Threat Modelling for Geodata in the Humanitarian Context

Brian K. Masinde * , Caroline M. Gevaert , Michael H. Nagenborg , Jaap A. Zevenbergen

Posted Date: 3 August 2023

doi: 10.20944/preprints202308.0312.v1

Keywords: geodata; group privacy; demographically identifiable information; humanitarianism; disasters, threat models

Article

Threat Modelling for Geodata in the Humanitarian Context

Brian Masinde [1,*], Caroline Gevaert [2,†], Michael Nagenborg [3,†] and Jaap Zevenbergen [1]

[1] Department of Urban and Regional Planning and Geoinformation Management, University of Twente
[2] Department of Earth Observation, University of Twente
[3] Department of Philosophy, University of Twente
* Correspondence: b.k.masinde@utwente.nl
† These authors contributed equally to this work.

Abstract: The role of geodata technologies in humanitarian action is arguably indispensable in determining when, where and who needs aid before, during and after a disaster. However, despite the advantages of using geodata technologies in humanitarianism (i.e., fast and efficient aid distribution), several ethical challenges arise including privacy. The focus has been on individual privacy, however, in this article we focus on group privacy whose debates have recently gained attention. We approach privacy through the lens of informational harms that undermine the autonomy of groups and control of knowledge over them. Using demographically identifiable information (DII) as a definition for groups, we first assess how these are derived from geodata types used in humanitarian DRRM. Secondly, we discuss four informational harm threat models: (i) biases from missing/underrepresented categories, (ii) the mosaic effect – unintentional sensitive knowledge discovery from combining disparate datasets, (iii) misuse of data (whether it is shared or not); and (iv) cost-benefit analysis (cost of protection vs. risk of misuse). Lastly, borrowing from triage in emergency medicine, we propose a geodata triage as a possible method for practitioners to identify, prioritize, and mitigate these four group privacy harms.

Keywords: geodata; group privacy; demographically identifiable information; humanitarianism; disasters, threat models

1. Introduction

The role of geodata technologies (i.e., technologies used to collect, store, and analyze geodata) in humanitarian action is arguably indispensable; it is instrumental in determining when, where and who needs aid before, during and after a disaster (natural or man-made). Therefore, there has been a quickly evolving adaptation of geodata technologies by incorporating a variety of new geodata types, finding new uses for existing types, and new analytical methodologies, for example the use of Artificial Intelligence (AI).

However, despite the advantages of using geodata technologies in humanitarianism (i.e., fast and efficient aid distribution), several ethical challenges arise including privacy. Privacy becomes a particularly pressing issue since the data subjects are often among the most vulnerable in society [1–3] . Vulnerable not only due to the effects of disasters, but also because of existing and persistent socio-economic inequalities, injustices, and power imbalances. Moreover, privacy violations in the digital humanitarian space can be argued to challenge the humanity principle [1] [4,5] since privacy preserves human dignity [6].

But privacy continues to be a "contested concept" [7] with diverging legal, technological, and cultural dimensions [8] . Of all the conceptualizations of privacy, we focus on informational privacy which is strongly associated with (geo)data technologies [9]. Furthermore, viewing informational

[1] Humanity principle advocates for the unconditional safeguarding of every individual's life and dignity [4]

privacy through the lens of informational harms – as has been done for personal information by Van den Hoven [10] – allows for a better understanding of the impacts of privacy violations. However, rather than focus on individual privacy and harms we primarily consider group privacy, whose debates have emerged relatively recently, and how these group-related harms materialize from use of geodata technologies. Informational harms not only undermine individuals' control of knowledge about them but affects groups as well [9].

Previously, the trend was to focus more on the individual (i.e., personal data protection) and the informational privacy threats accompanying geodata collected on individuals [11,12]. Listing four challenges in informational privacy, Floridi [13], while giving "organizations" and "artificial constructs [of groups]" as examples, highlights the inadequacy of individual privacy concept as it does not cater for groups. But, unlike personal data and the re-identification problem in individual privacy, threats to group privacy are not as straightforward [14]. First, there is the challenge of defining groups and this has implications on the kind of privacy in question [15]. Grouping based on defining the properties first tend towards "its" privacy, while grouping first then defining objectives favors "their" privacy (sum of individual privacy) [15]. Despite the late start of debates on group privacy, concerns on group privacy are growing and compounded by the fact that aggregation, clustering or grouping individuals based on some characteristics is often the objective of data analytics [14,15] and the methods used to create such groupings or recommend decisions for groups tend to be opaque and prone to biases. Therefore, there has been a call to also consider the group and informational privacy threats arising from collection, aggregation, classification, processing and sharing of group level data [15]. Majeed et al. [16] remark that "group privacy is an underrated but worth studying problem". Group privacy has also recently attracted attention in civil societies' (incl. humanitarianism's use of (geo)data technologies), for example by Raymond [17] who tackles group privacy by first expounding on the groups of interest - through the concept of demographically identifiable information (DII) - and why it is problematic in terms on group privacy.

Raymond [17] defines DII 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, and/or other demographically defining factors. DII can include, though is not limited to, personal identifiable information (PII), online data, geographic and geospatial data, environmental data, survey data, census data, and/or any other dataset 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".

In this paper we use DII as the definition of a group. DII allows us to consider both algorithmically determined groups and social groups. Often, the impacts/outcomes of data technologies on algorithmically determined groups are felt disproportionately by existing social groups (e.g., biases) [18]. More precisely, algorithmically determined groups can correlate with not one but multiple intersecting social constructs (e.g., race, ethnicity, religion, gender, socio-economic status etc.). DII is therefore "rules first" method of defining groups and therefore leans on "its" privacy.

The main objective of this paper, is to expand our understanding on the link between location data processing and group privacy in the context of humanitarian action. An understanding of group privacy in this context requires an investigation of the geodata technologies and the groups they represent or form and the informational harms that arise. Therefore, we first explore the types of geodata used in disaster risk reduction and management (DRRM). Then, using the definition of DII we explore how these geodata types are used within the context of DRRM to classify, identify and track communities. For example, remote sensing images in combination with AI have been used to extract rich sets of DII (e.g., socio-economic characteristics in settlements) used for decision making.

Secondly, we give examples of threat models that emerge in the group context with respect to DII and geodata from first objective. We categorize these into four broad informational harms: (i) biases from missing/underrepresented categories; (ii) mosaic effect – unintentional sensitive knowledge discovery from combining disparate datasets and AI's role in facilitating and accelerating data mosaicking which obscures (minute) data problems (e.g., biases) that sum up in the end; (iii) misuse of data (whether it is shared or not); (iv) cost-benefit analysis (cost of protection vs. risk of misuse). Finally, we discuss geodata triage with examples of how to prioritize group privacy risks based on the four informational harms.

