Paula Helm

Group Privacy in Times of Big Data. A Literature Review

2016

https://doi.org/10.25969/mediarep/1026

Veröffentlichungsversion / published version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Helm, Paula: Group Privacy in Times of Big Data. A Literature Review. In: *Digital Culture & Society*, Jg. 2 (2016), Nr. 2, S. 138–151. DOI: https://doi.org/10.25969/mediarep/1026.

Erstmalig hier erschienen / Initial publication here:
https://doi.org/10.14361/dcs-2016-0209

Group Privacy in Times of Big Data

A Literature Review

Paula Helm[1]

Abstract

New technologies pose new challenges on the protection of privacy and they stimulate new debates on the scope of privacy. Such debates usually concern the individuals' right to control the flow of his or her personal information. The article however discusses new challenges posed by new technologies in terms of their impact on groups and their privacy. Two main challenges are being identified in this regard, both having to do with the formation of groups through the involvement of algorithms and the lack of civil awareness regarding the consequences of this involvement. On the one hand, there is the phenomenon of groups being created on the basis of big data without the members of such groups being aware of having been assigned and being treated as part of a certain group. Here, the challenge concerns the limits of personal law, manifesting with the disability of individuals to address possible violations of their right to privacy since they are not aware of them. On the other hand, commercially driven Websites influence the way in which groups form, grow and communicate when doing this online and they do this in such subtle way, that members oftentimes do not take into account this influence. This is why one could speak of a kind of domination here, which calls for legal regulation. The article presents different approaches addressing and dealing with those two challenges, discussing their strengths and weaknesses. Finally, a conclusion gathers the insights reached by the different approaches discussed and reflects on future challenges for further research on group privacy in times of big data.

Keywords: Group Privacy, Algorithms, Group Theory, Group Rights, Digital Age

1 Paula Helm has submitted her paper on her own initiative.

DOI 10.14361/dcs-2016-0209

Introduction

Technical developments are notorious for stimulating new debates on the boundaries and values of privacy. For instance, the famous claim for a "right to be let alone", formulated by two lawyers in 1890, was triggered by a case of wire-tapping (Warren/Brandeis 1890). With the right to be let alone, Warren/Brandeis aimed at strengthening defence-rights of the individual vis-à-vis the state. More recently, ground-breaking developments in information and communication technology, especially with the application of algorithms that collect and sort massive amounts of data, have given rise to a new wave of privacy concerns. The liberal idea of the individual's right to defence against the state still lies at the heart of these concerns.

However, this idea has been subject to much criticism for being too narrow (Shoeman 1985, Fuchs 2011, Bennet 2011, Cohen 2012, Helm 2016, Seubert/Becker 2016, Sevignani 2016). The critics have been provoked by phenomena such as mass-surveillance, brought about through new technologies and obviously pointing to the social and democratic relevance of data-mining. This clearly brings to light the need for an understanding of privacy-protection as a matter not only of individual choice-making but also social and political responsibility. Big and open data practices hence provoke a shift of focus, thereby also taking collective and social dimensions of privacy into account (Petronio 2002, Regan 2002, boyd 2014, Wolf/Willaert/Pierson 2014, Roberts 2014, Mokrosinska/Rössler 2015, Stahl 2016). Towards a collective conception, some privacy-scholars claim for instance to reach beyond the liberal idea of personal defence vis-à-vis the state by additionally taking into account the ever-increasing need for collective defence against powerful corporations as well (Gusy/Eichenhover/Schulte 2016). In terms of privacy, this concerns corporations who collect and sell massive amounts of data (Rössler 2015: 141–161).

The underlying conviction behind the idea that societies need to be able to defend themselves against the data-processing practices of not only state agencies but also private corporations and the potential cooperation between such power-players is an understanding of privacy as a fundamental resource of democratic societies.[2] Recent shifts in privacy scholarship can be considered as expressions of this conviction. Accordingly, it is necessary to call for a new examination of the group privacy-concept, which in its traditional sense needs to be considered as a mere add-on to individual privacy, thus failing to reflect the collective dimensions at stake. In this article I will review different research on group privacy that has been provoked by big data.

