Assessing Data Protection Perspectives Among the Residents of Rumphi and Karonga in Northern Malawi Regarding the Use of Unmanned Aerial Vehicles (Drones) for Humanitarian Intervention

Rogers Alunge(✉)

Faculty of Geo-Information Sciences and Earth Observation (ITC), University of Twente, Enschede, The Netherlands
alungerogers@yahoo.com

Abstract. Drones are used by humanitarian actors to collect data which could be classified as personally identifiable information (PII) and demographically identifiable information (DII). Though said to optimise intervention, they raise significant data protection challenges. An example is transparency: how effectively are community residents informed about the data drones collect of them and their community? How may this awareness affect their desire to consent, engage related group/community data protection rights, or to allow the data collector circumvent these rights to guarantee their faster access to aid.

This paper is based on two case studies: the Northern Malawi districts of Rhumpi and Karonga, earmarked as flood-risk areas and whose residents had witnessed humanitarian drone flights. The research uses qualitative analysis of focus group discussions with selected inhabitants on a series of data protection questions relating to drones. The results show that participants were mostly unaware of the high-resolution images drones take of them and their communities; their consent would hardly be valid because of their vulnerable situation, and they preferred extensive sharing of their data to attract external aid rather than engage any DII rights. This prompted the conclusion that guaranteeing responsible drone data collection and processing in humanitarian settings would rest entirely on the humanitarian organisation, with comparably little or no engagement by the local residents.

Keywords: Humanitarian intervention · data protection · transparency · drones · personally identifiable information · demographically identifiable information · Malawi

A. Seeam et al. (Eds.): InterSol 2023, LNICST 541, pp. 313–336, 2024.
https://doi.org/10.1007/978-3-031-51849-2_21

1 Introduction: Unmanned Aerial Vehicles (UAVs or Drones) in Humanitarian Action

Unmanned Aerial Vehicles (UAVs, otherwise called drones) are aircrafts without a human on board [1] which are controlled remotely, and can be equipped with different sensors that could capture and record visual and audio data for monitoring and mapping operations [2]. Originally, drones were primarily used by military organisations for surveillance and reconnaissance purposes in the 1950s [3, 4]. In recent decades however, they have been increasingly used by civilian sectors for a vast array of activities ranging from logistics, supply chain management [5, 6], agricultural surveys and monitoring [7] aerial imaging, mapping, town planning, or aerial cargo services [8]. Irrespective of their applications, the general motivation behind the use of drones is their ability to increase the speed and flexibility of supply chain, data collection and communication processes, while enhancing precision and cost efficiency. As noted by Jumbert & Sandvik, government actors (first responders like firefighters, search-and-rescue crews, and police), civil society actors (environmentalists, conservationists, cultural-heritage advocates, human-rights activists), the press (especially the so-called "citizen drone" journalists and enthusiasts) as well as the agriculture, mining and maritime industries are all exploring opportunities and possibilities offered by drone technology to attain their objectives, enhance work effectiveness and increase productivity [3]. Drones could be equipped with sophisticated devices to observe and track ground movements with high resolution images, move at alternating altitudes, relay information at very high speed and transport supplies, offering easier and faster data collection processes and enhancing decision-making.

Drones are also increasingly used by humanitarian actors (hence the term "humanitarian drones" [9]) for locating survivors and assessing infrastructure damages following a disaster, and monitoring population movements. They are also useful in conducting needs assessments to determine where, and how many people are in need and what their needs are, and building better short-term strategies for handling humanitarian logistics and distributing relief [10]. Due to their possible remote sensing abilities and rapid spatial information collection, drones have also been widely used in emergency surveying [11], and in case of disasters, they can go deep into specific locations, which reduces danger and security-related issues for accompanying human rescue teams. Significantly, they are equally used for disaster prevention, as they can collect aerial data of an area which can be processed to determine or measure the impact of some predicted disaster, an example being the objectives of the UNICEF Malawi drone corridor[1].

Sophisticated equipment like high-resolution cameras can be attached to a drone to generate clear, high-resolution aerial photographs [12] of a community through which

[1] In June 2017, the Government of Malawi and UNICEF launched a 40km-radius air corridor at the Kasungu Aerodrome in Central Malawi to as a base to test drones for various humanitarian purposes including flood modelling. Aerial images would be captured and run through AI image recognition and flood modelling software to predict flood impact and identify areas which will be most affected, aiming to better inform emergency preparedness through early warning. Retrieved from https://www.arm.com/blogs/blueprint/arm-unicef-malawi. Accessed 26/03/2023.

individuals, groups of persons or a community can be identified by the entity which deployed the drone. For this reason among others, notwithstanding their lauded contributions to humanitarian intervention, an important amount of literature attests to the important data protection/privacy and ethical challenges involved with the deployment of drones in humanitarian contexts (so-called humanitarian drones [9]). However, there has not been so much research yet on data protection from the perspective of the data subject i.e. examining the perceptions which people in vulnerable situations may have regarding their privacy and data protection in relation to the use of drones in their towns or community. As contribution towards bridging this gap, this paper examines data protection and/or privacy-related perspectives which persons in vulnerable situations may have regarding humanitarian drones. It investigates their awareness of the data about them collected by means of drone technology (principle of transparency of collection and/or processing), how their awareness may reflect on their readiness or willingness to consent to the data collection, and also discusses the idea of a community rather than individualistic approach to data protection.

The chosen case study areas are the Northern Malawi districts of Rumphi and Karonga, both internationally earmarked as flood-risk areas and tagged by UNICEF Malawi for an impact-based flood-modelling survey using drones. I organised focus group discussions (FGDs) with the locals who witnessed the flying drones, to find out the extent to which they are aware of what data about them and/or their community can or are actually being collected by the drones, and how this awareness could impact their consent to such data collection or processing. Also, I sought to establish whether they may wish to exercise group/community data rights over the processing of aerial, high-resolution images collected on their community, and finally how willing they are to allow the drone-processing organisation to waive aside its data protection responsibilities towards them and their data if that would guarantee faster accessibility to external aid. In this light, the following section briefly presents the subject matter of data protection: personally identifiable information (PII) and demographically identifiable information (DII), and briefly discusses the data protection principle of transparency and its importance in (humanitarian) data collection processes. Section 3 then gives a general presentation of the research project, Sect. 4 presents our methodology and data collection tools i.e. the FGDs, and Sect. 5 discusses the participants' responses gathered from the FGDs. Finally, Sect. 6 presents a general conclusion to the paper.

2 PII, DII and Processing Transparency Regarding Humanitarian Drones

As noted by Weitzberg et al., humanitarian actors increasingly rely on data and technology for humanitarian response [13], with humanitarian drones actively involved in the collection and processing of vast amounts of data. A lot of this data is personally identifiable information (PII) and demographically identifiable information (PII) – a distinction of these follows below. As Kuner et al. importantly observe here, what is of interest in the case of drones as regards data collection and processing is not the use of the drones *per se,* but rather the different technologies they are or could be equipped with, such as high-resolution cameras and microphones, thermal imaging equipment,

sensors or devices capable of intercepting wireless communications [14]. It follows that the PII or DII a drone collects or can collect will depend on the data collection devices fitted to it.