These four harms are motivated by the fact that decisions are based on inferences from the group and these inferences are often prone to biases. There is also a tendency to merge disparate datasets to complement each other, creating new information with unprecedented potential for misuse by other parties. All these in combination with the unknown costs-benefits of protecting group privacy creates a situation where violations go undetected. While we do not offer mitigation strategies due to the broadness and contextual dependency of these informational harms we see the urgency and importance in a triage process which can be used to determine which group informational harms should be prioritized for mitigation when faced with resource constraints and an impending humanitarian disaster. There is an inherent tension in (disaster) humanitarianism between fast response, accuracy and non-maleficence that requires a debate about prioritising and its ethical implications. We build on Raymond's "demographic threat triage" [17] which we interpret as a two-stage process of proactively and critically assessing the threats accompanying different datasets and their corresponding application context (threat modelling) followed by assessing the urgency of remedial action for each.

Discussion on group privacy in geodata studies is well overdue given the potential of location data in analytics and its implications on privacy. In this paper we hope to bridge the gap between philosophy, ethics, and geodata technologies in the context of humanitarian action for DRRM and contribute to the discussion on the meaning of a trustful and ethical use of geodata technologies. We aim to show (using DII as a way of conceptualizing groups) humanitarians and geodata scientists how to evaluate the impact of group privacy on vulnerable communities.

2. Geodata in Humanitarian Action—Drrm

DRRM includes both anticipatory actions and response to disasters by humanitarians. Risk in this context is defined as a function of hazard, exposure and vulnerability (social and/or physical) [19] and it quantifies the probability of loss/damage of assets in the event of a hazard (see Equation (1)). The factor of location is central to all three components in the risk equation and thus important in determining where and whom to give resources. This explains the ever-evolving variety of geodata types used for DRRM. Incorporating different kinds of geodata in DRRM complements the inadequacy of individual geodata types in expressing demographic characteristics required to estimate the risk of the population due to a hazard. In this section, first we give examples of geodata types used for DRRM particularly focusing on remote sensing data and in-situ data. We do not intend to give an extensive review of all geodata types, but rather a brief description of both commonly used and nascent types with reported potential for future use. These geodata typologies become useful in the following sections on the discussion of the threats emerging especially from data mosaicking. Secondly, we categorise what DII each geodata type represents distinguishing between exposure, physical and social vulnerability.

$$Risk = f(hazard, exposure, vulnerability) \tag{1}$$

Remote sensing (RS) data is a broad category of geodata used in DRRM which includes satellite images, imagery from unmanned aerial vehicles (UAVs), and street view images. The use of UAVs and street view images is nascent in DRRM applications compared to satellites. The main advantage of using RS data is the timeliness of data collection, cost efficiency and the relative ease of scaling up [20–22]. This is compared to using in-situ data collection methods like field surveys which can be costly and time consuming when the area coverage is large. RS data capture two important components in the risk equation, namely the exposure (i.e., the exposed infrastructure) and physical vulnerability (i.e., susceptibility of the exposed infrastructure to the hazard). Social vulnerabilities are only implicitly inferred from RS data via proxies from characterization of the exposed infrastructure and their corresponding vulnerabilities. Social vulnerability thus often requires datasets that complement the RS data, for example, social protection data, household surveys, and or census data which also often contain spatial references [20].

In-situ geodata used for DRRM include - but are not limited to - surveys (e.g., household), census, call detail records (CDRs), and social protection data. In-situ data can be point observations with geographical references or spatially aggregated data. For example, household surveys can contain the coordinates of participants' houses, CDRs contain the location of a mobile phone user at a particular time. In contrast to other in-situ data, CDRs present different ethical problems primarily due to lack of explicit consent by the data subjects and claims that anonymizing CDRs is a solution for the privacy concerns while overlooking the group tracking implications [23]. We therefore find it important to include CDRs in this discussion. In summary, the main advantage of in-situ data collection is that it can be tailored to capture specific information that are otherwise unavailable (e.g., specific household vulnerability) but with the downside of costs.

Since each component in the risk equation aims to empirically infer different information, in the following subsections we describe the DII derivable (via use of proxies) for exposure, physical and social vulnerability estimation. These components are primarily used to infer patterns in the population that particularly make them susceptible to hazards.

2.1. Exposure

RS data give high resolution information on the exposed elements in an area. These include buildings, transport infrastructure (e.g., roads), service infrastructures offering critical service (e.g., power/communication lines, water reservoirs/points). Satellite images and UAVs offer a view from above that gives insight on the characteristics and distribution of infrastructure on ground while street view images give a street perspective, for example, the façade of buildings and number of floors - which are not observable from above [24,25]. Having an overview of what is exposed is a step that precedes vulnerability quantification while determining the risks. Street view images have gained importance in auditing the built environment for post-disaster evaluation [26] and recovery [27]. Though the use of CDRs is not common, research notes that it has high potential for future use in DRRM [28]. CDRs give insights on population distribution and mobility [28]. These can be assessed prior and after a disaster [29]. Population distribution is important in quantifying exposure, especially when census data is unavailable. In this case CDRs can give lower bound on the number of people affected [28]. CDRs have particularly become a niche geodata type in tracking spread of diseases as cascading effects of disaster (e.g., post Haiti 2010 earthquake) [28,29]. The location where diseases occur become the point of interests used to classify, track and identify groups at risk, hence in this case location is the primary DII compared to RS data where infrastructure are the DII.

2.2. Physical Vulnerability

In DRRM literature, it is anticipated that among the exposed assets, there would be varying susceptibility to different kinds of hazards. This leads to the physical vulnerability characterization of the communities' exposed assets. This characterization is inferred by the proxies of building density, road network, façade building materials, building heights, and roof types. For example, Harb et al. [30], note that roof-types can be used as a proxy to physical vulnerability as different roof-types have differential susceptibility to hazards, while heterogenous building heights in a neighborhood increase physical vulnerability of an area in case of earthquakes. Similarly, façade building characterization is important for earthquake, tsunami, and flood physical vulnerability assessments [21,24,25,31].

2.3. Social Vulnerability

In a review of RS data proxies in disaster management, Ghaffarian et al. [20], elaborate how roof-typology, land use ratio, green spaces, road widths and densities can be used to infer socio-economic vulnerability. Roof typology as a social vulnerability proxy (extractable from RS data because different materials reflect different colors) is based on the assumption that roof materials are indicators of income or wealth since it costs more to construct buildings with quality roofing materials [20]. However, this assumption, is dependent on the locational context. The quality of roads (density/connectivity and potholes) is used as a proxy since, often deprived areas have poor road connectivity [20]. Land use ratio and available green spaces are also proxies for social vulnerability as green spaces are often scarce in low-income areas/neighborhoods [20]. Similar to roof typology, building typology derivable from street view images is also considered a proxy of social vulnerability as low-income households and business owners often live or rent buildings with high physical vulnerability to disasters simply because they cannot afford otherwise. However, these (building typology) are usually considered to be weak proxies for social vulnerability [20]. It is also important to note that street view images usually capture more than just the building and can include people walking on the streets and license plates of cars. These are usually blurred before sharing or using in maps (e.g., Google Street View) but interestingly some homeowners are averse to having the images of their houses captured in the first place [32]. As mentioned before, RS data have limits in quantifying social vulnerability and this is where in-situ data become very important. In-situ data collection methods are usually tailored to directly capture demographic variables that are direct factors for vulnerability. For example, household survey and social protection data would capture information such as income, occupation, household size and composition. For CDRs, the main utility in the context of social vulnerability is in tracking movement in and out of a disaster zone and becomes especially useful monitoring spread of infectious diseases (i.e., a disease breakout in an area can be spread to new areas where the affected migrate to) [28,29]. In-situ data sets also serve as ground truth data for RS data.