2 In this regard, see for instance the work that is being undertaken by the research project "Transformations of Privacy". ULR: http://www.strukturwandeldesprivaten.de/index_eng.htm

To do so, I will start by briefly sketching out what I suggest calling the traditional notion of group privacy, referring back to a book written by Edward Bloustein in 1978. I will confront this traditional notion with a number of recent publications all pointing at the need for further research on the matter of group privacy in a digital age (2). In the main part of this article, I will proceed by discussing three different approaches to group privacy in the digital age in more detail (3): Linnet Taylor on the ethics of tracking mobility, Allessandro Mantelero on the collective dimension of data protection and Albert Ingold on group rights in the digital age.

All three approaches provide potentially fruitful contributions to a discussion that aims at developing an understanding of group privacy which takes into account groups qua groups, thus overcoming an individual-centric notion of group privacy. I chose to discuss especially those three in more detail, because I found that while all put forward important arguments, they are at the same time lacking crucial aspects in their studies which are – then again – covered by the other approaches discussed here. By reviewing them together, this article aims to show how the three chosen approaches can complement each other in a very fruitful way.

Linnet Taylor's empirical study on mobile tracking in Africa will be discussed first since her insights make very clear the urgency of framing group privacy as a matter of societal and political relevance. Allessandro Montelero, whose research will be discussed next, provides an overview of the field by suggesting possible starting points for a systematic approach to a new concept of group privacy rights. Finally, an article written by Albert Ingold will be reviewed. It presents a very creative and innovative approach to group rights in the digital age, by taking up central problems, which can be considered as blind spots within the other two approaches. However, as we will see, Ingolds' considerations need to be revisited very critically with regard to possible practical consequences that might follow from his theoretical proposals. In the discussion section (4) I will reflect on the question of how far all three approaches present important contributions to the question of group privacy in a digital age. Finally, I will discuss how they could be interlinked in order to develop a concept of group privacy that could do justice to what is at stake in current times, times of big data (5).

Background

The idea of Group Privacy originally goes back to Edward Bloustein, who was the first to argue that an individual right to privacy should become applicable to group contexts. In his book "Individual and Group Privacy" (1978), Bloustein firstly outlines what he understands under the concept of "individual privacy". This he does by referring to Warren & Brandeis's "right to be let alone". Secondly he introduces a right to group privacy, which he describes as the "right to huddle"

(p. 123). I argue that Bloustein's concept needs to be considered as dated, in that it does not suffice to meet the threats posed for groups in the digital age. This is mainly because Bloustein's approach is limited in two regards.

The first concerns Bloustein's attitude towards group rights. In explicitly referring to himself as an individualist who rejects holism, he consequently dismisses the idea of groups having a right qua group and indeed does not even give this option further thought. Instead, when speaking about a right to group privacy, Bloustein is exclusively concerned with the individual's right to privacy. He defines group privacy as a *"form of privacy that people seek in their associations with others. Group Privacy is an attribute of individuals in association with another within a group, rather than an attribute of the group itself."* (p. 124). Bloustein's innovative notion towards group privacy focuses exclusively on the individual deserving privacy protection not only when acting alone but also when acting from within group contexts. However, it does not concern the group itself and in light of this, Bloustein's approach to group privacy is to be considered rather as an add-on to the concept of individual privacy than a discrete concept in its own right. The second reason why Bloustein's traditional notion of group privacy seems to be too narrow can be found in its underlying understanding of privacy. As it concerns only individual defence rights, it needs to be considered as individualistic, blinding out important collective dimensions of privacy.

Since Bloustein's concept of group privacy is based on an individualistic understanding of privacy and since it is narrowed in reducing group rights to individual rights, it fails to face important problems involved with group privacy in the digital age. This is why a new debate on group privacy is urgently needed. In this I follow Luciano Floridi, who has called for an updated understanding of group privacy that overcomes an "atomistic ontology" (Floridi 2015: p. 2). As one step in this direction, Floridi – together with Linnet Taylor and Bart van der Sloot – is working on an anthology of group privacy. His aim is to collect different kinds of research that together reflect the variety of challenges facing group privacy, brought about by new data technologies (Taylor/Floridi/van der Sloot est. 2017). While this volume is still awaited, Floridi already recognises the need for further research on the matter by discussing it in a recent literature review on "the ethics of big data", co-authored with Brent D. Mittelstadt (2015). The idea and concept of the review is not only to provide a narrative of existing literature but also to point at other areas not yet acknowledged but requiring attention. In terms of group privacy, the authors make clear that further research is needed. They identify foreseeable ethical problems arising from big data practices connected to the group-level. In this regard they see in "group privacy rights" a potential measure "that could restrict the flow and acceptable uses of aggregated datasets and profiling" (Mittelstadt/Floridi 2015: p. 327). However, they do not follow this line of thought any further, but instead merely point to its potential.