2.1 Personally Identifiable Information (PII)

PII is any data that directly or indirectly identifies, or can be used to identify an individual. It includes, but is not limited to the person's name, address, identity number, gender, age or date of birth, financial account numbers, image or location [15] The collection of PII, also known as personal data [16], is crucial for the provision of humanitarian assistance where there is need to determine and identify persons in need e.g. to give out food or cash coupons, or administer medical aid. As pointed out by the World Food Programme (WFP), loss, theft or misuse of personal data may cause harm to the people needing assistance[2]. An individual whose personal data is unduly disclosed may be subjected to very serious abusive behaviours, particularly in armed conflict settings and other highly volatile socio-political situations such as dictatorships or ethnically motivated conflicts. As drones are (always) equipped with cameras, sensors and even with devices capable of intercepting communications, they are very likely to capture PII or communications about individuals. For instance, a political opposition leader fleeing his country and hosted in a refugee camp may be identified from aerial, high-resolution images of the camp and pursued by government officials of his/her country if they get access to those images. Also, when the drone is equipped with two or more multidimensional cameras, it will not only collect data about the target, but also about other persons within the field of view of the drone (like images of people within the confines of their compound). These and related situations raise protection concerns which demand careful and responsible handling of PII by humanitarian drone operators.

2.2 Demographically Identifiable Information (DII)

DII, also known as "group data", has been defined as either individual and/or aggregated data points that allow inferences to be drawn that enable the classification, identification, and/or tracking of both named and/or unnamed individuals, groups of individuals, and/or multiple groups of individuals according to ethnicity, economic class, religion, gender, age, health condition, location, occupation. It can include PII, geographic and geospatial data, environmental data, survey data, and/or any other data set that can – either in isolation or in combination – enable the classification, identification, and/or tracking of a specific demographic categorization constructed by those collecting, aggregating, and/or cross-corroborating the data [17]. In other words, these are data which would not single out an individual from a group, but could rather single out or differentiate a group of persons from within a bigger group of people, or differentiate a community from other (similar) communities. DII would also include (especially in rural, less developed sectors) data like high resolution images of a community depicting data like housing structures, monuments, shrines, agricultural and agropastoral patterns, religious practices, dress codes of the people which (when combined with other available datasets) can

[2] Ibid.

enable the identification or recognition of that community from other communities. And like PII, DII could be used to target and harm an identified group of people. A case in point is the Harvard's Signal Program on Human Security and Technology, which operated a project analysing satellite and other spatial data to identify areas most affected during the 2011 conflict in Sudan. The researchers later discovered that their analyses of these data were being hacked and used by hostile actors on the ground to better target their enemies [18].

However, while PII has conveniently been protected under contemporary data protection regulation, there currently is no legal regime *rationae materiae* protecting DII. Current privacy and data protection regulatory frameworks are individualistic, triggered only when the information of a distinct, identified or identifiable individual is processed [19], and as van der Sloot [20] rightfully argues, they do not provide a satisfactory response to risks affecting individuals which arise from processed data relating to groups of individuals[3]. UNICEF for example expressly states in its Policy on Data Protection that the Policy does **not** apply to "…data that can identify a group, demographic or community, but not an individual."[4] Even the World Food Programme defined "personal data" without including data which identifies or which could identify a group of people[5]. Other internationally influential data protection regimes like the 2018 EU General Data Protection Regulation or 2014 African Convention on Cybersecurity and Data Protection also strictly apply to data relating to individuals with no reference to group or community data.

It should be mentioned however, that though contemporary data protection regimes are individualistic, and their data collection and processing principles were conceived to apply (only) to PII, it appears reasonable that DII can be largely covered by these principles. It would obviously be tricky to determine how to enforce rights like the right of access, rectification, or deletion of DII especially as members of the same group or community may feel differently about or could be differently affected by the same dataset. But principles like those requiring a data collector to have a specific, pre-set and limited purpose for processing (purpose limitation), determined period to store the collected data (storage limitation), to collect just what data is needed (data minimisation), taking appropriate measures to secure data collected (security of processing), or having a lawful ground for collecting that data, can all seemingly and conveniently be applied to DII. This observation was echoed by Kuner et al. [15] in their discussion about the use of drones in humanitarian interventions, where they examined the idea of "consent

[3] This is even more so considering that the concept of a "group", especially in the age of Big Data analytics, is a vastly dynamic concept with practically unlimited variables, and groups are digitally created by cross-referencing large amounts of data which results in these groups not being structured. And one individual could be the subject of many groups e.g. one individual can belong to the categories "men over 30 who own a car in Kenya" "medical doctors who are married in Kenya", "Manchester United FC football fans below 40 in Africa". See Kammourieh, Lanah, Thomas Baar, Jos Berens, Emmanuel Letouzé, Julia Manske, John Palmer, David Sangokoya, and Patrick Vinck. "Group privacy in the age of big data." *Group privacy: New challenges of data technologies* (2017): 37–66.

[4] Paragraph 8, UNICEF POLICY ON PERSONAL DATA PROTECTION, Document Number: POLICY/DFAM/2020/001. Effective Date: 15 July 2020.

[5] World Food Programme Guide to Personal Data Protection and Privacy (supra).

of the community" or the "consent of authorities" as a plausible alternative to individual consent offered by contemporary data protection regimes. This could involve, for example, obtaining consent only from representatives of a group of vulnerable individuals and not the individuals themselves. The following discussions would therefore examine the FGD results in Annex I below in line with established data protection principles of processing, the implementation of which remains the responsibility of the processing organisation.

2.3 The Data Protection Principle of Transparency

Data protection is here understood as those set of rules and safeguards to be observed when processing (personal) data in order to protect the fundamental rights and freedoms of individuals from any eventual violation [21]. Drones and their applications entail the collection, processing, recording, organisation and storing, of PII. This means their deployment over civilian settlements triggers data protection (and privacy) concerns [22]. Drones have especially offered increased capacity for domestic surveillance through high-definition cameras, real-time video streams, their ability of massive geographical sweep, heat and motion sensors, automated text and facial recognition technologies.[6] Moreover, their small size and ability to fly very high makes them likely to operate undetected, which could raise some issues as regards (the fundamental data protection principle of) transparency.