In the conversation of informational privacy and harms it does not suffice to only examine data typologies without investigating the role of technologies/methods used to process data to meaningful actionable information. For example, large scale RS satellite is processed using AI (e.g., building detection/classification) and certainly this makes satellite data actionable. In the section that follows, we briefly discuss the complexities that AI presents in privacy. This is an important precursor for threat models section.

3. Geodata Technologies: Artificial Intelligence (Ai) in Humanitarian Action

AI has gained much attention and accelerated adaptation in humanitarianism. The shift from reactive to an anticipatory approach in humanitarianism is arguably one of the reasons why AI has become useful. Anticipatory approach through use of AI and data (both small and big data [2]) facilitates the prediction of needs of vulnerable communities before a disaster occurs through impact-based forecasting (i.e., pre-disaster impact assessment on communities through DRRM) and forecast-based financing (i.e., early access to funds before a disaster to mitigate the predicted impact) [33,34]. The use of AI is now very much engrained in RS methods in the two broad categories of object-based methods and pixel-based methods. It is used to map settlements, detect damaged buildings, and audit the built environment for recovery post disaster. Figure 1 demonstrates building detection and delineation using AI while Figure 2 shows classification outcome of a UAV image.

[2] Big data includes both structured and unstructured data with the four Vs properties; volume, veracity, velocity and variety

doi:10.20944/preprints202308.0312.v1

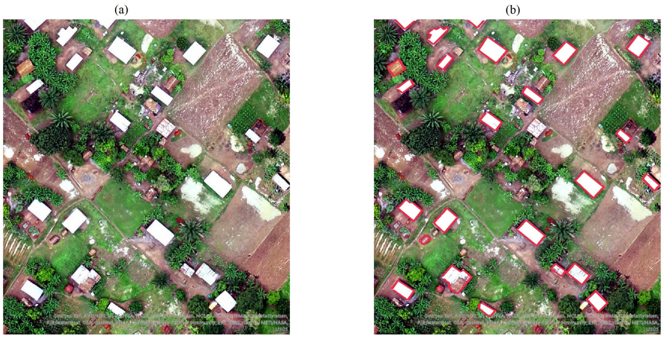

Figure 1. (a) Shows UAV image and (b) is a corresponding dummy example of building delineation - a task that is commonly done using AI.

The use of AI raises the concerns of biases and data privacy in humanitarianism. However, the discussion on these two ethical concerns is often focused on the individual (for the latter) and assumed to be disjointed. The link between biases and privacy is not adequately explored in ethics of humanitarian use of geodata technologies with only implicit references to human rights law; privacy as a human right and protection from discrimination (e.g., by Beduschi [1] and by Pizzi et al. [35]). On biases, recently, examples abound, the neutrality and fairness of AI (including the data used to train AI models) has been in question. For example, in predicting recidivism [36] and recruitment process [37]. AI and data are not neutral tools and are known to include and amplify biases [38]; biases from the data collection and biases of the designers (algorithmic bias) [39]. This is further compounded by the black-box nature of most AI algorithms that makes it difficult to understand how the algorithm reaches it's decision [40]. Bias concerns thus become entwined with group privacy (because of AI's ability to learn, amplify and reinforce biased patterns) these affect the group and not just an individual.

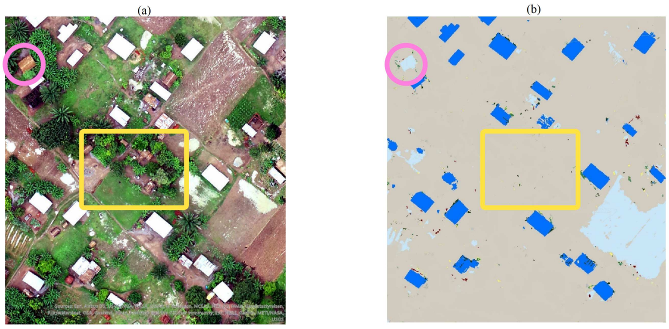

Figure 2. (a) Shows UAV image with areas of interest while (b) shows a classification outcome using AI. Both show how biases occur in AI mapping. The building circled in pink is misclassified while other similar types are not identified at all (area in yellow rectangle).

4. Threat Models

Threat models describe the privacy challenges (geo)data technologies present. It is becoming increasingly important to conduct privacy threat modelling considering the fast evolution and adaptation of sociotechnical systems across all fields with unprecedented privacy risks and harms [41]. Threat models go beyond the checklist procedure that is typical of privacy impact assessments which Shapiro [42] finds to be inadequate for tackling informational harms. And thus threat modelling could range from reflections on what could possibly go wrong to sophisticated simulations of how a socio-technical system affects privacy. In this article we rely on reflections on informational privacy concerns based on informational harms concerns already identified for data technologies using AI.

As mentioned before, there has been a tendency to focus on individual privacy which does not cover the informational privacy issues that accompany use of data technologies especially in the age of AI. Majorly, the informational harms that arise from creation of group level data and categorization. Literature on ethical uses of data technologies for humanitarian action often mention bias as a concern. Recently, there has been a call to also consider the mosaic effect; being new knowledge accrued from the combination of disparate datasets (see Capotosto [43]). Privacy literature argues that though respective datasets may seem harmless (with little privacy concerns) the combination of these create new data products with information and inferential opportunities beyond what was originally intended [42,44]. We observe that geodata, specifically coordinates, boundaries (spatial references), and AI make it easy to combine (add layers of disparate datasets), process, analyze and perform predictive tasks with relative ease. It is also prudent to consider other (mis)use of the data acquired for humanitarian action. Furthermore, threat models have to consider the utility between cost of preventing harm and the probability of the informational harms. The costs of preventing harm may outweigh the probability of some informational harms.

In light of the issues discussed above vis a vis (geo)data technologies and AI we limit the discussion on informational harms to four threats. The first are biases from missing/underrepresented categories. Second, the mosaic effect – unintentional (sensitive) knowledge discovery from combining disparate datasets; and AI's role in facilitating and accelerating data mosaicking which obscures (minute) data problems (e.g., biases) that sum up in the end. Third, misuse of data (whether it is shared or not). Fourth, cost-benefit analysis (cost of protection-vs-misuse risk). These threat models are agnostic and can be investigated in any geodata technology for humanitarian action. To the best of our knowledge there are no other studies that conduct group threat modelling for geodata technologies in humanitarian action.