Mittelstadt/Floridi's drawing on the ethical potential of group privacy rights is concerned with the data-processing practices of powerful entities. It aims at

regulating power-imbalances. Quite differently, Wolf/Willaert/Pierson in their quantitative study to do with group privacy management on SNS unfortunately take into account only the horizontal level – the sharing and withdrawing of information amongst peers. In this paper, I pursue a critical interest by focusing on vertical relations in regard to group privacy – relations of power-imbalances. Despite their differences in perspective, Wolf/Willaert/Pierson nevertheless provide an important argument for the matter I am concerned with, in that their study shows quite clearly that the indicators for group privacy management do indeed differ from the indicators for individual privacy management. With this finding, they add empirical substance to the claim that it is reductionist to limit group privacy to the sum of a number of individual's interests. Hence, they also conclude by arguing, that more research on group privacy is required.

Three Perspectives on Group Privacy in Times of Big Data

Group Privacy and Mass Tracking

Linnet Taylor, with her investigation of mass tracking *(No place to hide? The ethics and analytics of tracking mobility using mobile phone data)* provides an empirical example of the consequences that might follow from a lack of privacy protection for groups in the digital age. In an exploratory case-study she analyses new forms of tracking mobility using mobile phone data in African countries such as the Ivory Coast. Taylor here very impressively addresses the problems that are being created by a one-sided legibility, which evolves when Western aid organisations use the data of African citizens provided by powerful mobile-phone companies. On top of an increased power asymmetry that results, which is already problematic in itself, Taylor finds further problems evolving from a lack of understanding on both sides: the side of the poorly informed data-subjects who are not aware of what happens with their data and the data-interpreters who often misunderstand the information due to a lack of culturally and socially relevant background knowledge.

By referring to an extreme example, which illustrates cases of mutual misunderstanding paired with extreme power imbalances, Taylor shows how individuals can become subjected to discrimination without even noticing that their personal right to privacy has already been violated. With this, she provides an empirical example showing why privacy harm cannot be answered merely by invoking individual rights. Moreover, Taylor also gives examples of cases, where it is not only the algorithmic creation of groups which is problematic due to a lack of protection-rights, but also the tracking of already existing groups such as a tribe. Here, the individual's privacy might be taken care of through anonymisation, but there might be an ethical violation nevertheless because the misinterpretation or biased

interpretation of data about their group can harm group members even when not being identified personally (p. 328). In such cases it is not so much respect for the individual members' privacy which is at stake but respect for the group's privacy as a whole.

Taylor frames the legal and ethical problem we are facing here, by comparing the case with Michel Foucault's critique of catholic confession-practices. In both instances, people are made "legible" in the name of care and protection, but the legibility is one-sided. This is when care turns into control. Often people in Africa use devices produced and programmed in foreign countries, potentially even giving their consent to data storage whilst being unaware of the possible consequences. Since the people being watched are not aware of what is being done with their data, they are not accountable as data subjects and thus not accountable as right holders. Taylor concludes, therefore, that new forms of legibility created through algorithmic tracking make people merely visible to control but yet invisible in terms of agency and rights (p. 331).

Taylor sees one reason for this in an unawareness of group rights when it comes to matters of privacy protection. This lack of awareness justifies keeping it with anonymisation, which refers only to the individual rights dimension of privacy. Another reason that Taylors identifies results from the first one. Since they are only concerned with the rights of the individual, companies which eventually operate the tracking, do not find it necessary to include cultural or sociological background studies on the groups they are aiming at. However, such studies are necessary to avoid misunderstandings and to ensure respect for the cultural properties of the people being made legible.

