A moderate interpretation of group privacy illustrated by cases from disaster management

Gerdes, Anne

Published in:
Journal of Contingencies and Crisis Management

DOI:
10.1111/1468-5973.12336

Publication date:
2020

Document version:
Final published version

Document license:
CC BY

Citation for pulished version (APA):
Gerdes, A. (2020). A moderate interpretation of group privacy illustrated by cases from disaster management. *Journal of Contingencies and Crisis Management*, *28*(4), 446-452. https://doi.org/10.1111/1468-5973.12336

Received: 6 October 2020 | Accepted: 7 October 2020
DOI: 10.1111/1468-5973.12336

ORIGINAL ARTICLE

A moderate interpretation of group privacy illustrated by cases from disaster management

Anne Gerdes

Department of Design and Communication, University of Southern Denmark, Kolding, Denmark

Correspondence
Anne Gerdes, Department of Design and Communication, University of Southern Denmark, Kolding, Denmark.
Email: gerdes@sdu.dk

Abstract
This article uses cases from disaster management as a springboard for presenting a critique of a right to group privacy in a strong sense. As such, the article challenges the idea of strong group privacy, which holds that there are situations in which the group, and not its members, is the holder of a right to privacy. The paper argues for a moderate interpretation of group privacy, stressing that group privacy is a matter of privacy for the members constituting the group. Although data-driven knowledge discovery implies profiling by group categorization, this observation does not constitute a reason to introduce a right to group privacy for other purposes than to protect the individual's right to privacy. The article demonstrates preliminary theoretical considerations, which may inform the creation of a framework that protects personal privacy by considering a moderate sense of group privacy suited to tackle privacy challenges implied by data analytics.

KEYWORDS
disaster management, group privacy, personal privacy

1 | INTRODUCTION

Recently, in the wake of privacy risks generated by big data analytics, discussions in favour of the concept of group privacy have gained momentum both in privacy studies in general and in the field of disaster management (Taylor (2017), Mantelero (2018)). Technological mediation utilizing big data analytics may enhance all phases of a disaster management life cycle and empower emergency organizations' capabilities. Still, such data-driven interventions do not come free of cost and may exacerbate privacy infringements. Profiling makes it possible to discover correlations between data sets that reveal patterns that may identify, explain and predict the behaviour of individuals based on their resemblance to a group. There are good reasons to be concerned as data protection legislation fails to protect data subjects from risks posed by profiling activities at the group level. As an example, protection by anonymization does not prevent violation of privacy as classifiers applied to diverse data sets without identifiers enable making inferences about individuals' behaviour. Also, in the wrong hands, adversarial use of data analytical insights may endanger vulnerable individuals. On this backdrop, the notion of group privacy is discussed. The article claims that although data-driven knowledge discovery implies profiling by group categorization, this does not justify the introduction of a notion of group privacy in a strong sense, that is arguing that there are cases in which it is only possible to anchor privacy at group level meaning that the group is the holder of a right to privacy. Moreover, examples reflecting data-driven intervention in the field of disaster management are drawn upon in illustrating privacy risks arising from group profiling activities.

2 | BACKGROUND

Before entering a detailed discussion of group privacy, the article presents techniques within data analytics to set the frame for reflections on the role of group privacy in protecting individuals' privacy. Initially, it is worth emphasizing that big data analytics is not a neutral tool as "the techniques and practices underpinning Big Data reveal the ways in which social values are encoded into mathematical processes and automated through techniques that scale normative logic" (Ellish & boyd, 2018:58).

Bearing this reservation in mind, exploratory big data analytics may apply data mining tools, data fusion, data integration techniques, and machine-learning algorithms. As such, data fusion supports data mining by using reduction techniques to produce a homogeneous representation of unstructured data, preparing data sets for subsequent processing by data mining tools. To prioritize retaining data, one may apply integration techniques allowing for the assimilation of big data sets, which produces a close to complete picture of data one has available within a given domain (PTCAS report, 2014:25). As a result, data mining algorithms may both increase the amount of accessible data and sense-making opportunities, viz discovery of patterns across large data sets. Also, by means of supervised machine learning (there are unsupervised machine algorithms, but I shall leave them aside), systems may "learn" a domain by being "rewarded" for extracting useful patterns from a training data set. After trial-and-error training sessions, machine-learning algorithms build up a domain-specific model, which can classify new data patterns. Yet, such models do not guarantee actionable insights or speak by themselves as they "usually cannot tell the user the value or significance of … patterns" (PCAST, 2014:25). Consequently, data-driven knowledge generation is less about data availability, and more about capability, that is, whether one has available the kind of human domain expertise needed to sift out relevant knowledge in revealed data patterns. As an example, domain expertise is required to sort out which data patterns, for example clusters, are relevant to a specific purpose. Likewise, domain knowledge is needed to clarify whether given anomalies, in clustering results, represent ground truth, "noise" or constitutes an outlier, that is "an observation deviation which deviates so much from other observations as to arouse suspicion that it was generated by a different mechanism" (Hawkins, 1980).