4.1. Biases (From Missing Categories or Missing Data on Entire Groups or Misclassification)

Considering the types of geodata commonly used in humanitarian action, and the use of AI for anticipatory disaster management, it is evident that informational privacy in this context leans towards the collective. Remote sensing data, especially, contain very little to no personally identifiable information but in combination with AI it is used to create categories of people with differing needs for aid (e.g., characterizing physical vulnerability by classifying roof typologies). Using geodata and AI as categorization technologies then leads us to consider biases as informational privacy harms as underrepresentation, misclassification, and ill-constructed categories affecting the collective with common DII attributes. No doubt that these biases trickle down to the individual, but this effect is only possible via the use of the DII in question [15]. Viewing biases as violations of privacy is in line with other informational privacy research. For example, from a legal perspective Crawford and Schultz [45] list discrimination as one of several informational harms from "predictive big data"[3] . Not to forget the implications on autonomy which is fundamental for informational privacy [9,46]. Categorization that is characteristic of (geo)data technologies considered here provides no autonomy for individuals and groups to decide whether or not they want to be part of the group [47].

In the following paragraph, we consider an example of using remote sensing images to identify and delineate buildings now commonly used analysis step in data-driven humanitarian work. It is not always the case that there is homogeneity in the size, roof-type, and spacing of buildings (see example in Figure 1). Given the trend to use remote sensed data and AI to generate maps on vulnerable communities, it has emerged that such complexities (i.e., size, roof typology, and spacing among buildings) can lead to biases in the generated maps. Notably, these attributes are proxies of demographic aspects (e.g., socio-economic status) and hence DII. A specific case is where a humanitarian organization is interested in mapping an area prone to flooding. Assuming the only

[3] "Predictive big data" is used as a collective; both data and the AI technology

geodata available to humanitarians in this scenario is satellite images or UAV images limited to giving an overhead perspective of the area. This constrains the mapping exercise to identify buildings via their roof types. Heterogeneity in roof typology complicates automated mapping using AI especially if there is low occurrence of some types. Such sample imbalance often results in biased classifications in mapping using AI (e.g., Abriha et al., [48]). Often standard practice in experimental situations is to remove classes with low samples so as to improve overall accuracy. While roof typologies are strong proxies (in some contexts/locations) for socio-economic status, they are not social groups per se (i.e., not a social construct like ethnicity) and thus possibly no discrimination with respect to visibility of the households solely based on those roof typologies. But misclassification creates a situation where humanitarians have to worry about which other biases are amplified. For example, some roof types may correlate with informal settlements which are often inadequately served by government functions. This scenario can be extrapolated to using street view images for identification and classification of buildings.

Biases do not only occur during classification. They can occur during data collection or from the data generating process. Mehrabi et al., [49] give a comprehensive survey of the different ways biases materialize in machine learning. Certainly, biases can also occur in in-situ data collection methods.

It is important to note that conversation on biases irrespective of the data technology used cannot/shouldn't be separated from issues of power (imbalance) and (in)justice. In this case, the power lies with the humanitarians; they decide on which communities to focus and the approaches to take. It is not certain whether humanitarians actively involve vulnerable communities in all stages of designing AI methods for anticipatory action.

4.2. Mosaic Effect

The mosaic effect is a phenomenon that occurs when seemingly unrelated datasets or pieces of information are combined to create new information [43]. While each individual datasets may seem harmless [44], combining them especially through analysis, allows creation of a new information product that reveals more about an individual/population than originally intended as "boring" data points gain more significance [42]. Adriaans [50] links mosaicking to the additivity concept where two datasets give more information than one. Though the mosaic effect is often discussed from an individual privacy perspective with the harm being re-identification, for example in linkage attacks that aim to re-identify individuals such as in Netflix data [51] or DNA genotype-phenotype data [52], new data mosaics may have far-reaching implications for group privacy as well. In the context of humanitarian action this line of research is still nascent with literature highlighting mosaic effect concerns on open datasets for humanitarian action mosaicked with social protection data [43]. An example that showcases this trend in combining social protection data and other geodata is in Malawi [53].

In geodata, direct (e.g., coordinates) and indirect (e.g., addresses or administrative boundaries) spatial references [54] are a medium that facilitate linking disparate datasets. For example, satellite and UAV images can be linked with street view images, census data, social protection data and surveys or census data. As mentioned before, integrating socio-economic data complements the shortcomings (sometimes weak proxies) of some remote sensing data and this is only possible through intersecting locations of various datasets. This is evident in anticipatory action for disasters in humanitarianism, for example mosaicking UAV images with street view images and social protection data. While UAV images and street view images combine to show physical vulnerability due to a hazard, social protection data complements this by showing the social component of vulnerability (e.g., income and health). Depending on the granularity (e.g., from administrative boundaries to household level) of the mosaicked data this can show patterns in the populations such as clusters with incidents of certain diseases. This information is important for humanitarianism but a group privacy threat if accessible to the wider public.

The role of AI in data mosaicking cannot be overstated. Each dataset may have its own information extraction process. For example with satellite or UAV images the task may be to classify built areas, map green spaces, or classify parcels of lands into use categories (e.g., industrial, farm, residential). Street view images on the other hand can be used to classify building typologies, while other datasets like household surveys give insights on socio-economic and behavioral patterns of communities. All these tasks are increasingly carried out by AI which makes the informational flow easier and faster for decisions. Ultimately, this creates a rich set of detailed DII. Repeating the process from data collection, to processing using AI with some more regular frequency then this becomes quintessential surveillance with immense knowledge accrual on vulnerable communities. Whether this knowledge is shared with people or organizations with similar principles of "do no harm" or not does not excuse the question whether so much knowledge on vulnerable groups should be gathered and stored in the first place without understanding the risks first [17].

As an example, consider a flood prone area where, for aid delivery other than predictions of the amount of rainfall or flood level, a humanitarian organization would also need to know what is exposed, what are the physical vulnerabilities and the social vulnerability of the community (i.e., can they cope?). Should they also worry about disease outbreaks that commonly accompany flooding? No one dataset suffices to give information on all of these characteristics. RS data with the use of AI as discussed previously is used to detect and classify buildings and based on this characterization a damage index can be developed for the various building typologies. But that is as much information extricable from RS data. For social vulnerability, humanitarians in this case would turn to in-situ geodata (e.g., social protection data) that gives information on how well the community is able to cope with the disaster. These data would contain indices such as, household income, level of education, and health etc. Combining RS data and social vulnerability geodata humanitarians can make group level inferences for example socio-economic and vulnerability status for the various building typologies. Such inferences consequently are used to decide the amount of aid to give to various groups. Adding CDRs to these datasets enables tracking; where are the various groups of affected people moving to? The resulting mosaic DII exceeds the potential for each individual dataset typology with potential for other (mi)uses. Even though it might not be fine grained DII but from a broader view/perspective gives information on groups. Furthermore, if there are biases in each geodata typology and the resulting inferences then these problems sum up and result in a biased DRRM process.