Case studies such as the one undertaken by Linnet Taylor can very vividly illustrate why thinking of privacy protection only from the perspective of the single individual cannot suffice in the age of big data. However, Taylor unfortunately does not systematise her findings within a more general theoretical framework of group rights, privacy rights, and social theory.

The Collective Dimension of Data Protection

A rather systematic approach including a more comprehensive perspective has been put forward by *Allessandro Mantelero*. In his article titled *"Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection"* he very convincingly argues why so far all takes on group privacy fall short with regard to what he calls "a collective dimension of data-protection", which he sees violated due to the use of big data. Mantelero's key point thereby concerns the same problematic issues to which Taylor has been alluding. He too sees data-subjects' unawareness as right holders and the power imbalance between the trackers and the tracked as the two major problems related to an individualistic take on group privacy. However, Mantelero is not so much concerned with matters of global injustice between rich and poor countries as he is in decrying injus-

tice resulting from unawareness and power imbalances present today within the European Union. To show this, he refers to a range of empirical studies dealing with new forms of groups generated through algorithms. With relation to different examples (Neighborhood Credit Scores, Target Advertising, Price Discrimination, PredPol), he points out how the newly created forms of groups can be a source of unjust discrimination.

After preparing his argument by means of empirical references, Mantelero provides an extensive overview of existing approaches to group privacy, not only referring to Bloustein but also to other related concepts. He classifies the existing takes into three categories: "group privacy", "organizational privacy", and "extension of individual data protection to collective entities". Although he attributes potentials for integrating a collective dimension to the third category, which conceptualises groups as autonomous entities, Mantelero nevertheless concludes that eventually none of the three takes overcomes an atomistic ontology. However, such ontology solves matters of group rights by reducing them to individual rights (Floridi 2014). Doing so, they cannot solve pressing problems related to unawareness and power-imbalances.

A possible answer for this blind spot in privacy theory can be found in the underlying understanding of what characterises a group as such. Mantelero here differentiates between two dominant sociological strands of group theory. The first is called "individualistic theory" (p. 244) in that it defines the group from the perspective of individual members. It is the theory which underlies the traditional concept of group privacy, within which two criteria are relevant: a) stability/consolidation and b) awareness of membership. Both criteria are inapplicable to new types of groups, having been created through the use of digital technologies. On the one hand, there are new types of groups being formed through social networking on the Internet. Such groups are characterised by their low access threshold and hence enjoy a high dynamic in their membership. On the other hand, new types of groups that are being created by algorithms classifying individuals without their being aware of having been made part of a group. Neither type is in line with individualistic group theory.

Mantelero calls the second sociological strand of group theory "organic theory". Here the group is understood as "an autonomous unit that assumes the form of an organized collective entity". Such an understanding is based on the concept of organizational privacy, which provides a better starting point, therefore, when wanting to react to what Mantelero calls a new dimension of protection: the collective dimension of data-protection. In the central section of his article, Mantelero not only describes this new dimension of protection but also points to its democratic relevance. He convincingly argues that safeguarding the collective dimension of data protection is in line with safeguarding the quality of society, since at stake here are the most fundamental values of democracy. To do so, Manteleo once more refers to the concept of "unjust discrimination", this time more systematically than at the beginning of his article. By referring to the example of price

discrimination, he points out how the unjust treatment of different categories of people could be avoided by acknowledging that data protection has a collective dimension which not only refers to individual rights but also to common values. This leads to his drawing parallels between other fields of legal regulation, such as environmental protection. Here the collective representation of common interests (such us equal justice), which cannot be reduced to individual rights, has already found representation in law.

In this regard, Mantelero draws particular attention to the similarities between his claim for a collective concept of data protection and the concept of consumer law. In both fields legal protection refers to the common interest of certain groups of people (users or consumers) but the subjects of the protection have no relationship to each other. However, the difference between both fields is that the potential damages covered by consumer law are often more evident and easier to defend than the damages caused by privacy violation. The latter are usually either of a subtle, ethical nature or difficult to trace back. This difference could hold as an explanation as to why the collective interest in data protection has yet to be recognized, quite unlike consumer or environmental protection.

