F. Ní Aoláin, above note 91, p. 11, footnote 67.

Also, other critics have for example stressed how "gathering digital ID and biometric data carries particular risks for vulnerable groups who face conflict or oppression: their data could be shared or leaked to hostile parties who could use it to target them."[133] Thus, whilst Afghanistan and Somalia are important contexts in which to explore unintended consequences of biometric data-makings and flows, the concerns that emerge are illustrative of far broader challenges.

Afghanistan, Somalia and beyond

While Afghanistan and Somalia are unique in many ways, exploring biometric data-makings and flows with reference to examples from these two contexts can generate insights of broader relevance.[134] On example of this is the paradox that although several challenges relating to biometric experimentation, data-making and intended/unintended data flows have surfaced – particularly risks related to the security and confidentiality of civilians – faith in the presumed centrality of biometrics as a counterterrorism and wider intervention technology seems largely intact. Several actors in diverse intervention contexts still collect, store and share biometric data, often on a large scale. Looking ahead, what does this sustained faith in biometrics, amidst growing examples (from Afghanistan, Somalia, and elsewhere) of how biometric data may cause risks and insecurity, imply for actors engaged in the making of biometric intervention infrastructures? On the one hand, we have seen the emergence of new biometric policies that explicitly move away from biometric data collection. Oxfam's Biometric Policy, for example, specifies that when deciding whether biometric data processing is appropriate, it is imperative to ensure that "the likely flow of data is knowable and known," meaning that it is necessary to understand "who will have access to data throughout its life."[135] The ICRC's Biometrics Policy (2019) "requires the ICRC

[133] B. Parker, above note 78.

[134] Indicative of how the use of biometrics may come with new forms of insecurity in other contexts too is, for example, the case of biometric data flows producing risks to Rohingya refugees. Looking beyond Afghanistan and Somalia, flows of biometric data produced by humanitarian actors have been documented in other contexts and shown to have negative implications. As argued in a Human Rights Watch report, the UNHCR has put Rohingya refugees "at risk of forced return" by sharing biometric data with authorities in Myanmar, the State from which these refugees had fled: Human Rights Watch, "UN Refugee Agency Data Sharing Puts Rohingya at Risk of Forced Return", 2021, available at https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent. Though the contexts differ, the case still illustrates how the UNHCR data-sharing agreements (here with Bangladesh, who subsequently signed a data-sharing agreement with Myanmar) entails risks to individuals who the UNHCR is mandated to protect. On how "biometric data UNHCR collected from Rohingya refugees was shared with the country they fled, Myanmar", see also Zara Rahman, "The UN's Refugee Data Shame", *The New Humanitarian*, 21 June 2021, available at: https://www.thenewhumanitarian.org/opinion/2021/6/21/rohingya-data-protection-and-UN-betrayal; and Kate Hodal, "UN put Rohingya 'at Risk' by Sharing Data Without Consent, Says Rights Group", *The Guardian*, 15 June 2021, available at: https://www.theguardian.com/global-development/2021/jun/15/un-put-rohingya-at-risk-by-sharing-data-without-consent-says-rights-group.

[135] Oxfam, "Oxfam Biometric & Foundational Identity Policy", 2021, available at: https://oxfam.app.box.com/v/OxfamBiometricPolicy.

to limit the use of biometric data to specific use cases,"[136] which, for example, contrasts with how, for the UNHCR, biometric registration is considered a "routine feature"[137] and strategic decision.[138] Along similar lines, is the recent intensification of debates about data deletion and the right to be forgotten,[139] with "growing calls from a number of organisations for a greater focus on the risks of new digital technologies."[140] However, not only is biometric data still collected and stored by numerous actors, but deletion may not always be an easy option: "For those in official databases, particularly the APPS [the U.S. funded 'Afghan Personnel and Pay System' database], user deletion is not an option."[141] Another interviewee similarly noted: "By design, UNHCR's registration systems do not allow the deletion of IC files. An IC can be 'deactivated' but not be deleted."[142]

Biometric intervention infrastructures: ambiguity rather than accuracy

Looking ahead, another issue in relation to expanding biometric intervention infrastructures is the question of how this still somewhat elusive infrastructure affects several important distinctions and boundaries like wartime/peacetime, friend/enemy and sovereign/intervention.[143] Whilst in some cases biometric data flows may lead to increased accuracy, it is crucial, however, to emphasize how flows of biometric data (via formal agreements or involuntary paths) may in other cases produce increased ambiguity. Ambiguity may come about at two levels. First, pertaining to processes through which individuals are categorized by different authorities as legitimate refugee, legitimate counterterrorism target and/or subject of experimentation, the analysis showed the importance of foregrounding questions about how and by whom biometric data is gathered, shared and processed to establish such categories. Attending to data flows encourages analysis of how ostensible biometric accuracy does not always translate into unambiguity in data flows, with biometric data sometimes obtained via shadowy data-sharing practices. Put differently, biometric data-sharing agreements or cases of hacking represent different infrastructural

[136] ICRC, above note 104.