4.3. Misuse—(Known) Blind Spots: What Else Could This Data Be Used For?

Data misuse is simply using data for purposes that were not originally intended. In individual informational privacy, this is framed as uses which individuals did not explicitly consent to. The informational harms towards individuals and groups are covert surveillance and unwanted solicitation [55], for example through personalized ads and marketing strategies that nudge people to spend on items, vote in favor or against someone/something or generally behave in a certain way. Inferences that allow for this targeting are made possible by DII which allow for categorization and tracking of groups in the first place. In modelling misuse threats of geodata technologies one has to consider other parties' interests (e.g., governments and organizations). Context and socio-political dynamics also factor in. For example, in countries with civil strife, the concern is that geodata collected by humanitarians could be used for surveillance by oppressive governments or malevolent groups. With experimental technologies modelling threats due to misuse requires quite a bit of foresight, otherwise one has to rely on past incidences as examples – as we do here.

Geodata and geodata technologies discussed in sections before not only provide useful DII for DRRM applications but have value in other applications as well. Remote sensing images will inevitably capture or contain other objects of interest for other applications. Hence, there is a concern about geodata and the resulting DII acquired from vulnerable communities for anticipatory action being used for other purposes that do not align with the humanitarian agenda. Examples include but are not limited to: (i) detailed temporal geodata could be used for surveillance by malevolent parties on vulnerable communities (ii) geodata is useful in marketing and service industry (iii) upgrading programs that can lead to displacements or gentrification; for example in informal settlements. Raymond et al. [56] give an example case of the project Sentinel where temporal satellite data was used to analyze the progression of conflict in the Sudan. The DII in this case was vehicle size used to identify military vehicles and house clusters showing settlements. The temporal satellite data did not meet the humanitarian objective but instead may have unintentionally served the antagonists with real time intelligence through the sharing of the near real time information and analysis [56]. Raymond et al. [56] further remark that this might have turned "everyone" else to a witness. This example shows that sharing information in a conflict setting is harmful despite the good intentions of humanitarian work.

RS data are also used in other development agendas and this are usually multi-stakeholder (e.g., governments and private investors). RS data has uses for poverty/deprivation mapping [57]. This is useful in determining where to focus resources for development. While development is advantageous at face value, critical studies ask advantageous for whom(?). Communities living in such deprived areas are often concerned about displacement without alternatives [57]. If it is improved housing or neighborhood that is hazard resilient it could end up being out of financial reach for the original inhabitants leading to gentrification. This is no doubt a social justice issue.

In sum, threat modelling for misuse not only shows that we need to consider other uses but also requires a review of whom to trust and this can be done through considering compatibility of principles/values. In the case of sharing data humanitarians are urged to "share alike", that is share information with others that subscribe to the same principles of "do no harm" [43,58]. This means that trust is needed among humanitarian organizations and between organizations and communities that share geodata containing DII. Due diligence cannot be over-emphasized to ensure geodata and geodata technologies are not misused to disadvantage vulnerable communities.

4.4. Cost-Benefit Analysis

Cost–benefit analysis in this context considers the cost of protecting group information versus the potential for misuse. Cost-benefit here does not consider the economical tradeoffs with respect to costs but rather as values. If the costs of protection outweigh the potential for misuse then there's no incentive for protection leaving data subjects vulnerable to informational harms. With regard to group privacy and DII, the risks are not usually perceived to be as grave as those posed to an individual. This is not necessarily true, especially in the context of (geo)data technologies and AI where the risks of collecting and sharing DII are not immediately clear and this might be confused for non-existent or minimal risks. While there's no evidence to show that the protecting group information is less important compared to individual information, this can cause a laxity and the potential for information harm still goes undetected and unchecked. Reactiveness as opposed to proactiveness in threat modelling on group informational harms persist - if not increase - the potential for informational harms as more varieties of geodata and geodata technologies are used.

In humanitarianism there is an inherent tension between visibility and privacy from the beneficiaries' point of view [59]. While generating knowledge on vulnerability of groups is problematic in this case it is actually needed for aid resource allocation. The issue to consider is whether the discussion is balanced rather than leaning towards a lax stance; lack of threat modelling and triage while only looking at the knowledge discovery potential. Given that we do not yet have a comprehensive understanding of informational harms poised to the group (given they are context specific) therefore cannot claim that the benefits always outweigh the risk.

5. Geodata Triage

Raymond [17] advocates for continuous "demographic threat triage" as a mechanism to identify and keep abreast with the evolving harms related to DII collected and processed by civil society (incl. humanitarianism). Triage here is thought of as an independent step following threat modelling (identification of the risks and harms possible) since triage can only be done after understanding the harms. Therefore, revisiting our threat models discussed above, we give examples of triage scenarios with respect to DII and context.

Triage is useful when there are situations competing for attention amidst a lack of resources. For instance, in emergency medicine, incoming patients at a hospital undergo an initial assessment of "severity of illness or injuries" prioritizing resources (e.g., time, equipment, and personnel) for the most urgent cases [60]. Triage concept has also been utilized for other situations where resource constraints necessitate prioritization. DRRM in humanitarianism for example, is essentially a triage process with its own ethical considerations [61]. Besides triaging vulnerable communities at risk of disasters and assessing the data needs for decision making it is prudent that informational privacy triage should be undertaken as well. Ideally, all kinds of (geo)data should be handled with utmost care but resource constraints (e.g., time, personnel etc.) during anticipatory preparations and response would compel humanitarians to prioritize some data types and analysis approaches over others.

Similar to medical triage we find it useful to categorize geodata technologies into intervention, observation and non-action based on informational harms from DII (see Table 1). The intervention category includes contextually sensitive DII (especially when opaque AI methods are used) with potential for most harm, and must be prioritized for appropriate intervention. Observation, would contain geodata with DII that do not immediately warrant intervention but none the less should be monitored. For example geodata and use cases where the informational harms are not yet immediately clear. Non-action category means the geodata is stored securely and not in use, and therefore the threat discussed above do not apply.

Table 1. Geodata Triage

Category	Description
Intervention	Contextually sensitive geodata should always be prioritized for intervention. Lower tier move up to intervention with active use of the geodata for intervention. With appropriate interventions the geodata and technology can be moved to observation category.
Observation	Non-action category moves up to observation category once we plan to use geodata and especially when considering merging disparate data (i.e., mosaicking).
Non-action	Due diligence has been done on datasets and respective processing technologies and they have been stored in secure servers. In this category the geodata are not in use nor shared.

It is also important to consider the movement between categories. We suggest that location context and evolving situations on the ground play a role in category movement. For example, if a disaster-prone area suddenly and unfortunately became a contested territory between two rival countries then any geodata and processes that allow for aggregation, categorization and tracking of groups becomes even more sensitive. Because such scenarios are hard to predict it therefore becomes ever more important to continuously triage geodata.