Finally, Mantelero also thinks about possible solutions on how to exercise a law that reflects the collective interest in data protection. Here he points to the idea of having authorised third parties being responsible for licensing web providers. This idea has already been put forward in terms of individual privacy and personal data protection. Mantelero further suggests extending the risk assessment standards for becoming licensed in regard to the collective dimension of protection. Respective standards should reflect not only the individual interests at stake with privacy but also the collective interests. This requires taking into account ethical and social concerns related to privacy violations. The outcome of a respective extension should be extensive enough, Mantelero concludes, that companies would be encouraged to start working with a broader range of privacy by using design solutions.

With his article on the collective dimension of data protection, Mantelero provides a useful overview of the state of the art regarding group privacy. Not only does he refer to a wide range of empirical studies making visible urgent problems in relation to protection gaps, but he also quite extensively reviews existing privacy concepts dealing with the issue. By doing so, Mantelero also acknowledges the global dimension of data protection in the digital age when turning to both sides of the Atlantic, comparing and relating European and American discourses. Here his focus lies not so much on criticising existing approaches as it does on reviewing them for ideas that might help outlining a common interest-approach to data protection. Even though he identifies a common starting point in the concept of organisational privacy, he nevertheless concludes that so far all existing privacy concepts are suffering from being limited to an individual rights perspective, which cannot suffice to meet the threats posed by big data.

Mantelero locates the roots of their individualistic limitation in their attitude towards groups in general. While there were always people making claims for the irreducibility of a certain quality which can be created by and through social groups (starting with Aristotle's considerations about metaphysics), in the privacy discourse most people reject this idea, maintaining that eventually every group can be reduced to its members. Bloustein, for instance, chose the easy way out of the metaphysical question, simply by taking sides with individualism without further explaining his reasons. However, for Mantelero this cannot be a satisfactory option. He takes a stand contra individualism by stating that "collective data protection concerns collective interests, which are not the mere sum of individual interests" (p. 246). He defines a group, the entity to which such a dimension of data protection applies, as "being characterized by non-aggregative interest" (p. 249).

Indeed, both these statements reject an individualist approach, yet they provide only negations as alternatives (not the mere sum, non-aggregative interests). With this, Mantelero leaves us with more questions than answers. What are collective interests if not aggregative interests? What makes them non-aggregative and how can they be attributed to a group? Without engaging with possible answers to such questions, Mantelero cannot provide a solid argument against common critiques raised by individualists, who claim that collective interests can also be reduced to individual interests. His theoretical approach unfortunately remains underdeveloped in these very central aspects of his claim. The merit, therefore, of what Mantelero himself describes as "an introductory study of a new approach to group privacy" should not so much be searched for in what could be regarded as his own approach as in what is an extremely valuable overview of the most central problems at stake with present day group privacy. Mantelero points us to the most urgent fields of action, one of which is to develop a theoretical basis on which to build a concept of group privacy that is fit to meet the challenges of the digital age.

Group Rights in the Digital Age

Such a basis has been considered by *Albert Ingold*. Even though he is not referring to privacy explicitly, the underlying problem he is concerned with shares common ground with claims for a new approach to group privacy, such as those being put forward by authors like Mantelero, Floridi or Taylor. Ingold is similarly concerned with a lack of protection manifesting in light of new group-phenomenon's being made possible by digital technologies. His theoretical considerations on the matter could be instructive for new approaches to group privacy since he defends an alternative to the individualistic definition of groups. Ingold's major concern in relation to this is to find a model which may also serve to protect such forms of groups legally that are not captured by the traditional definition based on stability

and consolidation. His intention is to define a meaning which better reflects a social reality permeated by digitally mediated communication practices.

In his quest for a model which includes legal protection for new forms of groups, Ingold structures his article in a twofold manner. Firstly, he outlines an alternative definition for groups. Secondly, he runs through different scenarios, seeking the best way to fit such an alternative definition of groups into the framework of German law. Ingold starts by describing his concern from an empirical perspective, considering social phenomena such as *smartmobs*, *flashmobs, facebook-parties* or *hacker-* and *activist-collaborations*. Such collectives are characterised by their dynamic: Their spontaneity, their decentralised structure, by having a low access threshold and thus a high fluctuation of membership. Being featured by such characteristics, they do not fulfill the basic condition of a group as laid down by German law. This condition is to show a certain degree of organisational consolidation.