Similarly, from an epistemic perspective, emphasizing big data as a new form of ground truth may be problematic. The introduction of advanced data-driven knowledge generation may come at the cost of epistemic transparency. For example, in disaster risk management, it may be problematic to rely on real-time data streams obtained remotely far from the actual scene of events (McDonald, 2016; Taylor, 2017), and processed by opaque data analytical tools. In the same line, awareness of data quality is essential, as noted in a study by Gupta et al. (2013), which revealed that a significant number of fake images were shared and re-shared online during Hurricane Sandy. As the validation of results is increasingly slipping beyond human control, this increases the risk that biased results may go on unnoticed and hamper decision-making. Clearly, the epistemic status of inferential analyses may challenge individuals' right to privacy independently of whether the inference is correctly made or not. The mere fact that algorithmic decision-making can be legitimized does, of course, not protect the individual against privacy infringements.

A first pragmatic step towards fighting the threat from epistemic opacity is to acknowledge that domain expertise is pivotal to ensure that plausible conclusions are drawn from interpretations of statistical correlations in data patterns. Consequently, a reliable evaluation of both the quality of data sets and inferences made in explorative data analytics is a highly demanding task. Here, the fact that that explainability is challenged by black-box algorithms (Gunning, 2018) does not serve as an excuse for underestimating the role that expert-driven assessment plays in the legitimization of algorithmic decision-making.

3 | METHODOLOGY

With the above-mentioned epistemic concerns in mind, the article directs attention to issues of privacy and data protection in contexts in which data analytics utilizing profiling algorithms provides inferences and predictions at the level of groups, which subsequently facilitate the sorting out of individuals and thereby makes them vulnerable to privacy threats. Hence, the fair information practice principles behind the General Data Protection Regulation (GDPR) reflect the assumption that privacy protection equals controlling personal data, whereby the regulation of the collection, storage and retention of data plays a vital role. This control paradigm fails to meet privacy challenges in the era of big data. For example, the idea of controlling information by consent is not operational as big data analysis may reveal patterns of correlations, which nobody could foresee, which makes it impossible to ask for permission in the first place. Moreover, people do not read extensive privacy policies. If people took the time to read through privacy policies, it is estimated that they would have to spend 244 hr per year (Custers et al., 2018:253). Furthermore, the GDPR has shortcomings as it sets out to adequately protect personal data by defining personal data solely with reference to a data subject.

> "Personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
>
> (GDPR, Article 4 (1)).[1]

Taking departure in the protection of identifiable information about individuals does not hinder informational harm to individuals. Profiling activities do not need personal data to predict peoples' future behaviours or categorize them as belonging to a particular class of individuals sharing certain traits. Group profiles, without any identifiable information about specific data subjects, still make it possible to single out individuals and cause moral wrongdoing. Zuboff has coined the term *surveillance capitalism* to account for ways in which users' and groups' behaviours and preferences are predicted in a new kind of *behavioural futures market* in which people serve as raw materials for new *prediction products* (Zuboff, 2019:11). On this backdrop, the remaining parts of the article present examples from the field of disaster management to unfold a discussion of the notion of group privacy. Consequently, paying attention to groups is crucial, when describing data-driven privacy challenges and when developing data protection principles to improve data protection regulation. Some suggest that the group is the primary locus for privacy in the era of data-driven knowledge generation:

> During the Rwandan genocide, …violence was based purely on perceived ethnic group membership and not on individual identity or behavior
>
> (Taylor, 2017: 19).