Recalling the example of classification of buildings by roof types from UAV data with the outcome being a map of the affected area dictating where to concentrate resources. If AI is the primary method for classification, then biases as information harm trump other harms. The priority becomes determining which demographic groups are of interest in the classification task. If the harm is biases against a vulnerable group, then solving or mitigating for the biases takes precedence over novel knowledge creation and harms from misuse. Because of the urgency in humanitarian work this ensures that the task is done correctly and aid resources are allocated appropriately. Misclassifying roof types or buildings characteristic of a vulnerable demographic group would be a disastrous harm as it would lead to inadequate aid. If there are minimal risks to biases, but rather the greater risk is in misuse of the demographic data (e.g., tracking vulnerable groups by malevolent parties) then this case trumps general novel knowledge creation on groups. Then the mitigation in this case is careful consideration on the disclosure, sharing, and what else could it be used for including which other datasets could it be mosaicked with.

6. Discussion

Defining groups is certainly still a challenge in group privacy scholarship. In this paper we used the concept of DII coined by Raymond [17] which in sum is any information that can be used to classify, identify or track groups of people. We highlight that geodata is particularly prone for exposing DII and that it therefore requires special attention in responsibly making data actionable. Sampling a variety of commonly used and novel geodata types in humanitarianism for DRRM we set out to understand how they are used or can be used to classify, identify and or track people. Remote sensing data - which includes satellite images, UAV images and street view images - were most commonly used to classify physical vulnerabilities of infrastructure (esp. buildings). For example, roof types and building size have been documented to be useful DII in characterizing physical vulnerabilities. But often these need to be complemented by in-situ data types such (e.g., household surveys). CDRs on the other hand are an emerging geodata type specifically used to track movements in and out disaster areas with particular interest in spread of infectious diseases. The second objective was to conduct threat modelling for group privacy. Since geodata technologies used in disaster humanitarianism are used to classify or discriminate between groups that need aid, biases emerged as one of the major informational harms. Biases not only undermine the impartiality principle in humanitarianism, dampen trust between organizations and communities they serve but also may divert aid from where it is needed the most. Biases may occur from misclassification and biased data (in the case of in-situ data). There is also concern about the extent of new knowledge generation on vulnerable communities that comes from mosaicking disparate datasets. What emerges is that location makes it easy to merge disparate datasets and AI makes it easier to process such data. However, such automation with methods that are considered black box are prone to amplifying data problems. We also reflect on what else these geodata technologies could be used for: that is outside of the humanitarian context. The same data used to decide whom to give aid, may very well be used to decide whom to evict from disaster prone areas or contested land. Group privacy thus far has not received the attention it deserves compared to individual privacy. The costs and benefits analysis of group privacy needs a detailed investigation since so far the costs seem greater than the reward. In sum, as geodata technologies evolve threat models need to keep up as well. Though we do not yet offer solutions or mitigation strategies for the group informational harms discussed above, we do initiate a discussion on triage and what it would entail. Drawing from triage in emergency medicine we also find it useful to categorize geodata as either needing intervention, under observation or non-action. What we find to be particularly difficult with triage is the metrics to use in the categorization. The subjectiveness of the triage brings to the forefront the power of the decision maker. For accountability, triage processes should be transparent (i.e., making it known why certain geodata and informational harms are prioritized over others). An important lesson from our attempt at triaging, is the need to contextualize the harms. Asking which group is at risk and why gives insights in how to prioritize group privacy. The example triage given above may, however, not necessarily be optimal in other contexts. Therefore, we see applications for "contextual integrity" [62] in this group privacy triage as well.

7. Conclusions

The humanitarian field has strived to leverage (geo)data technologies, especially in DRRM to determine where, when and whom to give aid (e.g., the use of early warning early action and forecast based financing systems). Humanitarians always strive to abide by their core principles [4] and this

[4] Humanitarianism is governed by 4 core principles of humanity, impartiality, neutrality, independence [4]

translates to how they process information on vulnerable communities because of privacy concerns, mainly because of the potential of the information to be used for non-humanitarian purposes by malevolent groups. However, the privacy concerns focused on personal information (e.g., names of refugees) while, for example, location of camps and basic aggregate demographic information would still be available to the public. Moreover, it has emerged that geodata leveraged by humanitarians for DRRM purposes do not necessarily contain personal information but still have potential for harm. This is the premise of group privacy, more so when the objective and the norm of geodata technologies is to generate groups to aid in decision making [15].

We therefore set out to unravel the group privacy harms foreseeable from geodata technologies commonly used in humanitarian action, specifically DRRM. We leveraged the concept of DII which is concerned with information that can be used to classify, identify or track groups. Particularly focusing on geodata (e.g., remote sensing images) and the use of AI to analyze these we explored four potential informational harms. These were (i) biases, (ii) mosaic effect, (iii) misuse and (iv) cost benefit analysis.

One of the debates on group privacy is how to define groups in the first place and this has implications on whether to aim for "their privacy" or "its privacy" [15]. From the example use cases of geodata technologies we note that the groups are formed based on rules that are predefined and change based on context. For example, use of remote images to classify buildings by roof typology or build materials. These are not the typical demographic groupings (gender, age, etc.) but rather are used as proxies for other contextual attributes of interest. In case of flooding, different buildings characterized by their build materials will incur differential damage. Such background knowledge on the susceptibility of buildings to hazards dictates how to classify these buildings. But these are buildings that households live in and thus correlates with other socio-economic and cultural dynamics. Therefore, using DII to define groups means focusing on "its" (ref. group) privacy rather than "their" privacy.

Biases from data technologies in general is a rising concern especially where AI is involved to make decisions that affect people. Using the example of roof typology as DII and how biases can emerge during classification due to under-representation we demonstrated how these can perpetuate existing social inequities when applied to the humanitarian agenda. Furthermore, there is the persistent concern of what other new DII could emerge from combination of disparate geodata in combination with AI. There is the risk of these DII creating new knowledge with potential for misuse outside the scope of humanitarian work. The fact that cost-benefit analysis (cost vs potential for misuse) for group privacy is currently considered to be secondary to personal information privacy is a big informational harm concern. The potential for misuse of DII is equally concerning in some contexts as individual privacy if not more. In light of this, geodata triage becomes an important aspect in prioritizing geodata technologies and context for group privacy preservation. Looking ahead, geodata studies and humanitarianism would benefit from a more robust methodology for triaging group privacy for example through using a metric.

Author Contributions: Brian Masinde: Conceptualization, Writing - Original Draft, Investigation, Visualization. Caroline Gevaert: Conceptualization, Writing - Review & Editing, Supervision. Michael Nagenborg: Conceptualization, Writing – Review & Editing, Supervision. Jaap Zevenbergen: Writing – Review & Editing, Project administration.

Funding: "Do No harm" project is funded by Dutch Research Council (NWO – MVI) and UNICEF. The project also benefits from collaborations with 510, an initiative of the Netherlands Red Cross.

Acknowledgments: We acknowledge Fran Meissner for invaluable comments on the manuscript. We also acknowledge Adam Henschke for insightful discussion on privacy and data mosaicking.