Even though they do not fulfill the condition, they still deserve to be legally acknowledged as groups and not as mere aggregations of individuals, Ingold claims. To defend his claim, he refers to social theory. He looks at different group theories, especially focusing on those, which move away from taking consolidation as a necessary condition; he instead seeks to define groups from a rather metaphysical perspective. In this way, Ingold manages to pin down the intuition lying behind the negations formulated by Mantelero. Having reviewed a number of standpoints, Ingold concludes that the most adequate theories for this claim are those operating with the concept of "Emergenz" (i. e. Durkheim, Searle, Luhmann). Very roughly, the ontology of *emergence* (direct engl. translation for "Emergenz") could be described as the counterpart to an atomistic ontology. It describes the quality that evolves when the interplay between different elements leads to the creation of new properties. When considered in a social context, one can call such properties emergent if they show a certain kind of coherence. The aggregation of individuals then has developed a quality of its own which is irreducible to its separate parts. This irreducible quality ("Soziale Emergenz") is what differentiates a mere aggregation of individuals from a group.

Most recently the idea of "emergence" has received much attention as it has been made more tangible by a discourse that describes it by invoking the figure of a social swarm. This figure can quite adequately illustrate the special dynamic of technically initiated collective new forms. For instance, it helps to explain why *smartmobs* cannot be reducible to separate contributions. As with a biological swarm, a *smartmob's* smartness is the result of a social dynamic that is being created by a complex nexus of interdependent reactions between individuals, which at some point develops a coherence of its own. The smartness we are dealing with here, therefore, is that of a collectively developed logic rather than that of one person's brain. Along with the new wave of "Emergenz"-theories, by using the social swarm figure to translate an abstract idea into a framework of digital social reality, Ingold proposes to change the definition of groups laid down by German law so

that organisational consolidation as a necessary condition would be replaced by *social emergence* ("Sozialer Emergenz").

On the basis of this proposal, Ingold turns in the second part of his article to the German Constitution. He reviews three different models for integrating new definitions into the existing legal framework. Having dismissed the first two models (re-individualisation, objectification) for readily comprehensible reasons, he turns to the only remaining model. This model demands a reconceptualisation of the legal person. This reconfiguration would necessitate a shift from matters of being and existence towards matters of acting. It would imply changing the perspective from collective being towards collective acting when wanting to establish the criterion for when to acknowledge a collective phenomenon as a group that holds certain rights as a legal person. By integrating such a change to the concept of the legal person, it would be possible to leave aside the criterion of organisational consolidation and instead apply social emergence as a necessary but sufficient condition.

Although it generally proposes a very innovative and simultaneously instructive take on how to make group rights fit for the digital age, Ingold's approach unfortunately suffers from a few blind spots. For instance, when wanting to attribute protection rights to digitally generated groups, one has to take into account the fact that most of these groups communicate via social network sites which are provided by commercial entities. Such entities operate by implementing algorithms that follow commercial logics and which influence communication practices. As well as ignoring the fact that many new forms of groups are for the most part being co-created through such algorithms, even with groups which are the result of people consciously using online platforms to network and solidarise, Ingold fails to reflect that algorithms implemented by third parties are still involved (Wambach/Bräunlich 2016). However, this fact needs to be considered when proposing *social emergence* as sufficient condition for a group to hold a right as legal person because the algorithmic involvement might play a central role in the creation of the very coherence that defines the emergence. It thus seems difficult to decide when to speak of socially created emergence ("Soziale Emergenz") and when to speak of technically created emergence when it comes to digitally mediated groups.

Another blind spot concerns the global dimension of digitalisation. When considering possible ways of integrating his new definition of a group into the German legal framework, Ingold ignores the fact that the groups he is concerned with often act globally and are, therefore, hard to attribute to only one legal system. Despite these blind spots, Ingold's idea of legally laying down a new definition of groups based on a concept of *social emergence* nevertheless holds huge inspirational potential, especially in light of the fact that so far we are lacking an appropriate alternative. It seems more than worthwhile, therefore, to think further about *social emergence* as condition for a group to exist as such, and also in regard to group privacy and algorithms.