> Big Data's particularity lies precisely in its ability to extract valuable information about passive groups with no such self-awareness or capacity. Thus, on the one hand, a group privacy right can help active, structured groups assert their informational self-determination and protect their own interests. On the other hand, it must be supplemented by additional protections that recognize and address the privacy interest of passive groups extracted at the data analysis stage
>
> (Kammourieh et al., 2017: 62).

Nonetheless, ontologically speaking, the above observations do not imply that there is such a thing as group privacy apart for in the sense that we need to clarify the role of the group to protect or address the privacy of its members individually. In what follows, the article challenges contemporary arguments for group privacy in the strong sense, that is in its own right, and emphasizes the importance of personal privacy. To anchor privacy at the level of the person is not only theoretically plausible but also intuitively obvious. It may also be viewed as ethically essential, in a broader sense, as the notion of a "group" may be the first step to dehumanization and neglect of human dignity and responsibility.

4 | DISCUSSION

To escape naïve nominalism and realism, Floridi considers a group, not as something that is discovered or invented, but rather "(..) *designed*, that is, they [groups] are the outcome of the coming together of the world and the mind" (Floridi, 2017:86). Hence, when we are speaking about groups, we find ourselves at the epistemological level. When it occurs to us that there are, objectively speaking, natural groups, this is just a matter of our epistemological grouping and sense-making of the world:

> Referring to salad, tomatoes and potatoes as a group called food seem something as observer-independent and objective as possible, but this is only because we assume our own interest as organisms and eaters as the natural, intuitive, and relevant LOA [ed.: level of abstraction]. To a tiger, they would all look as unrelated and as eatable as grass and leaves to us
>
> (Floridi, 2017: 86).

There are salads in the world, and there are correct ways grouping them to fit a given purpose. Floridi does not claim a relativistic position in which groups are merely social conventions. Instead, "they are more or less correctly and successfully designed by our epistemological interests and practices *together* with the ontological constraining affordances provided by the world" (Floridi, 2017:87). As a result, groups are not there before our epistemological ordering of them. Our ordering is not arbitrary; it is constrained by a given purpose, framed by a given "interested" practice of grouping, such as the practice of profiling (Floridi, 2017:89). On this background, Floridi suggests that a notion of group privacy makes sense by defending both a strong sense of group privacy as a right that belongs to the group "as a group" and a moderate sense thereof. Initially, his general arguments concerning group rights may be summed up by the following quotation:

> Determining the LOA [ed.: Level of Abstraction] is what makes talking about groups ontologically unproblematic. By grouping people, according to specific criteria we create an individual (the group), which can both be targeted and claim to have rights as a group
>
> (Floridi, 2017: 90).

Floridi then demonstrates a moderate sense of group privacy with reference to a California privacy law for minors, which grants a child the right to be forgotten online. Following up on that line, Floridi notes that "it seems obvious from the text that any reference to minors as a group … is only a shortcut for a reference to each of its members." (Floridi, 2017:91). Next, Floridi moves on to a case in which, apparently, a notion of strong group privacy is at stake. In speculating about what is understood from the idea of "a private funeral," he mistakenly reaches a conclusion that:

> it seems counterintuitive to argue that each member of the group [ed.: the participants invited to the funeral] … has a right to a private funeral, or that the privacy demanded is just the collection of all individual privacies. It seems more reasonable to admit that we are in the presence of a strong, social sense of group privacy. It is the whole group as a group that has a right to that specific kind of privacy
>
> (Floridi, 2017: 91).

However, this case does not serve as a proper illustration of group privacy in the strong sense as a right that belongs to the group as a group. Rather, what this example shows is precisely the opposite, namely that people with preferences concerning how grief is appropriately dealt with at funerals may reach a joint agreement with others, who share the same views. In that sense, we may argue that personal privacy has been met by respecting, "a collection of individual privacies" (quotation above). Had some of the group members disagreed about the conception of "a private funeral," they would not feel comfortable during the ceremony. Consequently, these members would probably have tried to re-negotiate the idea of a "private funeral" ahead of the ceremony to strike common ground by aligning individual values and expectations among the participants.

Seeking to protect personal privacy requires careful attention to mechanisms for group sorting, which does not demand, ontologically speaking, group privacy in the strong sense. Hence, there are different ways in which members of a set can be said to share a property, in our case, a right. It can be argued that one may correctly state that the individual members of the group hold a right, whereas it is implausible to talk about rights at a group level independently of the members constituting that group. Clearly, when, for example, lesbians are granted a right to marriage, it is not the group who marries, but the individuals in the group. Also, granting rights to groups is done to promote human flourishing and ensure equality for the members of a given group, typically a minority group, whose members now obtain rights on par with the rest of the society. Thereby, each individual is included as a full member of society by sharing the same rights as the majority of individuals.