Conflicts of Interest: Authors declare no conflict of interest

Abbreviations

The following abbreviations are used in this manuscript:

DII	Demographically Identifiable Information
DRRM	Disaster Risk Reduction & Management
RS	Remote Sensing
CDRs	Call Detail Records

References

1. Beduschi, A. Harnessing the potential of artificial intelligence for humanitarian action: Opportunities and risks. *International Review of the Red Cross* **2022**, *104*, 1149–1169. doi:10.1017/S1816383122000261.
2. Hayes, B. Migration and data protection: Doing no harm in an age of mass displacement, mass surveillance and "big data". *International Review of the Red Cross* **2017**, *99*, 179–209. doi:10.1017/S1816383117000637.
3. Barnett, M.N. Humanitarian governance. *Annual Review of Political Science* **2013**, *16*, 379–398. doi:10.1146/annurev-polisci-012512-083711.
4. Slim, H. *Humanitarian ethics: A guide to the morality of aid in war and disaster*; Oxford University Press, 2015.
5. Sandvik, K.B.; Jacobsen, K.L.; McDonald, S.M. Do no harm: A taxonomy of the challenges of humanitarian experimentation. *International Review of the Red Cross* **2017**, *99*, 319–344. doi:10.1017/S181638311700042X.
6. Floridi, L. On human dignity as a foundation for the right to privacy. *Philosophy & Technology* **2016**, *29*, 307–312. doi:10.1007/s13347-016-0220-8.
7. Mulligan, D.K.; Koopman, C.; Doty, N. Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* **2016**, *374*, 20160118. doi:10.1098/rsta.2016.0118.
8. Bennett, C.J.; Raab, C.D. *The governance of privacy: Policy instruments in global perspective*; Routledge, 2017.
9. Roessler, B. Three dimensions of privacy. In *The handbook of Privacy Studies*; Groot, D.; Van der Sloot, B., Eds.; Amsterdam University Press Amsterdam, 2018; pp. 138–141. doi:10.1017/9789048540136.005.
10. Van den Hoven, J. Privacy and the varieties of informational wrongdoing. In *Computer ethics*; Weckert, J., Ed.; Routledge, 2017; pp. 317–330. doi:10.4324/9781315259697-34.
11. Georgiadou, Y.; de By, R.A.; Kounadi, O. Location Privacy in the Wake of the GDPR. *ISPRS international journal of geo-information* **2019**, *8*, 157. doi:10.3390/ijgi8030157.
12. Keßler, C.; McKenzie, G. A geoprivacy manifesto. *Transactions in GIS* **2018**, *22*, 3–19. doi:10.1111/tgis.12305.
13. Floridi, L. Four challenges for a theory of informational privacy. *Ethics and Information technology* **2006**, *8*, 109–119. doi:10.1007/s10676-006-9121-3.
14. Taylor, L. Safety in numbers? Group privacy and big data analytics in the developing world. In *Group privacy: New challenges of data technologies*; Taylor, L.; Floridi, L.; Van der Sloot, B., Eds.; Springer, 2017.
15. Taylor, L.; Floridi, L.; van der Sloot, B. Introduction: A new perspective on privacy. In *Group privacy: New challenges of data technologies*; Taylor, L.; Floridi, L.; Van der Sloot, B., Eds.; Springer, 2017; pp. 1–12.
16. Majeed, A.; Khan, S.; Hwang, S.O. Group Privacy: An Underrated but Worth Studying Research Problem in the Era of Artificial Intelligence and Big Data. *Electronics* **2022**, *11*, 1449. doi:10.3390/electronics11091449.
17. Raymond, N.A. Beyond "do no harm" and individual consent: reckoning with the emerging ethical challenges of civil society's use of data. In *Group Privacy: New Challenges of Data Technologies*; Taylor, L.; Floridi, L.; Van der Sloot, B., Eds.; Springer, 2017; pp. 67–82.
18. Taylor, L. What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society* **2017**, *4*, 2053951717736335. doi:10.1177/2053951717736335.
19. Wang, Y.; Gardoni, P.; Murphy, C.; Guerrier, S. Empirical predictive modeling approach to quantifying social vulnerability to natural hazards. *Annals of the American Association of Geographers* **2021**, *111*, 1559–1583. doi:10.1080/24694452.2020.1823807.
20. Ghaffarian, S.; Kerle, N.; Filatova, T. Remote sensing-based proxies for urban disaster risk management and resilience: A review. *Remote sensing* **2018**, *10*, 1760. doi:10.3390/rs10111760.