The principle of transparency in (personal) data protection requires that at least a minimum amount of information concerning the processing be provided to the individual whose data is being collected [14]. Typically, the specifics of the information to give the individual will depend on the legal basis and reason for which the data is being collected, but should generally include the nature of the data, the purposes for which it is collected, how long it shall be stored, whether it shall be transferred to third parties, and any rights which they may have in relation to this processing (e.g. access to their PII, correction or deletion; right to object to or to restrict processing) [23]. This information should be provided before the data is collected, is generally received orally or in writing and communicated directly to the individuals, should be easy to understand, expressed in clear and plain language. However, where this is not possible, the organisation should consider providing information by other means like radio communications, online adverts, flyers, posters displayed in a place and form that can easily be accessed (public spaces, markets, places of worship and/or the organizations' offices), radio communication, or discussion with representatives of the community [14]. Kuner et al. observe that with regard to drones, it would generally, for practical reasons, be difficult to inform everyone in the targeted area individually, which is why the ideal practice will be to use media campaigns targeting the local inhabitants, and actively involving the leaders of the target community, all before the drones are deployed (especially in non-emergency situations, as was the case with the UNICEF Malawi flood modelling activity in Northern Malawi). They also suggest that while flying the drones, the organisation could affix their marks

[6] Petition to the Federal Aviation Administration: Drones and Privacy (Washington, D.C.: Electronic Privacy Information Center, 2012), https://epic.org/wp-content/uploads/privacy/drones/FAA-553e-Petition-03-08-12.pdf Accessed 12/3/2023.

or signs on them [or to the extent possible, attach a flag bearing their logo on them] to fulfil transparency and information obligations. [14].

2.4 Importance of Transparency in Community Data Collection

Absence of sufficient communication and information circulation about a DII collection and processing activity in a community could lead to the data collector missing out on important data responsibility measures; a case in point being the collection of data which might be regarded as sensitive within a specific community. Concepts of what information should be considered sensitive or private may vary between cultures, age groups, interest groups and other demographics [24]. For example, traditional shrines or traditional cults are usually sacred to a community and may be accessed only by designated members of the community, which implies data relating to them could be considered sensitive by the community residents. They may not want details of what happens within these sacred settings to be known out of the community, hence they may react negatively to the generation and collection of aerial, high-resolution images depicting these settings.

This in turn impacts on other data protection perceptions which data subjects may have about the data collection, as awareness of exactly what data about them and their community is collected, as well as with whom it can be shared, will certainly be significant in guiding their decision whether to grant permission to the data collector to proceed. It therefore follows that if local residents are made aware in considerable detail of the high-resolution images which drones can take of their community, objects of their community which can come under the drone radar, as well as who will or could have access to these images, this might trigger their (data protection) sensitivities regarding this collection. Gevaert for example, during her research on the use of drones for town planning purposes in Rwanda and Tanzania, established that many residents expressed privacy-related worries regarding the capacity of the drones to take very high resolution and detailed images of their compounds and living environment [25]. Similarly, besides inquiring into their levels of drone awareness, this paper also seeks to find out whether comparable data protection worries will be voiced by the residents of Rumphi and Karonga when they are made aware of the high-resolution images of them and their community being (or capable of being) taken and collected by humanitarian drones.

3 Methodology

3.1 Fieldwork (in Collaboration with UNICEF and DODMA Malawi)

The research was qualitative: focus group discussions (FGDs) [26] with residents of the chosen case study districts who have witnessed drone activity in their community. To achieve this, I worked closely with UNICEF Malawi which had planned an impact-based flood modelling exercise using drones in Northern Malawi in November 2022, which included Rumphi and Karonga. I also enlisted the help of field officers of the Department of Disaster Management (DODMA) of Malawi in Rumphi and Karonga, who helped find volunteer participants for the FGDs (see Sect. 3.2 below). According to

our plans, UNICEF Malawi would go to these areas and carry out their flood-modelling exercise, and I come a day later to meet volunteer residents (who witnessed the drones flying overhead) and have group discussions with them on their data protection/privacy perceptions with regard to the drones they saw. The plan went well for Rumphi, but by the time I got to Karonga, the flood modelling activity had not started yet. So in order to attain our survey target, I enlisted the support of a private drone pilot, who flew a drone over the settlement, took high-resolution pictures of the people and their community which I used as the display image during the discussions. Then with the aid of the present DODMA officials, I selected 21 volunteer participants for the FGD from the (curious) onlookers, following the criteria elaborated in Sect. 3.2 below. I estimated that this would not jeopardize the results of the research as the most important factors for the discussions (i.e. residents of a disaster-risk community having witnessed drone activity) were met with this arrangement (Table 1).

Table 1. Summary of the organisation and planning of the FGDs

Casestudy district (villages visited)	Number of participants	Number of FGD sessions	Notable issues
Rumphi (Mlowe, Mzoto Chisokwo, Rumphi Boma)	21 (12 men, 9 women)	3 (7 participants per session)	No specific issues: UNICEF Malawi agents had been on site and flown their drones; participants had witnessed drone activity by the time I arrived
Karonga (Karonga Boma)	21 (11 men, 10 women)	3 (7 participants per session)	The flood-modelling had not begun yet, so a private pilot was hired to fly a drone over the community, and selected participants from the onlookers with the aid of DODMA officials

3.2 The Participants

As mentioned above, DODMA Malawi assisted in selecting participants for the FGDs. They helped select a total of 42 adults who had witnessed the drones flying overhead, 21 from each casestudy district and ensuring an even representation of men and women. I had a total of 6 discussion sessions (3 per casestudy district), with 7 participants per session. And to keep the discussions open and minimise power imbalances within the discussion groups, DODMA ensured that participants in each session were of about the same social class; traditional authorities were excluded from the discussions (see Table 3).

3.3 The FGDs

The discussions were triggered by a series of prepared questions aimed at investigating the participants' knowledge about the data processing abilities of drone technology. This was meant to induce discussions with the participants on any privacy or data protection concerns they may have regarding drone activity in their communities. I was assisted by a translator charged with translating the questions to Chitumbuka (the language commonly spoken in Northern Malawi) and posing them to the participants. We both then listened to their replies which the translator rendered back to me in English. He equally acted as moderator of the discussions. At the start of each FGD session, a prepared consent statement translated to Chitumbuka was read and explained to the participants by the translator. They were required to raise their hand if they still consented to contribute to the study, hence attesting to their valid and unequivocal consent to participate in the discussion. The entire discussions were recorded using an advanced portable audio recorder system. Below are the questions guiding the FGDs (Table 2).

Table 2. The FGD questions

Residents' first impressions on drone technology:	- What were your (first) impressions when you saw the drones fly? - Have you seen other drone flights? - Have you seen a picture taken by a drone before? - Do you think these drones (can) take clear, detailed pictures of your village, farms, houses, children?
Residents' individual opinions about drone image processing	- [Showing them an aerial drone image of a community] What do you see in this image (can they identify, roads, farms, private compounds)? - What are your impressions/opinions of these images? - What do you personally feel about these pictures, seeing that they can show details of your houses, farms and entire community? - Is there anything in this picture you may not like other people in the village or elsewhere to see (e.g. roofless toilets, waste disposal?) - Generally, with who may you not want such images of your property or community to be shared (maybe state land/town planning officials)?