Alternatively, one may argue that the notion of a group right makes sense understood at the level of the group, not at the level of its members. For instance, a company's status as a legal person and a nation's sovereignty and right of self-determination are typically drawn upon to account for this observation. Hence, at the level of states and nations, the individual cannot claim a right to sovereignty in the same sense as the nation (see, e.g., Kammourieh et al., 2017:55).

Yet, this observation may be questioned. In the American Constitution, the rights of the state are described as delegated rights. On the delegation of powers between the United States and the federal States, the 9th Amendment secure that individual rights cannot be overruled by federal states or government in the United States:

> The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.

Moreover, the 10th Amendment emphasizes that the rights of the states are "delegated" under certain conditions:

> The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.

In continuation thereof, in the book titled *Was is Autorität?* (What is Authority?), Bochénski rejects the notion of group authority by drawing attention to the contrasting ontologies of Aristotle and Hegel, *viz* Aristotle's reflection of the primacy of the individual over the group—"nach Aristoteles ist in der Gesellschaft the Einzelmensch das einzige letze Subject" ("according to Aristotle, in society the individual is the only last subject") (Bochénski, 1974:33), as opposed to the Hegelian notion of the group as a true subject—"Dagegen nimmt Hegel an, das die Gruppe ein wahres Subject is, das sogar einen eigenen Geist … besitzt" ("Against this claim, Hegel argues that the group is a true subject, which even has a mind of its own") (Bochénski, 1974:34). Clearly, according to Bochénski, Hegel does not indicate that the group, or society, as an objective mind (*Geist)*, is consciousness (*bewusstsein*). Instead, consciousness is instantiated by, for example statesmen, who, Hegel admits and mourns, of course, often lack proficiency (Bochénski, 1974:34). Bochénski coins the term "ontologischer communist" ("ontological communist") in referring to Hegel's prioritization of the group at the expense of the individual. Moreover, he points to that when speaking of the group as a holder of authority, this is only done out of convenience and serves merely as a short cut reference for the subject(s) of authority—"Der Träger der Autorität immer ist ein Einzelmensch" ("the holder of authority is always an unique individual" (Bochénski, 1974:35)). In a similar manner, the group, as such, cannot be the holder of a right to privacy besides in a moderate sense thereof.

4.1 | Personal privacy in the era of big data analytics

In continuation of the arguments above against group privacy in the strong sense, the article shall be moving on to consider the notion of personal privacy. Here, Floridi notes that information may be viewed as a "constitutive part" of a person's or group's identity, implying an interpretation of privacy as "an identity-constituting value." In a similar vein, Benn's conception of privacy emphasizes the importance of our struggle towards becoming the best versions of ourselves:

> Respect for someone as a person … implied respect for him as one engaged on a kind of self-creative enterprise, which could be disrupted, distorted, or frustrated even by so limited an intrusion as watching. A man's view of what he does may be radically altered by having to see it, as it were, through another man's eyes
>
> (Benn, 1984: 242).

Along the same line, to emphasize the importance of the context in which information is revealed and shared, a justificatory conceptual framework can be found in Nissenbaum (2010), who introduces the notion of contextual integrity to account for privacy in the era of public online surveillance. Here, Nissenbaum notices that privacy challenges cannot be adequately dealt with by invoking traditional dichotomies, assuming that information is either private or public, sensitive or not sensitive. Instead, a proper description of privacy has to be able to account for cases in which information is considered private all though it is publicly available. This is the case in situations where people experience privacy discomfort when discovering that what they share openly on social media is used by third parties for a variety of purposes. Hence, "a central tenet of contextual integrity is that there are no arenas of life not governed by norms of information flow, no information or spheres of life for which 'anything goes'" (Nissenbaum, 2004:119).