21. Velez, R.; Calderon, D.; Carey, L.; Aime, C.; Hultquist, C.; Yetman, G.; Kruczkiewicz, A.; Gorokhovich, Y.; Chen, R.S. Advancing Data for Street-Level Flood Vulnerability: Evaluation of Variables Extracted from Google Street View in Quito, Ecuador. *IEEE Open Journal of the Computer Society* **2022**, *3*, 51–61. doi:10.1109/OJCS.2022.3166887.
22. Curtis, J.W.; Curtis, A.; Mapes, J.; Szell, A.B.; Cinderich, A. Using google street view for systematic observation of the built environment: analysis of spatio-temporal instability of imagery dates. *International journal of health geographics* **2013**, *12*, 1–10. doi:10.1186/1476-072X-12-53.
23. McDonald, S.M. Ebola: a big data disaster. *Privacy, property, and the law of disaster experimentation (CIS Papers 2016.01). Delhi: Centre for Internet and Society* **2016**.
24. Park, H.; Cox, D.T.; Barbosa, A.R. Comparison of inundation depth and momentum flux based fragilities for probabilistic tsunami damage assessment and uncertainty analysis. *Coastal Engineering* **2017**, *122*, 10–26. doi:10.1016/j.coastaleng.2017.01.008.
25. Pelizari, P.A.; Geiß, C.; Aguirre, P.; Santa María, H.; Peña, Y.M.; Taubenböck, H. Automated building characterization for seismic risk assessment using street-level imagery and deep learning. *ISPRS Journal of Photogrammetry and Remote Sensing* **2021**, *180*, 370–386. doi:10.1016/j.isprsjprs.2021.07.004.
26. Lenjani, A.; Yeum, C.M.; Dyke, S.; Bilionis, I. Automated building image extraction from 360 panoramas for postdisaster evaluation. *Computer-Aided Civil and Infrastructure Engineering* **2020**, *35*, 241–257. doi:10.1111/mice.12493.
27. Mabon, L. Charting disaster recovery via Google Street View: A social science perspective on challenges raised by the Fukushima Nuclear Disaster. *International Journal of Disaster Risk Science* **2016**, *7*, 175–185. doi:10.1007/s13753-016-0087-4.
28. Cinnamon, J.; Jones, S.K.; Adger, W.N. Evidence and future potential of mobile phone data for disease disaster management. *Geoforum* **2016**, *75*, 253–264. doi:10.1016/j.geoforum.2016.07.019.
29. Bengtsson, L.; Lu, X.; Thorson, A.; Garfield, R.; Von Schreeb, J. Improved response to disasters and outbreaks by tracking population movements with mobile phone network data: a post-earthquake geospatial study in Haiti. *PLoS medicine* **2011**, *8*, e1001083. doi:10.1371/journal.pmed.1001083.
30. Harb, M.M.; De Vecchi, D.; Dell'Acqua, F. Phisical vulnerability proxies from remotes sensing: reviewing, implementing and disseminating selected techniques. *IEEE Geoscience and Remote Sensing Magazine* **2015**, *3*, 20–33. doi:10.1109/MGRS.2015.2398672.
31. Gonzalez, D.; Rueda-Plata, D.; Acevedo, A.B.; Duque, J.C.; Ramos-Pollan, R.; Betancourt, A.; Garcia, S. Automatic detection of building typology using deep learning methods on street level images. *Building and Environment* **2020**, *177*, 106805. doi:10.1016/j.buildenv.2020.106805.
32. Miller, C.C.; O'brien, K.J. Germany's complicated relationship with Google Street View. *The New York Times* **2013**.
33. Costella, C.; Jaime, C.; Arrighi, J.; Coughlan de Perez, E.; Suarez, P.; Van Aalst, M. Scalable and sustainable: How to build anticipatory capacity into social protection systems. *IDS Bulletin* **2017**. doi:10.19088/1968-2017.151.
34. Van den Homberg, M.J.; Gevaert, C.M.; Georgiadou, Y. The changing face of accountability in humanitarianism: Using artificial intelligence for anticipatory action. *Politics and Governance* **2020**, *8*, 456–467. doi:10.17645/pag.v8i4.3158.
35. Pizzi, M.; Romanoff, M.; Engelhardt, T. AI for humanitarian action: Human rights and ethics. *International Review of the Red Cross* **2020**, *102*, 145–180. doi:10.1017/S1816383121000011.
36. Angwin, J.; Larson, J.; Mattu, S.; Kirchner, L. Machine bias. In *Ethics of Data and Analytics*; Martin, K., Ed.; CRC Press, 2022. doi:10.1201/9781003278290-37.
37. Dastin, J. Amazon scraps secret AI recruiting tool that showed bias against women. In *Ethics of data and analytics*; Martin, K., Ed.; CRC Press, 2022; pp. 296–299. doi:10.1201/9781003278290-44.
38. Smith, C. Dealing With Bias in Artificial Intelligence. *The New York Times* **2019**.
39. Pessach, D.; Shmueli, E. Algorithmic fairness. *arXiv preprint arXiv:2001.09784* **2020**.
40. Diakopoulos, N. Algorithmic accountability: Journalistic investigation of computational power structures. *Digital journalism* **2015**, *3*, 398–415. doi:10.1080/21670811.2014.976411.
41. Sarrala, T.; Mikkonen, T.; Nguyen Duc, A.; Abrahamsson, P. Towards Identification of Privacy Requirements with Systems Thinking. International Symposium on Business Modeling and Software Design. Springer, 2022, pp. 249–258. doi:10.1007/978-3-031-11510-3_16.

42. Shapiro, S.S. Time to Modernize Privacy Risk Assessment. *Issues in Science and Technology* **2021**, *38*, 20–22.
43. Capotosto, J. The Revelation Risks of Combining Humanitarian and Social Protection Data. *Humanitarian Law & Policy* **2021**.
44. Henschke, A. *Ethics in an age of surveillance: personal information and virtual identities*; Cambridge University Press, 2017.
45. Crawford, K.; Schultz, J. Big data and due process: Toward a framework to redress predictive privacy harms. *BCL Rev.* **2014**, *55*, 93.
46. Tavani, H.T. Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy* **2007**, *38*, 1–22. doi:10.1111/j.1467-9973.2006.00474.x.
47. Kammourieh, L.; Baar, T.; Berens, J.; Letouzé, E.; Manske, J.; Palmer, J.; Sangokoya, D.; Vinck, P. Group privacy in the age of big data. In *Group privacy: New challenges of data technologies*; Taylor, L.; Floridi, L.; Van der Sloot, B., Eds.; Springer, 2017; pp. 37–66.
48. Abriha, D.; Srivastava, P.K.; Szabó, S. Smaller is better? Unduly nice accuracy assessments in roof detection using remote sensing data with machine learning and k-fold cross-validation. *Heliyon* **2023**, *9*. doi:10.1016/j.heliyon.2023.e14045.
49. Mehrabi, N.; Morstatter, F.; Saxena, N.; Lerman, K.; Galstyan, A. A survey on bias and fairness in machine learning. *ACM computing surveys (CSUR)* **2021**, *54*, 1–35. doi:10.1145/3457607.
50. Adriaans, P. Information. In *The Stanford Encyclopedia of Philosophy*; Zasta, E., Ed.; 2020.
51. Narayanan, A.; Shmatikov, V. Robust de-anonymization of large sparse datasets. 2008 IEEE Symposium on Security and Privacy (sp 2008). IEEE, 2008, pp. 111–125. doi:10.1109/SP.2008.33.
52. Harmanci, A.; Gerstein, M. Quantification of private information leakage from phenotype-genotype data: linking attacks. *Nature methods* **2016**, *13*, 251–256. doi:10.1038/nmeth.3746.
53. Gualavisi, M.; Newhouse, D.L. Integrating Survey and Geospatial Data to Identify the Poor and Vulnerable: Evidence from Malawi. Technical report, Washington, DC: World Bank, 2022.
54. Lakes, T. Geodata. *SSRN Electronic Journal* **2009**. doi:10.2139/ssrn.1452635.
55. Calo, R. The boundaries of privacy harm. *Ind. LJ* **2011**, *86*, 1131–1162.
56. Raymond, N.A.; Davies, B.I.; Card, B.L.; Achkar, Z.A.; Baker, I.L. While we watched: Assessing the impact of the satellite sentinel project. *Georgetown Journal of International Affairs* **2013**, pp. 185–191.
57. Lin, L.; Di, L.; Zhang, C.; Guo, L.; Di, Y. Remote Sensing of Urban Poverty and Gentrification. *Remote Sensing* **2021**, *13*, 4022. doi:10.3390/rs13204022.
58. Vannini, S.; Gomez, R.; Newell, B.C. “Mind the five”: Guidelines for data privacy and security in humanitarian work with undocumented migrants and other vulnerable populations. *Journal of the Association for Information Science and Technology* **2020**, *71*, 927–938. doi:10.1002/asi.24317.
59. Weitzberg, K.; Cheesman, M.; Martin, A.; Schoemaker, E. Between surveillance and recognition: Rethinking digital identity in aid. *Big Data & Society* **2021**, *8*, 20539517211006744. doi:10.1177/20539517211006744.
60. Christ, M.; Grossmann, F.; Winter, D.; Bingisser, R.; Platz, E. Modern triage in the emergency department. *Deutsches Ärzteblatt International* **2010**, *107*, 892. doi:10.3238/arztebl.2010.0892.
61. Zack, N. The ethics of disaster planning: Preparation vs response. *Philosophy of Management* **2009**, *8*, 55–66. doi:10.5840/pom20098216.
62. Nissenbaum, H. Privacy as contextual integrity. *Wash. L. Rev.* **2004**, *79*, 119.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.