(*continued*)

Table 2. (*continued*)

Residents' awareness of processing	- Were you aware the UAV flights you witnessed would take place? If yes, how were you informed? By who? - Were you aware or informed that the flying UAVs will be taking clear, detailed images of your community? - Do you know the person or organisation flying the UAV? Did they come and present themselves to you? - Did anyone tell you whether and why it is necessary to take these UAV pictures of you and your community?
Residents' opinions about informed consent for drone data processing	- Do you think you should be informed first before the flying of a UAV over your community to take such pictures? - Would you like to be personally able to grant or refuse permission for these images to be taken and/or shared with others? - In your opinion, should an authority be empowered to give permission on behalf of the entire community for these images to be taken? If yes, who do you think should have that authority? And why?
Residents' awareness of their data protection rights with regard to drone data processes	- Do you feel you may have any individual rights on these images? - Do you think as a community, you all as a group can have rights (besides monetary rights) on these images? - Are you aware of any specific information-related rights (besides monetary rights) you may have on these images? - Has anyone mentioned anything to you about any rights you may have regarding these images of you or your community?

(*continued*)

Table 2. (*continued*)

Residents' opinions of the benefits of UAV data processing	- In what situations do you think UAVs (can) really help or are necessary (maybe medical and relocation assistance in case of floods)? - Would you mind that these detailed UAV images of your property and community is shared with government and other parties, so they help you better during flood crisis, without caring much about your rights around these images? - Do you think humanitarian organisations or government could still help you effectively without the need for these UAV images and activity? - After the above discussions, what is your general opinion about UAV activity? Do you think it a positive or negative development for your community?

3.4 Envisaged Ethical Risks and Corresponding Mitigation Strategies.

Several potential ethical risks were identified which could be encountered during the organisation and progress of the discussions and adopted corresponding mitigation strategies as illustrated in Table 3 below.

Table 3. Potential ethical risks and mitigation strategies

Envisaged potential ethical risks	Mitigation strategies
Getting informed consent from the participants	Consent statement was translated from to Chitumbuka, read out and detailly explained to the participants by our translator at the start of each session
Limited participation	**Rumphi**: DODMA officials helped select one participant per household in each village visited **Karonga**: This was difficult to ensure as I had to select participants from among curious onlookers of our drone launch on the spot
Perception of power imbalance between the researcher and participants	I had a simple, layman appearance, and bore no logo or sign suggesting I am a government official or from any position of authority

(*continued*)

Table 3. (*continued*)

Envisaged potential ethical risks	Mitigation strategies
Intimidation by influential participants	I expressly excluded chiefs and traditional rulers from participating Also, selected participants were visibly of about the same social status [27]
Risk of political/religious opinions expressed during the discussion:	Interpreter was instructed and did well to moderate the discussion and guide the participants against emitting opinions with any political undertones
Risk of (physical and emotional) harm/security issues:	Discussions were moderated to prevent participants' disclosure of any sensitive information about their personal lives or those of other members of the community
Anonymity, confidentiality, and information security	FGD records were immediately transferred using VPN connection to and stored in the password-protected virtual drive of the University of Twente, with Bitlocker encryption installed. The records were then transcribed into text for in-depth analysis, and are currently stored in accordance with the University of Twente research data policies

3.5 Methodology Employed

This research relied on the relatively new Micro-Interlocutor Analysis methodology, proposed by Onwuegbuzie et al. [28]. This method was preferred principally for two main reasons. First because its collection phase is designed to have the opinion of every participant recorded, which is important especially in situations where a participant is silent, introvert or shy. It aims to include all voices, even those less heard during the group discussions. Secondly, the method proves efficient to record the main stance and positions of participants without absolutely needing to transcribe or understand the micro details of their declarations. This is crucial for our research due to the language barrier: I was interacting with the participants through a translator (doing simultaneous and summary oral renditions between Chitumbuka and English). And considering the differences in vocabulary as well as cultural differences in languages (especially regarding technology vocabulary), it would have been unfeasible to have granular details of the conversation orally translated in real time and recorded in English. In this case, it was essential to obtain just the position or opinion of each participant regarding specific questions discussed.

4 Findings Retrieved from the FGDs

After six discussion sessions lasting between 1.5–2 h each, the following findings were arrived at.[7]

4.1 Analysis: Discussion and Analysis of the FGD Results

Several interesting takes could be drawn from the FGDs. Before delving deeper in our analysis regarding data protection and data responsibility, it can be observed from the above table that drone technology is predominantly new to the locals of Rumphi and Karonga, with 88% of participants having never seen a drone fly before the FGDs took place. Notwithstanding, they were much more fascinated and curious than wary of the technology, with only 12% of participants admitting to a feeling of fear at the sight of the drones. There was also an overwhelmingly positive recognition of the advantages of the technology as a tool for community progress and development, with 98% of participants acknowledging drones were overall a positive development for their community.

A strong manifestation of community interests over individual interests could also be noted when discussing the issue of sensitive data with the participants. Illustratively, after being presented with some high-resolution UAV pictures of their community, 90% of the participants asserted that they did not find any unfavourable factors (not even open latrines) which should be considered sensitive enough to not be seen by third parties. These participants were also of the opinion that having images like open latrines or naked children playing shared to third parties would bring shame to the owner of the compound or parents respectively, which would act as a deterrent and coerce them to put roofs over the latrines or take better care of their children. Also, 93% estimated that the images could be shared with a wide range of third parties with no restrictions, even if the images showed details of their households behind a fence which would normally not be visible to their neighbours. They affirmed that to them, fences are built for security reasons (to prevent their livestock escaping or trespassers from getting in) rather than to protect their privacy; i.e. they do not mind the neighbours or a third party knowing details of their private residences behind the confines of their fences through drone aerial images.

Finally, a generally positive impression was noted among the participants regarding the deployment of UAVs for flood-related surveys in their communities, with 98% of them asserting that the abilities of drones to collect such pictures and share them in real time with government officials humanitarian actors makes them very necessary and indispensable for their progressive development. There also were no significant ethical worries or objections to the capacities of UAV technology, with only 4% of participants raising concerns about the possibility of drones capturing data like images of naked children or convicted prisoners (where the drone flies low enough to capture facial imagery), which they considered sensitive. Some specific observations are however worthy to be discussed in more detail, which is attempted below.

[7] For the full FGD results, please see ANNEX 1 below.

4.2 The Participants' Desire to Be Informed of UAV Data Processing

In line with the principle of transparency, the discussions revealed in the first place that the total 100% the participants expressed the wish to be informed of drone activities over their communities in advance, in line with the fundamental data protection principle of transparency as well as their right to information of processing. In Rumphi however, where UNICEF Malawi had already flown the drones by the time of our discussion, only 7 of the 21 participants attested to have been informed by traditional authorities who arrived to their homes to inform them about a flood modelling activity which will involve drones. The other 14 specified that while they were informed of a forthcoming flood-mapping exercise, they were not made aware that it will involve machines flying in the sky, taking overhead pictures of the community. One participant even mentioned that at the sight of the drone over his farm, he thought they were doing an aerial survey to sell of his land, which caused some panic.