According to Nissenbaum, whether the information is considered private or not may be settled by taking departure in context-sensitive informational norms, which considers (a) the types of information in the case, (b) the respective roles of communicators and (c) principles for information flow between the parties. As such, contextual integrity views privacy, not as a right to control over information, but as a right to appropriate flows of information in contexts with the right to two informational norms (Nissenbaum, 2010:127-): norms of "appropriateness" (e.g., it is considered appropriate for me to share information about symptoms with my GP but not vice versa) and norms of "distribution," that is the moment of transfer of information from one part to another. Consequently, the distribution of information happens according to different norms of distribution in relatively stable contexts. Violations of one of these norms potentially represent a privacy infringement. Still, they do not necessarily do so as changes in informational flows can arise due to the introduction of new technologies for distribution (e.g., the shift from posting letters to sending emails does not by itself cause a privacy infringement). Nissenbaum's account of privacy complements Floridi's idea of privacy as an identity-constituting value, that is you *are* your information, whereby "a breach of an individual's informational privacy [can be viewed] as a form of aggression towards that individual's identity." This observation resonates well with privacy challenges in the era of big data analytics. Perhaps, van den Hoven foresaw this in remarking that it "is not strange that we fear information-based harm now information is becoming more and more like a gun" (van den Hoven, 1997:35).

4.2 | Protecting personal privacy against group profiling

As argued above, Floridi does not present any compelling arguments in favour of group privacy in the strong sense. Instead, he provides evidence for adopting a moderate sense of group privacy in data protection, by noticing that "sometimes the only way to protect a person is to protect the group to which that person belongs" (Floridi, 2017:98). To protect personal privacy, I cannot but agree that we need to strengthen data protection legislation to meet the challenges from inferential analysis, such as group sorting by predictive profiling. Such data-driven interventions constitute a risk to personal privacy. The fact that data analytics enables us to identify and comprehend individuals' preferences and behaviours with reference to their resemblance with passive groups, of which they are unaware that they belong to, does not imply group privacy in the strong sense, meaning that the group is the holder of privacy.

The main points discussed so far are nicely recapitulated in the quotation below. Here, it is stressed that, nowadays, privacy challenges arise due to profiling activities, which do not necessarily imply personal identification of individuals, but nevertheless provide opportunities for third parties to invade individuals' lives:

> Even when individuals are not "identifiable," they may still be "reachable," may still be comprehensively represented in records that detail their attributes and activities, and may be subject to consequential inferences and predictions taken on that basis
>
> (Barocas & Nissenbaum, 2014: 45).

Following suit, cases from disaster management may serve as useful illustrations of ways in which the identification of individuals as part of a group might facilitate moral good and moral wrongdoing dependent on the context of use. The 2010 Haiti earthquake and the 2012 Hurricane Sandy in the United States demonstrate beneficial data-driven interventions. During these crises, people's information sharing on social media and GPS data from mobile phones gave useful intelligence about people's whereabouts and experiences, which facilitated disaster mapping and emergency responses (Bengtson, Lu, Thorson, Garfield, & von Schreeb, 2011; Watson & Rodrigues, 2018).

When disasters strike, tracking peoples' movements remotely, via real-time data streams from mobile phones and social media, may enable emergency organizations to respond promptly. Data science tools for carrying out predictive analyses make it possible to anticipate peoples' movements and behaviours, and the probability of the spread of diseases or epidemics during a disaster. As such, mobile data display individuals' responses to real-time events and may be used to represent ground truth models when constructing agent-based models that enable mapping and prediction of behaviour. However, such dataveillance practices may give rise to ethical concerns (McDonald, 2016; Taylor, 2017). As an example, agent-based models provide algorithmic groupings, which may be useful to anticipate group movements during natural disasters or epidemics. Yet, in other contexts, or the wrong hands, they might be "weaponized" (Raymond, 2017:76) and provide crime opportunities by facilitating tracking down vulnerable persons. Also, at the policy level, such models may provide actionable insights that enable political decisions about how to react to avoid refugees (Taylor, 2017:25). Likewise, the quotation below highlights that traditional means, such as anonymization and informed consent, fall short of protecting privacy. Anonymization techniques are challenged when fragmentized information about data subjects enables re-identification, as illustrated in this hypothetical case below:

> an NGO managing several displaced persons' camps in country X has allowed a UN agency to publish a map showing the camps with the largest population influxes of displaced people in recent months. Sensitive infrastructure, in particular, a protection center for demobilized child soldiers, have been excluded from the maps to protect vulnerable demographics residing in the camps. Meanwhile, an agency working to assist the demobilized child soldiers at the protection center has published an online blog stating that it is providing services to these children at an unnamed camp that has experienced the largest influx of displaced people. A non-state armed actor seeking to reclaim child soldiers that had previously fought in its group cross-corroborates the de-identified map with the detail about the displaced person influx at the camp in the de-identified blog story to locate where the former child soldiers are living, enabling them to attack the camp and abduct the children
>
> (Raymond, 2017: 76).