[137] See, for example, UNHCR, "Planning and Preparing Registration and Identity Management Systems: 3.6. Registration Tools", available at: https://www.unhcr.org/registration-guidance/chapter3/registration-tools/.

[138] Katja Lindskov Jacobsen, "On Humanitarian Refugee Biometrics and New Forms of Intervention", *Journal of Intervention and Statebuilding*, Vol. 11, No. 4, 2017.

[139] I. Loy, above note 65. It has also been argued that biometric data should be "deleted once it has served its purpose"; see Kerrie Holloway, Reem Al Masri and Afnan Abu Yahia, "Digital Identity, Biometrics and Inclusion in Humanitarian Responses to Refugee Crises", Humanitarian Policy Group (HPG) Working Paper, ODI, London, October 2021, pp. 34–5, available at: https://cdn.odi.org/media/documents/Digital_IP_Biometrics_case_study_web.pdf.

[140] E. Schoemaker, above note 117.

[141] This point was also made by an anonymous interviewee: Anonymous interview, September 2021.

[142] Anonymous interview, November 2021.

[143] Arguably, another commonplace distinction that biometric system may also challenge is that of individual/relationships, given that many new biometric systems on the market enable identification not only of individuals but of lineages.

interconnections of military and non-military biometrics, the effects of which are best understood not simply through an imaginary of accuracy, but rather as potentially engendering increased indeterminacy for biometrically registered individuals left unsure of how their biometric data is being processed, by whom and to what effects. By tentatively illuminating emerging ambiguities and insecurities at the level of biometric infrastructures, the article added to the existing literature on the fallacy of accuracy in contemporary counterterrorism.[144]

Second, exploring data-makings and data flows highlighted how an expanding biometric intervention infrastructure may breed another critical ambiguity, namely fluidity in the distinction between war and peace when it comes to the collection and use of biometric data. What happens to the distinction between armed conflict and peacetime when biometric data gathered during armed conflict is passed over to or retained by a State, including its intelligence services, and potentially used for peacetime operations? If biometric data gathered by US soldiers during military intervention in Afghanistan is retained indefinitely, i.e. also after warfighting has officially ended, what do such data flows and retention practice imply for the security of these individuals? Such practices of retaining biometrics beyond "war's end" expand the possible space of counterterrorism action into "peacetime" as illustrated in the following quote from a biometric expert: "we need to take a federated approach to our biometric databases, since they are a powerful weapon that can be used in peacetime, as well as on the battlefield."[145] Such expectations about the value of biometrics for counterterrorism purposes feed a practice of data retention which in turn generates another sense of ambiguity that highlights the limits to how biometric accuracy "translates" into more accurate and presumably more legitimate form of counterterrorism. Insofar as the above analysis offers additional nuances to existing debates about the tensions and fallacies of current counterterrorism, the argument also illustrates how looking at biometric infrastructures, with attention to both military and non-military actors, offers an entry point through which to illuminate broader tensions and contradictions.

Concluding reflections

As the above analysis demonstrates, we have seen how besides risks of new instances of unintended sharing of biometrics data (potentially with actors whose friend/enemy distinctions are diametrically opposed to those of institutions that beneficiaries and other subjects originally trusted their sensitive data with), it is necessary to expand our appreciation of how biometrics may generate insecurity. Moving forward it is of course crucial to look at actual data flows, but certainly also at the makings and flows of various immaterial elements, be they success

[144] Lucy Suchman, "Algorithmic Warfare and the Reinvention of Accuracy", *Critical Studies on Security*, Vol. 8, No. 2, 2020.