Further, all 14 participants, after I showed them a sample of drone aerial shots, said they were not aware of the capacities of the drones to take clear, high-resolution pictures of their community, nor that they had the capacity to zoom in and possibly identify individuals. They were not also informed why such pictures are necessary, who they ae or might be shared with, how long it will be stored, which organisation was in charge of the project (the identity of the data controller), nor were they provided with any details on how to contact the organisation in the event of any complaints. Also, they were not made aware of any rights they may have towards any data collected by the drones. Moreover, during the data collection process, the drone pilots did not bear any organisation logos, and 5 of the participants attested to having approached them for identification, and were informed they were there on behalf of UNICEF Malawi.

From the above it can be concluded that UNICEF Malawi, as the data processing organisation, did try to comply with the transparency principle to inform the residents about the data collection process, using door-to-door communications in Rumphi. Notwithstanding, some essential information about the processing was not communicated to the residents. As pointed out by Kuner et al., the medium of information used to inform individuals about the collection or processing of their data, as well as the information considered essential to be communicated to crisis-affected individuals in a humanitarian context are determined on a case-by-case basis [31]. Considering that drones typically process data over a wide surface area, it will be unfeasible to determine exactly which individuals may come under their radar, and hence impracticable to inform people of the locality individually. UNICEF Malawi, by engaging with traditional rulers to inform households, can be said to have used a reasonable medium of communication. Also, with the direct target of this exercise being DII and not individuals, information like who the data will be shared with or how long it will be stored would probably not be essential for the residents in this context. However, knowing who oversees the project and being aware that clear, high-resolution pictures are being taken would probably be information which should have been duly communicated to the residents for transparency purposes.

4.3 The Participants' Desire to Consent to UAV Data Processing

Consent is an age-old concept in legal relations and a basic, well-known pre-condition for contractual engagements between individuals and legal entities. In relation to data protection, it basically is any freely given, specific and informed indication of a data subject's agreement to allow the processing of their PII[8]. While probably the most popular legal ground for processing PII, consent may, however, not always be sufficient especially within a humanitarian context.

As Kuner et al. [14] observe, given the vulnerability of most beneficiaries and the nature of humanitarian emergencies, humanitarian organisations will generally not be able to rely on consent for most of their data processing. As consent in data protection is generally required to be freely given,[9] with the data subject presented with a clear choice to give or withhold it, there could always be situations where making such a choice available to data subjects (and hence making their consent valid) is impracticable. Kuner et al. advance several typical humanitarian situations where an organisation will hardly be in a position to validly and sufficiently inform data subjects about their processing operations in order for their consent to be considered freely given. These included cases where processing operation is of a very large scale and will involve data of a large number of people; where the data subjects are particularly vulnerable (e.g. children, elderly or disabled persons) at the time of giving consent; where they have no real choice to refuse consent due to a situation of need and vulnerability, including a lack of alternative to the specific assistance being offered; or where new technologies are involved, characterized by complex data flows and multiple stakeholders, including data processors and sub-data processors in multiple jurisdictions [15]. It is also interesting to note that while requiring data subjects to be informed of processing to ensure they know what they are consenting to, contemporary data protection regimes do not require an indication from the data subject that they understand the information provided to them by the data controller [29]. This makes it difficult for a processing organisation to get reliable evidence that data subjects effectively understand and appreciate the risks and benefits of a processing operation sufficiently enough to consider their consent valid.

As observed in the FGD results table above, consenting to data collection seemed highly valued among the participants, with 88% wishing their permission could be sought before UAV images of their community are taken and processed. Further, 86% preferred that such consent should not be taken on their behalf (by a traditional authority) but they should be actively involved. However, similar situations as those cited above by Kuner et al. could be equally observed. First, as gathered from my collaboration with UNICEF Malawi, the drones were mapped to cover a very wide scale of territory occupied by thousands of residents among whom there inevitably were elderly people and children. Also, the people had not been proposed alternatives for flood modelling over their communities other than drones; and the drones are relatively new technologies involving data

[8] Art.2(h) Data Protection Directive: European Parliament and the Council of the European Union, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (23.11.1995).

[9] Article 2, Malawi Data Protection Bill 2021; Annex 1 Paragraph 5, UNICEF Policy on Personal Data Protection, July 2020; Recital 32 EU GDPR.

flows between two or more stakeholders (UNICEF engaged an undisclosed third-party processor to fly the drones and collect the data on their behalf in Rumphi). It could equally be observed that the participants had a low level of data literacy and had never been sensitized or triggered on the possibility of UAV-collected or generated PII or DII being misused in ways which could negatively affect them in the short or long run. Concepts like digital surveillance, online tracking and tracing, data breaches or algorithmic bias were completely foreign and unknown to them. Moreover, 76% of the participants said they will not mind the non-consideration of their rights by humanitarian organisations provided the collection and processing of their data grants them access to external aid; a point further confirming the influence of their vulnerability on any consent they might give for processing. These point to the conclusion that though most of the FGD participants voiced their desire to be able to provide their consent for UAV data processing within their communities, their vulnerable position makes such consent a less solid basis for the data processing organisation to rely on. Kuner et al. observe that in such a case, other legal bases might be more appropriate[10].

4.4 Group Data Protection and Community Rights Over UAV-Processed DII

As already discussed above, data protection is intrinsically individualistic, with current data protection frameworks limited in their scope of application to protecting identified or identifiable individuals (PII), and essentially excluding groups of people (DII). So in essence, DII or community data, as long as it cannot be linked to a specific, identified or identifiable individual, will not fall under the scope of current data protection law. As Van der Sloot observes, this status quo tends to inhibit the protective intention of data protection, because nowadays most people are not profiled as individuals but, instead, as a member of a specific (digital) group or community. Organisations no longer tend to gather data about a specific person, but rather an 'undefined number of people during an undefined period of time without a pre-established reason' [20]. These data are then processed on a group or aggregated level through the use of statistical correlations to make targeted decisions; a tendency which has often been criticised for yielding biased or discriminatory results on individuals who get algorithmically classified under such groups but may not actually have the traits for which they were made part of the group [30]. The result is thus that the 'individual' element is mostly lost in the process.

In this light, with data protection having originated from the need to protect the individual's right to privacy in the information age [31, 32], there have been discussions on alternative means of conceiving privacy as a concept which preserves the autonomy of the individual by equally preserving his/her relationship with their immediate surroundings. Proponents of a so-called 'relational autonomy' in particular, argue that people's identities, needs, interests – and indeed autonomy – are always also shaped by their

[10] Besides consent, Kuner et al. set out five other legal basis which organisations could rely on to process (personal) data of vulnerable or crisis-affected people: where processing is necessary for the vital interest of the person (e.g. to save the person's life); processing is necessary for important grounds of public interest; processing is necessary for the organisation's legitimate interest; for the performance of a contract to which the organisation is subject; or for compliance with a legal obligation.

relations to others [33]. And as Reviglio & Alunge observe, the view that the individual self is considered constrained by social factors (relational autonomy) and the realization that people are not always in control of information regarding them (especially in the big data era) necessitate the consideration of top-to-bottom norms which emphasize the dignity of humanity as a community or group over the dignity of individuals [34]. It follows therefore that data relating to a community or group through which specific individuals of that community or group may not be identified, but which processing could lead to decisions affecting them, should be covered as practicably as possible by data protection.