Raymond notes that the notion of informed consent is neither required nor violated in this situation. Also, due to profiling, individuals may be members of passive groups without their awareness and hence unable to consent. Furthermore, *the tyranny of the minority* implies that even though an individual has never consented to anything, she may still be a subject of profiling since informed consent from few members of a group makes it possible to infer others, who share the same traits as the group (Barocas & Nissenbaum, 2014).

On this backdrop, Vedder suggests that companies and organizations are held morally and legally accountable as they presumably "may have at least a hunch of the possible social impacts of these activities" (Vedder, 1997). But whereas this may be feasible in the context of ordinary business to costumers' relations, alas, as illustrated above, despite the best intentions, the involved parties may end up causing moral wrongdoing. The above-mentioned hypothetical scenario illustrates a case, which cannot be solved by data protection legislation, but rather demands updating the code of ethics and conduct, which NGOs follow. According to Raymond, a refinement of the NGO code of ethics and conduct is demanding as it requires "ethical core competencies, tested methodologies, and ethical protocols that do not currently exist" (Raymond, 2017:77).

When judging data-driven interventions, it is crucial that ethical evaluations, as well as data protection regulation, take departure in what constitutes reasonable expectations of privacy within a given context of use, that is whether the data analysis is appropriate given a specific usage context (Barocas & Nissenbaum, 2014; van Hoboken, 2019). On this backdrop, it has been suggested to regulate "at the 'moment of particularization' of data about an individual, or when this is done for some minimum number of individuals concurrently" (PCAST, 2014:49). Here, the notion of a group—as "a minimum number of individuals concurrently"—is awaked to account for situations in which the group level precedes the "moment of particularization" at which the individual is reached by either being directly singled out or targeted via group membership. Clearly, here, privacy is addressed as a matter of personal privacy with attention to ways in which profiling by groups challenges personal privacy. Correspondingly, Vedder points to the need to pay particular attention to the group to safeguard the individual's privacy. He introduces the notion of *Categorial privacy* (Vedder, 1997) to account for ways in which the individual's privacy needs to be protected in cases where personal information has been transformed to de-identifiable information relating to groups. His notion of categorical privacy align with group privacy in the moderate sense in that it "has its point in respecting and protecting the individual, rather than the group to which the individual belongs" (Vedder, 1997).

5 | CONCLUSION

Increasingly, data-driven interventions mediate work processes in all phases of a disaster management life cycle by supporting, for example real-time disaster mapping and decision-making procedures, as well as enabling predictive analysis to prevent future disasters. Despite being motivated by noble goals, such initiatives can lead to moral good and moral wrongdoing, depending on the usage context. Seeking to protect the individual's right to privacy by, for example, anonymization does not prevent hostile interventions, or privacy violations brought about by big data analytics. Hence, profiling algorithms can reveal patterns in data, which makes it possible to comprehend, categorize and target individuals even though they, to begin with, were unidentified. As a result, the notion of group privacy has recently attracted attention as a possible means to protect individuals against being treated in harmful ways. However, although data-driven knowledge generation implies profiling by group categorization, this does not constitute a reason to introduce a notion of group privacy in the strong sense, indicating that the group, per se, is the holder of a right to privacy. Hence, the article outlines preliminary reflections in defence of a notion of group privacy in a moderate sense as an instrument to shield the individual's right to privacy. As such, it is argued that group privacy is a matter of privacy for the members constituting the group. Consequently, there is no right to privacy for groups for other reasons than to protect the individual's right to privacy.

ORCID

Anne Gerdes https://orcid.org/0000-0002-2991-5074

ENDNOTE

[1] GDPR: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Accessed on 13 June 2019.

REFERENCES

Barocas, S., & Nissenbaum, H. (2014). Big data's end run around anonymity and consent. In J. Lane, V. Stodden, & S. Bender (Eds.), *Privacy big data, and the public good* (pp. 44–75). Cambridge University Press.