[145] S. Gold, above note 33.

stories or fear, both of which may in very different ways affect the safety of beneficiaries or other biometrically registered subjects. For example, where biometric registration remains mandatory with no changes to retention and sharing policies, there is a risk that potential beneficiaries may decide not to register with the WFP, UNHCR or other humanitarian agencies, out of fear of what could happen to their biometric data. Could it end up in the hands of actors who would use it in ways that would create additional insecurity for these already vulnerable individuals? Indeed, as shown in this article, this is a very real risk considering recent examples as well as the extent to which several intervention actors – military and otherwise – produce biometric databases vulnerable to exposure and unintended data flows. Moreover, with stories about unintended access circulating, what also gets produced is fear. And with stories about new real-world proof of biometric reliability or scalability, what also gets produced are success stories. While intangible, both success stories and fear affect the contours of the future of biometric data collection, though potentially in opposed directions. Success stories buttress a broader imaginary of "more biometrics, more safety," and of the centrality of biometrics in current and future counterterrorism, as "a powerful weapon in peacetime and on the battlefield."[146] Fear and anxiety, on the other hand, may more indirectly generate insecurity – be it for refugees who decide not to register with the WFP whereas they would be entitled to do so, or for biometrically registered Afghans who fear that their iris scans are on the databases that the Taliban claims to have access to.[147] We have seen in other contexts how biometric registration may "create security concerns that could prevent some refugees from registering with UNHCR. This has been the case with Syrian refugees in Lebanon."[148] More specifically, the use of biometrics may affect the mobility of refugee in ways that can in turn give rise to unintended negative implications for refugee safety. For example, for refugees who "due to security considerations [have] not entered Lebanon through an official border crossing,"[149] the use of biometrics may "increase an already prevalent fear that they may be arrested when crossing an internal checkpoint."[150]

A widening abyss between the imaginary of biometric security and the (silenced) emergence of insecurity is critical. Also importantly regarding silenced insecurity, it must of course be said that besides the focus in this article on certain types of consequences there is a plethora of other largely untold stories about unintended consequences from biometrics encountered by people in various marginalized settings. For example, the UNHCR and WFP note in a joint

[146] *Ibid.*

[147] There have always been numerous refugees who decided not to register with aid agencies, also before the advent of biometrics. Thus, biometrics is one of many factors affecting whether refugees seek registration or not; there are indeed other factors which might encourage refugees not to register.

[148] Katja Lindskov Jacobsen, "UNHCR, Accountability and Refugee Biometrics", in Kristin Bergtora Sandvik and Katja Lindskov Jacobsen (eds), *UNHCR and the Struggle for Accountability*, Routledge, London and New York, 2016.

[149] NRC, "The Consequences of Limited Legal Status for Syrian Refugees in Lebanon", NRC Lebanon Field Assessment, NRC Lebanon, March 2014, p. 6.

[150] K. L. Jacobsen, above note 148.

assessment of their "Kenya Refugee Operations" how "school-going children or child-headed families" were forced to "skive school in order to comply with the requirements of the biometric food distribution system."[151] Examples of how humanitarian uses of biometrics may unintentionally generate negative implications for refugees have also been noted in several other contexts. For urban Syrian refugees in Lebanon, "who 'due to *security considerations* [have] not entered Lebanon through an official border crossing',[152] the use of biometric identification may increase an already prevalent fear that they may be arrested when crossing an internal checkpoint."[153] Indeed, the likelihood that biometric data collection and sharing may unintentionally have negative implications on refugee mobility and safety is a concern that has been voiced for several years. An unpublished study highlighted several risks, including that "data falling into the wrong hands could result in persecution, discrimination or even imminent threat to liberty and life" and that data "acquired by host governments" may be used "to assist efforts to imprison or persecute populations."[154] Many more examples and voices deserve attention if we are to understand the myriad of ways in which biometric data-makings and flows may generate unintended effects, including the risk that incorrect data is replicated across different systems, may preclude individuals from applying for resettlement or from registering a child's birth.[155] Assembling existing accounts alongside adding additional examples of the impact of biometric data-making and flows on people whose data is being processed and shared would in important ways contribute to giving voice to individuals whose encounters may indeed make even more apparent why we need to pay attention to the risk of unintended consequences of expanding biometric intervention infrastructures.

Drawing on Tilley's notion of "living laboratory," that analysis also unpacked how an important dimension of the imaginary of biometrics as central to counterterrorism is a quest for relentless real-world testing of new biometric systems, including new modes of collecting and connecting biometrics. Like in the case of the WFP, framing the limits of biometrics for infants as a call for more research, so too are other limitations framed as an invitation to add more: new trials, new capture devices, more biometric data. In this sense, the analysis alluded to another expansion, an inbuilt logic of continuity where failures are "offset" by adding more of the same. Failing to prove the reliability of biometrics

[151] WFP/UNHCR, "Joint Assessment Mission – Kenya Refugee Operation: Dadaab (23–27 June 2014) and Kakuma (30 June–1 July 2014) Refugee Camps", 2014, p. 18, available at: https://www.unhcr.org/54d3762d3.pdf. Many other examples, including more recent ones, deserve attention. See, for example, Belkis Willie, "A Cautionary Tale: When Humanitarian Data Collection/Transfer Harms Beneficiaries", NetHope 20th Anniversary Summit, 15–19 November 2021, available at: nethopeglobalsummit.org.