Discussion

In light of the different arguments reviewed above, it becomes apparent that more research on group privacy is urgently required. All articles call for an approach to group rights that would be elaborated enough to face the challenges lying in store for us with digitalisation. Referring to new group-phenomena made possible through new technologies, they also make strong cases for why their claims are justified. Yet, they all suffer from limitations when it comes to the question of appropriate ways to meet their claims.

Linnet Taylor, in her article on "the ethics and analytics of tracking mobility using mobile phone data" points out serious dangers resulting from an absence of legal regulation when it comes to matters of mass-tracking. Furthermore, she provides possible causes for the dangers involved when criticising the ignorance of powerful agencies regarding cultural and social peculiarities of the people they are tracking. Unfortunately, though, she does not offer any concrete solutions to the problems she has analysed.

Allessandro Mantelero deals with the question of legal regulation regarding algorithmically created groups in his article on "personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection". Here he provides an overview on what is at stake with the collective dimension of data protection. He introduces us to further research on a new approach to group privacy that encompasses the non-aggregative interests implied with group protection in the digital age. To do so, he leaves behind an individual-rights perspective on group privacy, rejecting an individualistic understanding of groups in general. However, in doing so he gives only short shrift to the central but complex question of what could be implied with non-aggregative interests. He also leaves us in the dark when it comes to the question of what an alternative to the individualist understanding of groups would need to imply. His claim for the collective dimension of data-protection generally suffers from a lack of theoretical foundation, without which it is not fit to challenge an atomistic ontology.

Challenging this very ontology can be considered one of the major merits of *Albert Ingold's* article titled "Grundrechtsschutz sozialer Emergenz" (engl. Acknowledging Social Emergence in German Law, own transl.). Ingold here draws on social theory in order to underpin his argument for extending group rights towards metaphysical collective dimensions. By grounding his jurisprudential argument on swarm and emergence theory, Ingold develops a cogent alternative to the individualistic definition of groups, which currently underlies German case law. His aim thereby is to do justice to the potential protection needs of digitally created collectives, which due to their dynamic fail to be covered by present German group law. However, he does not expatiate what dangers he is more explicitly referring to when indicating a lack of legal protection and he also fails to engage with empirically and normatively relevant factors such as the involve-

ment of algorithms and commercial interests. A more specific reflection of the question as to when an extension of group rights would be justified in the name of fundamental values such as justice and freedom could be accomplished by, for instance, linking Ingold's argument with a discourse that deals with the social dimensions of privacy and the values that are at issue (see for instance Rössler/ Morkosinska 2015).

Conclusion – Towards an interdisciplinary account on group privacy

Reviewing three different approaches on the matter of privacy and groups in times of big data, we can find a number of valuable contributions to an issue which calls for urgent consideration. They include an explorative case study, an overview on related legal and empirical discourses together with an approach to group rights, which would enable the inclusion of new group forms within the legal framework. Missing are interdisciplinary links between the different contributions, without which each approach is lacking crucial integrating arguments necessary in developing a group right to privacy that is up to the challenges posed by digitalisation.

Developing such a right calls for interdisciplinary team work, first and foremost because it needs to be thought of as a reaction to empirically proven protection-gaps related to new kinds of groups. Such gaps are to be identified according to fundamental values, found to have been violated due to a lack of regulation. Secondly, empirically proved gaps should lead to a group theory that serves to de-contextualise and hence systematise characteristics and functional chains related to new kinds of collective action in the digital age. Finally, both the empirical findings and related theoretical conceptualisations need to reflect the fundamental values that western democracies consider to be justifying legal regulation. This reflection should ultimately lead to policy recommendations about when and to what extent the privacy of groups operating with and through the use of digital technologies calls for legal protection.

In light of the above, we can see that in order to develop a comprehensive approach to privacy protection for groups which is fit for adoption by policy makers, a new form of interdisciplinary research is needed. Such interdisciplinary research could be considered radical in that it not only involves sharing information and perspectives but also actually requires working together in teams. Such teams need to include at least three disciplinary perspectives: the perspective of empirically specialised disciplines such as empirical anthropology, information or communication science, the perspective of theoretically specialised disciplines such as political, cultural or social theory as well as the normative perspective of legal scholars and ethicists.