Relatedly, during the FGDs in Rumphi and Karonga, a sense of community action towards DII could be observed among the participants. When asked whether they feel they could have any individual claims or rights over the UAV images, 52% of the participants answered in the affirmative. On the other hand, 55% asserted that they believed the entire community as a unit could benefit from community rights on the images, which could probably be engaged and enforced via the traditional chiefs or community leaders if need be. This view was prompted by their observation that because the images depicted their way of life and habits to considerable accuracy, and could influence decisions by the government or UNICEF Malawi affecting them, it was only plausible that they could be given the opportunity to have a say on how the images are processed. Notwithstanding, it is important to point out that these were more of abstract opinions than strong positions which they wished to have implemented, as they were silent and manifested no interest towards discovering any data-related rights they may have as regards the aerial images of their communities. They evidently preferred to trust the government or humanitarian organisations to use the DII diligently and for the best interest of their community. In essence, they were much more interested in getting large scale visibility to attract external aid; and much less vocal about (DII) rights. This further points to the conclusion that the burden of guaranteeing data protection compliance to drone-processed DII relating to the Rumphi and Karonga communities would eventually rest almost entirely on the data controller organisations, with minimal participation expected from the residents.

5 Conclusion

The last few decades have witnessed a progressively important and significant employment of drone technology in humanitarian interventions, and this, it seems, would remain on an increase in the coming years. The advantages offered by drones to reach and collect data from hard-to-access or dangerous areas, cover vastly wide territorial scopes, enable direct communications and data transmissions between humanitarian actors, transport medical and other supplies at much faster rates and at much less costs make them an ideal and arguably indispensable tool for humanitarian action. Still, they are usually equipped with additional technology like remote sensors, high-resolution cameras or even communication interceptors which, though serving the purpose of precise and accurate data collection, pose significant privacy and data protection challenges. Drones have already been originally used and established by military organisations as highly proficient tools for intelligence spying and infiltration during warfare, a fact which is almost inevitably bound to raise concerns regarding surveillance, privacy and data protection whenever they are deployed over inhabited communities.

One of such data protection concerns is transparency of processing: with data protection requiring data subjects to be informed in considerable detail about the processing of their data, it follows that individuals whose data are being processed by drones should at least be made aware of the nature of the data being collected, how that data can be used and why it is collected. Further awareness of the exact nature of the data collected or which could be collected would further inform their decision to consent to this collection (for example, if some of such data is deemed sensitive by their standards), as well as influence any informational rights or claims they may feel they have towards such data. To satisfy the requirement of transparency and hence valid consent as regards drone data processing, a prior, important consideration should be to find out what the residents of the target communities actually know about the processing abilities of drones.

This was the objective of this research carried out, as chosen case study areas, in the Northern Malawi districts of Rumphi and Karonga, both internationally earmarked as flood-risk zones. Both districts were also part of a vast territory to be covered by an impact-based, flood-modelling exercise organised by UNICEF Malawi Malawi, and our intended research targets were 21 residents from each of these districts (total of 42 residents) who had witnessed the drones flying over their community. By the time of our visit, UNICEF Malawi had carried out the exercise in Rumphi but suspended their progress before getting to Karonga, which led us to improvise into hiring a private drone pilot to fly a drone over the community, take some high-resolution pictures and select some research targets from the onlookers. And to ensure engagement from the research targets, this research opted for focus group discussions (FGDs - Khan et al.) as data collection tool, based on the Micro-Interlocutor Analysis methodology proposed by Onwuegbuzie et al.

From the results of the FGDs, it was observed first of all that a large majority of the participants were seeing a drone for the first time (with the UNICEF Malawi flood-modelling in Rumphi and our private drone in Karonga), and were mostly fascinated by it. In Rumphi, they admitted that they were unaware of the high-resolution images of their communities which drones can take; which led to the conclusion that UNICEF Malawi, as data processing organisation, did not adequately inform the locals of their processing operation, hence they did not effectively guarantee the data processing principle of transparency. Also, while most of the participants wished they could provide consent for such high-resolution images to be taken of them and/or their community by drones, the paper concluded that such consent (most certainly through a traditional ruler) would hardly be valid as a ground for collecting and/or processing aerial image data of their community, given their vulnerable position as persons in crisis. And finally, the discussions revealed an albeit slight favourable opinion towards a feeling of community data rights, with a slight majority of the participants believing the nature of the drone images of their community could reasonably warrant some related collective community right or claim. However, they manifested no real interest in knowing more about these community rights on drone images of their settlements. Rather, a significant 76% of them preferring to have drone data of their community shared to as many third parties as possible to attract external aid, and appeared less bothered about any eventual violations of their (DII) community rights.

The above prompts the conclusion that considering certain low levels of data literacy and unawareness of (big) data analytics among people in vulnerable situations, and associated risks like surveillance, algorithmic bias or profiling, protecting PII or DII in humanitarian situations should be the full responsibility of the processing organisation. Not much participation may be expected from the affected individuals who are in (sometimes urgent) need hence vulnerable, or would generally lack the resources to engage with the organisations as regards any rights they may believe they have on data collected about them or their community. This is even more ominous when we consider the idea that humanitarian innovation could be regarded as an inherently 'experimental' process [35] with novel and untested technologies and tools sometimes being deployed to manage crisis. These innovative technologies may also belong to private sector organisations who may be taking advantage of crisis situations to "test" new technologies or products to aid intervention, with the intent of using the feedback to prepare the product for a proper commercial launch. It is worth mentioning here that the 2021 Malawi Data Protection Bill states that personal data can be processed (among other legal bases - and hence no need for consent from the individuals) where such processing is necessary for a 'humanitarian initiative.'[11] A direct interpretation would mean drones could legally be deployed to a community to collect aerial imagery (and without need for consent by the residents) if the collector organisation claims it is doing so for a humanitarian initiative. It would however appear relevant in this context for the Malawi legislator to go further and set the scope of what constitutes a 'humanitarian initiative', specify who can execute it and set other modalities to comply with, in order to prevent abuse of this basis of data processing (and hence avoid humanitarian experimentation) by tech enterprises.

It can therefore be concluded from the above that it is up to organisations to act responsibly and implement data protection-by-design strategies to protect data subjects when deploying drones to these communities e.g. integrating no-fly zones into the drone settings, or ensuring that the technology employed collects just the images needed to attain the objective for collection and/or processing. Another point to consider here for further research and discussion would be to assess the extent to which humanitarian organisations, especially those not subject to national law, invest to comply with their own data protection policies, or otherwise how they can effectively be held accountable for PII or DII processing violations. The conundrum being that though international law does provide for (data processing) principles to which international organisations pledge allegiance, they are not subject to some authority which could, for example, impose sanctions on them for data-related misconducts; like a national data protection authority would do on an organisation subject to national law.