[152] NRC, above note 149.

[153] K. L. Jacobsen, above note 148.

[154] Simon Davies, "How a United Nations Agency Buried a Security Report that Warned of Potential Genocide", *The Privacy Surgeon*, 2012, available at: http://www.privacysurgeon.org/blog/incision/ how-a-united-nations-agency-buried-a-security-report-that-warned-of-potentialgenocide/.

[155] I am very grateful to the two anonymous reviewers who stressed the importance of accentuating the impact on people whose biometric data is being processed and shared, and of the need for more attention to the perspective of those affected, particularly since their voices are often ignored.

for children under 5 years was formulated as an opportunity for more real-world trialing of infant biometrics. Failing to make biometric databases "interoperable" in Iraq and elsewhere has not genuinely challenged the imaginary of ubiquitous biometrics and accurate identification of enemies globally, but instead propelled new interoperability trials. With reference to "limited interoperability and sharing of data between humanitarian agencies" working in Somalia, a recent report points to efforts to explore "ways to establish interoperable databases."[156] Again, this is not exclusive to counterterrorism biometrics but a tendency observed in relation to other counterterrorism engagements as well. Exploring French counterterrorism in the Sahel, Guichaoua argues: "This is a maximalist logic: failure does not lead to the withdrawal of an initiative but to the design of a new one."[157]

Attending to such logics, another interconnection becomes visible: for humanitarian and for counterterrorism purposes the use of biometrics involves "self-sustaining dynamics" whereby limitations and failures do not lead to questioning of devices or imaginaries but to calls for additional real-world trialing. For example, when the IOM replaced one-digit fingerprint readers with ten-digit readers, at eight Somali border crossings,[158] this was simply presented as a technical "upgrade" of existing systems, invisiblizing the politics of implementing new systems capable of checking "data records against national and international alert lists for suspected criminals." Insofar as "failures" become productive, the implication is that biometric trials never fail in the sense of highlighting lack of evidence of biometrics as a counterterrorism panacea. They are only failures in a different sense: as productive of a quest for new trials, more biometric data and further interoperability.[159] To what extent may this logic impel infrastructural expansions that the analysis of this article presents a critical reading of? Attending to questions about data-makings, flows and infrastructural interconnections of counterterrorism biometrics and biometrics used by non-military actors, this article highlighted critical ambiguities and opaque distinction makings that challenge imaginaries of biometric accuracy and the often-unabated assumption that biometric data gathered by various actors is central to the design of counterterrorism operations.

Finally, can we fully appreciate the continuous expansion of biometric databases without asking questions about the role of donors and their influence on humanitarian actors' practices of collecting and sharing biometric data? As the above-mentioned report from the UN Special Rapporteur notes: "donors have

[156] B. Owino, above note 14.

[157] Yvan Guichaoua, "The Bitter Harvest of French Interventionism in the Sahel", *International Affairs*, Vol. 96, No. 4, 2020.

[158] Chris Burt, "IOM Installing 10-Digit Fingerprint Readers at Somalian Ports of Entry", *BiometricUpdate.com*, 7 June 2018, available at: https://www.biometricupdate.com/201806/iom-installing-10-digit-fingerprint-readers-at-somalian-ports-of-entry.

[159] Thanks to Marijn Hoijtink for hosting a workshop that facilitated these discussions. Thanks to Debbie Lisle, for highlighting this during fruitful workshop discussions.

repeatedly pushed for the integration of biometrics in aid delivery."[160] To what extent may biometric data-making confront humanitarian actors as a condition for receiving funding, defined by donors? Moving forward, we need to add such consideration to questions about the conditions under which biometric data is produced in order to appreciate how humanitarian actors confront difficult choices insofar as "no to biometrics" might mean no funding and thus, no assistance to the people whose exposure to risks from biometrics is thus entangled with their vulnerabilities without assistance in the first place. Yet, such consideration should certainly not downplay the critical importance of revisiting humanitarian and other actors' biometric data-making and data-sharing practices.

[160] K. Huszti-Orbán and F. Ní Aoláin, above note 91, p. 7; The Engine Room and Oxfam, "Biometrics in the Humanitarian Sector", March 2018, available at: https://www.theengineroom.org/wp-content/uploads/2018/03/Engine-Room-Oxfam-Biometrics-Review.pdf; Kristin Bergtora Sandvik, Katja Lindskov Jacobsen and Sean Martin McDonald, "Do No Harm: A Taxonomy of the Challenges of Humanitarian Experimentation", *International Review of the Red Cross*, Vol. 99, No. 904, 2017.