Bibliography

Bennet, Colin (2011): "In defence of privacy: The concept and the regime." In: Surveillance & Society 8/4, pp. 485–496.

Bloustein, Edward J. (1978): Individual and Group Privacy, New Brunswick: Transaction Books.

boyd, danah m. (2014): It's complicated. The social lifes of networked teens, New Haven: Yale University Press.

Cohen, Julie E. (2012): Configuring the Networked Self. Law, Code, and the Play of Everyday Practice, New Haven: Yale University Press.

De Wolf, Ralf/Willaert, Koen/Pierson, Jo (2014): "Managing privacy boundaries together: Exploring individual and group privacy management strategies in Facebook." In: Computers in Human Behavior 35, pp. 444–454.

Floridi, Luciano (2014): "Open Data, Data Protection and Group Privacy." In: Philosophical Technology 27, pp. 1–3.

Fuchs, Christian (2011): "Towards an alternative concept of privacy." In: Journal of Information, Communication and Ethics in Society 9/4, pp. 220–237.

Gusy, Christoph/Eichenhover, Johannes/Schulte, Laura (2016): "e-Privacy – von der Digitalisierung der Kommunikation zur Digitalisierung der Privatsphäre." In: Jahrbuch des öffentlichen Rechts der Gegenwart (JöR) 64, pp. 385–409.

Helm, Paula (2016): "Freiheit durch Anonymität? Privatheitsansprüche, Privatheitsnormen und der Kampf um Anerkennung." In: West-End. Neue Zeitschrift für Sozialforschung 1/2016, pp. 133–144.

Ingold, Albert (2014): "Grundrechtsschutz Sozialer Emergenz. Eine Neukonfiguration juristischer Personalität in Art. 19 Abs. 3 GG angesichts webbasierter Kollektivitätsformen." In: Der Staat 53/2, pp. 193–226.

Mantelero, Alessandro (2016): "Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection." In: Computer Law and Security Review 32/2, pp. 238–255.

Mittelstadt, Brat D./Floridi, Luciano (2015): "The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts." In: Sci Eng Ethics 22/2, pp. 303–41.

Petronio, Sandra (2002): Boundaries of Privacy: Dialectics of Disclosure, Albany, NY: SUNY Press.

Regan, Priscilla M. (2002): "Privacy as a Common Good." In: Information, Communication and Society 5/3, pp. 382–405.

Roberts, Andrew (2014): "A republican account of the value of privacy." In: European Journal of Political Theory 14/3, pp. 320–344.

Rössler, Beate/Mokrosinska, Dorota M. (eds.) (2015): Social Dimensions of Privacy. Interdisciplinary Perspectives, Cambridge: Cambridge University Press.

Rössler, Beate (2015): "Should personal data be a tradable good? On the moral limits of markets in privacy." In: Beate Rössler/Dorota M. Mokrosinska (eds.):

Social Dimensions of Privacy. Interdisciplinary Perspectives, Cambridge: Cambridge University Press, pp. 141–161.
Seubert, Sandra/Becker, Carlos (2016): "Privatheit, kommunikative Freiheit und Demokratie." In: DuD, Datenschutz und Datensicherheit 2/16, pp. 73–78.
Sevignani, Sebastian (2016): Privacy and Capitalism in the Age of Social Media, London: Routledge.
Stahl, Titus (2016): "Indiscriminate mass surveillance and the public sphere." In: Ethics in Information Technology 18, pp. 33–39.
Taylor, Linnet (2015): "No place to hide? The ethics and analytics of tracking mobility using mobile phone data." In: Environment and Planning. Society and Space, doi:10.1177/0263775815608851.
Taylor, Linnet/Floridi, Luciano/van der Sloot, Bart (Eds.): Group privacy: New challenges of data technologies, New York: Springer (forthcoming).
Wambach, Tim/Bräunlich, Katharina (2016): "Retrospective Study of Third-Party Web Tracking." In: Proceedings of the 2nd International Conference on Information Systems Security and Privacy, pp. 138–145.
Warren, Luis/Brandeis, Samuel D. (1890): "The Right to Privacy." In: Harvard Law Rev. 4, p. 193.