[11] Article 18(2)(g), Malawi Data Protection Bill 2021.

ANNEX 1: Full Results of FGDs

FGD QUESTIONS TO PARTICIPANTS	RESPONSES		TOTAL % RESPONSES
	RUMPHI (21 participants. *Pertinent opinions raised by some participants in italics*)	**KARONGA (21 participants. *Pertinent opinions raised by some participants in italics*)**	
What were your (first) impressions when you saw the drone fly?	15 excited 6 curious	10 excited 6 curious 5 fear	**60% Excited 28% Curious 12% Fear**
Have you seen other drone flights and where?	16 No 5 yes	21 No	**88% No 12% Yes**
Have you seen a picture taken by a drone before?	19 No 2 Yes	21 No	**95% No 5% Yes**
Do you think these drones (can) take clear, detailed pictures of your village, farms, houses, children?	14 yes 7 no *(drones were too far up*)	17 yes (*noticed camera when drone was flying low*) 4 No	**74% Yes 26% No**
- [Showing them an aerial drone image of their district] What do you see in this example of aerial imagery (can they identify and/or recognise, roads, farms, private compounds)?	21 Can identify objects. *Can also identify richer vs poorer households based on roof material*.	21 Can identify objects. *Can also identify richer vs poorer households based on roof material.*	**100% Can identify objects of their community in the aerial images**
What are your impressions/opinions of these images?	20 Fascinated, Awed 1 Sceptical: *says they should be informed about purpose of the images*	21 Fascinated	**98% Fascinated 2% Sceptical**
What do you personally feel about these pictures, seeing that they show details of your houses, farms, and entire community?	19 Positives (*beautiful, touristic pictures; it is good to know what the community looks like*) 2 Worried about zooming ability of the drone and possibility of identifying someone	20 Positives (*the image of my house does not bother me if the image contains other houses of the community*). 1 Worried about purpose for taking the image	**93% Positive 7% Express some worries**
Is there anything in this picture you may not like other people in the village or elsewhere to see (e.g. roofless toilets, new property, maybe inside a fenced compound)?	20 Nothing about the pictures to hide or is sensitive. [*no police so it contributes to security, community development, flood management, humanitarian intervention. Sharing images of roofless toilets will force owners to put roofs over them to avoid shame. We fence our houses against thieves, not for privacy*] 1 *Cites naked children playing as sensitive and should not be*	18 Nothing about the pictures to hide or is sensitive. [*Sharing images of roofless toilets will force owners to put roofs over them to avoid shame]* 3 Say prisons could be sensitive [*it's not ok to capture and share identifiable images of high-end criminals like murderers*]	**90% Nothing to hide 10% Some data could be sensitive and may not be shared outside the community**

	captured		
Generally, with who may you not want such images of your property or community to be shared (maybe state land/town planning officials)?	20 No restrictions: images may be shared widely. [*The wider the shared audience, the more likely we are to receive external aid*] 1 Share widely but first edit out sensitive data like naked children or open toilets.	18 No restrictions: images may be shared widely [*if images depict something shameful it will only deter the person concerned into responsible behaviour*] 3 Share widely, leaving out sensitive data like prisons	**90% No sharing limitations** **10% Some data is sensitive and may not be shared outside the community**
Were you aware the drones flights you witnessed would take place?	7 Yes 14 No [*no one specified that there will be machines flying in the sky and taking pictures]*	[irrelevant]	**67% Yes** **33% No (Rumphi Only)**
If yes, how were you informed? And by who?	Traditional authorities moved door to door	[irrelevant]	/
Were you aware or informed that the flying drones will be taking clear, detailed images of your community?	21 No	[irrelevant] *But 21 expressed the wish to be informed beforehand about the details of the images*	**100% No (Rumphi Only)**
Do you know the person or organisation flying the drones?	21 No	irrelevant	**100% No (Rumphi Only)**
Did they come and present themselves to you?	21 No [*5 participants approached the drone pilots and were informed the activity was organised by UNICEF*]	irrelevant	**100% No** **(Rumphi Only)**
- Did anyone tell you whether and why it is necessary to take these drones pictures of you and your community?	21 No	irrelevant	**100% No** **(Rumphi Only)**
Do you think you should be informed first before the flying of a drones over your community to take such pictures?	21 Yes	21 Yes	**100% Yes**
Would you like to be individually able to grant or refuse permission (consent) for these images to be taken and shared with third parties?	18 Yes [*7 of these 18 believed it has to be in consultation with the chief i.e. you have to pass through the chief, then the chief consults them*] 3 Not really [*our government cannot harm us*]	19 YES 2 not really [*once informed, our consent does not need to be sought because it concerns the community*]	**88% Yes** **12% Not Really**

- In your opinion, should an authority be empowered to give permission (consent) on behalf of the entire community for these images to be taken and shared with third parties?	15 NO [*The authority must consult us or at least some key community members*] 5 YES [*provided the images are not sensitive, as is the case with these images*] 1 Neutral	21 NO [Authority must consult us or at least some key members of the community]	**86% No** **12% Yes** **2% Neutral**
If yes, who do you think should have that authority? And why?	21 The traditional chief. Because he is closer to the residents.	/	**100% Traditional Chief**
- Do you feel you may have any individual rights on these images (e.g. how long they keep it, who they share it with), considering they show your compound or farm?	9 Yes 12 No [*The drone images of their community are not so important to warrant individual rights*]	13 Yes 8 No [*The drone images of their community are not so important to warrant individual rights*]	**52% Yes** **48% No**
Do you think as a community, you all as a group can have any rights e.g. how long they keep it, who they share it with, on these images showing your community?	11 yes 10 No [*The drone images of their community are not so important to warrant community rights*]	12 yes 9 No [*The drone images of their community are not so important to warrant community rights*]	**55%Yes** **45% No**
Are you aware of any specific information-related rights you may have on these images?	20 No 1 Yes [*cites their right to access to information in the Constitution of Malawi*]	21 No	**98% No** **2% Yes**
Has anyone mentioned anything to you about any rights you may have regarding these images of you or your community?	21 No	irrelevant	**100% No** **(Rumphi Only)**
- Would you mind that these detailed drone images of your property and community is shared with government and other parties so they help you better during (flood) crisis, without caring much about your rights around these images?	21 No, the images can be shared with as many third parties as necessary [*1 participant says they should at least be made aware of whom they intend to share the images with*]	11 No, the images can be shared with as many third parties as necessary. 10 Yes [*if there are any rights available, we still want them to be respected*]	**76% No** **24% Yes**
Do you think humanitarian organisations or government could still help you effectively	21 No [*we think drone pics are necessary, they make it easier to bring us the help needed*].	20 No [*we think drone pics are necessary, they make it easier to bring us the help needed*].	**98% No** **2% Neutral**
without the need for these drone images?		1 neutral	
After this discussion, do you think drones are a positive or negative development for your community?	21 Positive [easier survey, faster information processing and communication] *1 participant cites safety concern if drone malfunctions and falls to the ground*]	20 Positive [easier survey, faster information processing and communication] 1 neutral	**98% Positive** **2% Neutral**