Bengtsson, L., Lu, X., Thorson, A., Garfield, R., & von Schreeb, J. (2011). Improved response to crisis s and outbreaks by tracking population movements with mobile phone network data: A post-earthquake geospatial study in Haiti. *PLoS Medicine*, *8*(8), e1001083. Retrieved on 20 March 2020, from. https://doi.org/10.1371/journal.pmed.1001083ebola-a-big-data-crisis

Benn, S. I. (1984). Privacy, freedom, and respect for persons. In F. D. Schoeman (Ed.), *Philosophical dimension of privacy – An anthology* (pp. 223–245). Cambridge University Press.

Bochénski, J. M. (1974). *Was ist Autorität? - Einführung in die Logik der Autorität* (p. 439). Herderbücherei: Bd.

Custers, B., Dechesne, W. P., Schermer, B., & van der Hof, S. N. (2018). Consent and privacy. In P. Schaber, & A. Müller (Eds.), *The Rutledge handbook of the ethics of consent* (pp. 257–258). Routledge.

Elish, M. C., & Boyd, D. (2018). Situating methods in the magic of Big Data and AI. *Communication Monographs*, *85–1*, 57–80.

Floridi, L. (2017). Group privacy: A defence and an interpretation. In L. Taylor, L. Floridi, &L. van der Sloot (Eds.), *Group privacy – New challenges of data technologies* (pp. 83–101). Springer.

Gunning, D. (2018). *Explainable Artificial Intelligence (XAI)*. Retrieved on 20 March 2020, from (https://www.darpa.mil/program/explainable-artificial-intelligence)

Gupta, A., Lamba, H., Kumaraguru, P., & Joshi, A. (2013). *Faking sandy: Characterizing and identifying fake images on twitter during hurricane sandy*, Proceedings of the International World Wide Web Conference Committee (IW3C2), Rio de Janeiro, Brazil.

Hawkins, D. (1980). *Identification of outliers*. Chapman and Hall.

Kammourieh, L., Barr, T., Berens, J., Letouzé, E., Manske, J., Palmer, J., Sangokoya, D., & Vinck, P. (2017). Group privacy in the Age of Big Data. In L. Taylor, L. Floridi & L. van der Sloot (Eds.), *Group privacy – New challenges of data technologies* (pp. 37–67). : Springer.

Mantelero, A. (2018). AI and Big Data: A Blueprint for human rights, social and ethical impact assessment. *Computer Law & Security Review*, *34*(2018), 754–772.

McDonald, S. M. (2016). *Ebola: A big data crisis. Privacy, property, and the law of crisis*.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*(2016), 119–158.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford Law Books.

PCAST (2014). Executive Office of the President. *Big Data and privacy: A technological perspective*. The White House, Executive Office of the President. The White House.

Raymond, N. A. (2017). Beyond "Do no Harm" and individual consent: Reckoning with the emerging ethical challenges of civil society's use of data. In L. Taylor, L. Floridi & L. van der Sloot (Eds.), *Group privacy – New challenges of data technologies* (pp. 67–83). : Springer.

Taylor, L. (2017). Safety in numbers? Group privacy and Big Data analytics in the developing world. In L. Taylor, L. Floridi, & L. van der Sloot (Eds.), *Group privacy – New challenges of data technologies* (pp. 13–37). Springer.

van den Hoven, J. (1997). *Privacy and the Varieties of Informational Wrongdoing in an Information Age*. Cepe 97.

Van Hoboken, J. (2019). The privacy disconnect. In R. F. Jørgensen (Ed.), *Human Rights in the Age of Platforms* (pp. 255–285). MIT Press.

Vedder, A. H. (1997). Privatization, information technology and privacy: Reconsidering the social responsibilities of private organizations. In G. Moore (Ed.), *Business ethics: Principles and practice* (pp. 215–226). Business Education Publishers.

Watson, H., & Rodrigues, R. (2018). Bringing privacy into the fold: Considerations for the use of social media in crisis management. *Journal of Contingencies and Crisis Management*, *26*, 89–98.

Zuboff, S. (2019). We make them dance. In R. F. Jørgensen (Ed.), *Human Rights in the Age of Platforms* (pp. 3–53). MIT Press.

How to cite this article: Gerdes A. A moderate interpretation of group privacy illustrated by cases from disaster management. *J Contingencies and Crisis Management*. 2020;28:446–452. https://doi.org/10.1111/1468-5973.12336