References

1. Jones, R.W., Despotou, G.: Unmanned aerial systems and healthcare: possibilities and challenges. In: 2019 14th IEEE Conference on Industrial Electronics and Applications (ICIEA), pp. 189–194. IEEE (2019)
2. Tang, C.S., Veelenturf, L.P.: The strategic role of logistics in the industry 4.0 era. Transp. Res. Part E: Logistics Transp. Rev. **129**, 1–11 (2019)
3. Jumbert, M.G., Sandvik, K.B.: Introduction: what does it take to be good?. In: The Good Drone, pp. 1–25. Routledge (2016)
4. Clarke, R.: Understanding the drone epidemic. Comput. Law Secur. Rev.. Law Secur. Rev. **30**(3), 230–246 (2014)
5. do C. Martins, L., Hirsch, P., Juan, A.A.: Agile optimization of a two-echelon vehicle routing problem with pickup and delivery. Int. Trans. Oper. Res. **28**(1), 201–221 (2021)
6. Haidari, L.A., et al.: The economic and operational value of using drones to transport vaccines. Vaccine **34**(34), 4062–4067 (2016)
7. Bolman, B.: A revolution in agricultural affairs: dronoculture, precision, capital. In: The Good Drone, pp. 129–152. Routledge (2016)
8. Unal, M., Bostanci, E., Sertalp, E.: Distant augmented reality: Bringing a new dimension to user experience using drones. Digit. Appl. Archaeol. Cult. Heritage **17**, e00140 (2020)
9. Wang, N., Christen, M., Hunt, M.: Ethical considerations associated with "humanitarian drones": a scoping literature review. Sci. Eng. Ethics **27**(4), 51 (2021)
10. Lidén, K., Sandvik, K.B.: Poison pill or cure-all: drones and the protection of civilians. In: The Good Drone, pp. 75–98. Routledge (2016)
11. Li, G.Q., Zhou, X.G., Yin, J., Xiao, Q.Y.: An UAV scheduling and planning method for post-disaster survey. Int. Arch. Photogrammetry Remote Sens. Spatial Inf. Sci. **40**, 169–172 (2014)
12. Lei, T., et al.: The application of unmanned aerial vehicle remote sensing for monitoring secondary geological disasters after earthquakes. In: Ninth International Conference on Digital Image Processing (ICDIP 2017), vol. 10420, pp. 736–742. SPIE (2017)
13. Weitzberg, K., Cheesman, M., Martin, A., Schoemaker, E.: Between surveillance and recognition: rethinking digital identity in aid. Big Data Soc. **8**(1), 20539517211006744 (2021)
14. Kuner, C., Marelli, M., Barboza, J.Z., Jasmontaite, L.: Handbook on data protection in humanitarian action. International Committee of the Red Cross (2020)
15. World Food Programme Guide to Personal Data Protection and Privacy (2016)
16. Schwartz, P.M., Solove, D.J.: Defining 'personal data' in the European Union and US. Bloomberg BNA Priv. Secur. Law Rep. **13**(1581), 1–6 (2014)
17. Raymond, N.A.: Beyond "do no harm" and individual consent: reckoning with the emerging ethical challenges of civil society's use of data. Group Priv.: New Challenges Data Technol., 67–82 (2017)
18. Taylor, L.: Safety in numbers? Group privacy and big data analytics in the developing world. In: Taylor, L., Floridi, L., van der Sloot, B. (eds.) Group privacy. Philosophical Studies Series, vol. 126, pp. 13–36. Springer, Cham (2017)
19. Purtova, N.: Health data for common good: defining the boundaries and social dilemmas of data commons. In: Adams, S., Purtova, N., Leenes, R. (eds.) Under Observation: The Interplay Between eHealth and Surveillance. LGTS, vol. 35, pp. 177–210. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-48342-9_10
20. van der Sloot, B.: Do groups have a right to protect their group interest in privacy and should they? Peeling the onion of rights and interests protected under article 8 ECHR. In: Taylor, L., Floridi, L., van der Sloot, B. (eds.) Group privacy. Philosophical Studies Series, vol. 126, pp. 197–224. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-46608-8_11

21. Hustinx, P.: EU data protection law: The review of directive 95/46/EC and the proposed general data protection regulation." Collected courses of the European University Institute's Academy of European Law, 24th Session on European Union Law (2013)
22. Ottavio, M.: Privacy and data protection implications of the civil use of drones European Parliament Brussels (2015)
23. UNICEF Policy on Personal Data Protection (2020). https://www.unicef.org/supply/media/5356/file/Policy-on-personal-data-protection-July2020.pdf. Accessed 27 Mar 2023
24. UN-GGIM, Future trends in geospatial information management: the five to ten year vision, Second Edition, 2015
25. Gevaert, C.: Unmanned aerial vehicle mapping for settlement upgrading (2019)
26. Khan, M.E., Anker, M., Patel, B.C., Barge, S., Sadhwani, H., Kohle, R.: The use of focus groups in social and behavioural research: some methodological issues. World Health Stat. Q. **44**(3), 145–149 (1991)
27. Morgan, D.L.: Focus Groups as Qualitative Research, vol. 16. Sage publications, Thousand Oaks (1996)
28. Onwuegbuzie, A.J., Dickinson, W.B., Leech, N.L., Zoran, A.G.: A qualitative framework for collecting and analyzing data in focus group research. Int J Qual Methods J Qual Methods **8**(3), 1–21 (2009)
29. Solove, D.J.: Murky consent: an approach to the fictions of consent in privacy law. SSRN 4333743 (2023)
30. Dressel, J., Farid, H.: The accuracy, fairness, and limits of predicting recidivism. Sci. Adv. **4**(1), eaao5580 (2018)
31. Solove, D.J.: The Digital Person: Technology and Privacy in the Information Age, vol. 1. NyU Press, New York (2004)
32. De Hert, P., Gutwirth, S.: Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action. In: Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. (eds.) Reinventing data protection? Springer, Dordrecht (2009). https://doi.org/10.1007/978-1-4020-9498-9_1
33. Dove, E.S., Kelly, S.E., Lucivero, F., Machirori, M., Dheensa, S., Prainsack, B.: Beyond individualism: is there a place for relational autonomy in clinical practice and research? Clin. Ethics **12**(3), 150–165 (2017)
34. Reviglio, U., Alunge, R.: I am datafied because we are datafied: an Ubuntu perspective on (relational) privacy. Philos. Technol. **33**(4), 595–612 (2020)
35. Sandvik, K.B., Jacobsen, K.L., McDonald, S.M.: Do no harm: a taxonomy of the challenges of humanitarian experimentation. Int. Rev. Red Cross **99**(904), 319–344 (2017)