
Universiteit
Leiden
The Netherlands

One for all in privacy law: a relational view on privacy based on the ethics of care

Boeken, J.; Sen, J.

Citation
Boeken, J. (2024). One for all in privacy law: a relational view on privacy based on the ethics of care. In J. Sen (Ed.), *Data privacy* (pp. 1-17). IntechOpen. doi:10.5772/intechopen.1006844

Version:	Not Applicable (or Unknown)
License:	Creative Commons CC BY 4.0 license
Downloaded from:	https://hdl.handle.net/1887/4212535

Note: To cite this publication please use the final published version (if applicable).

We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

7,200
Open access books available

192,000
International authors and editors

210M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

14%
Contributors from top 500 universities

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

Chapter

One for All in Privacy Law: A Relational View on Privacy Based on the Ethics of Care

Jasmijn Boeken

Abstract

This chapter proposes a transition from an individualistic conception of privacy to a relational perspective, challenging traditional approaches on two main fronts. First, considering privacy as an individual matter constitutes an unequal playing field when it is balanced against communal rights. Second, information shared by one person can significantly impact others. This chapter highlights research on group and relational privacy but emphasizes a need for a theoretical foundation, proposing care ethics as a normative basis for a relational perspective. Caring privacy should entail the following criteria: (1) minimizing what is known about persons, (2) recognizing persons as embedded in relationships, (3) viewing the private-public distinction as a continuum, (4) no distinction between personal and general data, (5) information is contextual, (6) respecting personal space, and (7) everyone has it. The core contribution of the caring perspective of privacy is that a loss of privacy for one is a privacy loss for all.

Keywords: privacy, ethics, feminism, AI, care ethics, group privacy

1. Introduction

> *There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live – did live, in the assumption that every sound you made was overheard, and except in darkness, every movement scrutinised. ([1], pp. 4-5)*

George Orwell's prophecy in his famous book 1984 did not come to him through a prophetic revelation. Surveillance has been a pervasive practice throughout history, used in times of peace and war, targeting both adversaries and allies. Nevertheless, Orwell accurately perceived that things were changing. In the past, surveillance was labor-intensive and focused on specific individuals, whereas contemporary surveillance consists of large-scale, automated operations, aided by artificial intelligence. Tracking cookies can follow your every step online; in the physical world, as in

London, every dweller is captured by the CCTV [2], and government agencies aspire backdoors into encrypted communications [3]. As privacy has become a pressing topic due to technological advancements, there is an increased scholarly interest in conceptualizing this evolving landscape.

Traditional academic literature on privacy is very extensive and challenging to categorize. To provide some clarity, this chapter divides the work on privacy into three approaches: (1) control over information, (2) the right to be let alone, and (3) the reductionist approach. While the reductionist stance argues that common law adequately protects privacy, the other two perspectives have influenced privacy laws in the United States [4, 5] and the European Union [6]. While novel privacy theories are developed, these traditional theories are still important to discuss due to their influence on privacy and data protection laws. This chapter does not provide an exhaustive overview of privacy literature but rather discusses some of the most influential works in order to challenge the individualistic perspective. While providing distinct views on privacy, what these traditional conceptions have in common is their consideration of privacy as an individual matter [7–10]. This individuality is especially prevalent within the "notice and consent" focus of the GDPR. While the notice and consent paradigm has had a significant share of critique regarding people's ability to understand the complexities of privacy [11, 12], this chapter will mainly focus on the general challenges of treating privacy as a matter of the individual.

This chapter discusses two main challenges for the individual conception of privacy. First, considering privacy as an individual matter constitutes an unequal playing field as it is often balanced against communal rights such as national security [13, 14]. Second, and most important for this chapter, information that one person might consensually give away can have a profound impact on others who did not give such consent [8, 9, 15]. This critique of the individualistic conception of privacy leads to the question of whether privacy as an individual right still fits the current reality of large-scale data collection and its use in AI models. An alternative approach could be to look at privacy as relational instead of individualistic. The question that this chapter will answer is: what might a relational conception of privacy entail? While previous work has been done on the idea of relational privacy and group privacy, these novel conceptions miss the solid theoretical foundation that the traditional conceptions of privacy have within the liberal tradition. This chapter aims to provide a normative foundation of relational privacy by using the ethics of care. The ethics of care is based on a conception of individuals as relational and therefore fits with the evermore networked reality of current society [16].

This chapter will first define assessment criteria for a conception of privacy, followed by discussing the three traditional perspectives and assessing their appropriateness. The subsequent section debates, in more detail than the introduction, why the individualistic view on privacy is problematic. This is followed by an overview of alternative ideas on privacy, such as group privacy and relational privacy. Finally, care ethics is introduced, and a caring approach to privacy is proposed.

2. Individualistic conceptions of privacy

In 1970, Westin observed that it is remarkable that a concept as important as privacy has been so poorly theorized. Since then, a lot of scholarly work on privacy has emerged. This section will set forth four conditions that a conception of privacy

must meet. The preceding sections will discuss the three traditional perspectives on privacy and assess their usability.

Parker [17] suggests that a definition of privacy should meet three criteria: (1) it must fit the data, (2) it must be simple, and (3) it must be applicable in the courtroom. Gavison [18] adds that the concept of privacy should be value-neutral, because otherwise, it would be too difficult to identify a loss of privacy. While agreeing that neutrality is important in defining a concept, I also want to emphasize that absolute neutrality is impossible. The fourth condition that a conception of privacy should meet, therefore, is to endeavor neutrality. Massing this together, a definition of privacy should be fitting, simple, useful, and endeavor neutrality.

The subsequent sections will discuss three different conceptions of privacy and some of the authors that contributed to this broad field of literature. These conceptions will be put against the four criteria that a definition of privacy should meet as described above. What must be considered is that times have changed significantly since many of the definitions below have been developed. While they thus might have met the criteria before, they could fail to do so in the light of new technological developments.

2.1 Control over information

Westin [19] is the most prominent author of the conception of privacy as having control over information, which constitutes the dominant view in current privacy law and aligns with the broader liberal paradigm [6]. This section will discuss the work of Westin and scholars influenced by Westin. Following this exploration, the applicability of the four criteria for a definition of privacy will be assessed.

Westin famously described privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." ([19], p. 7). The key element in this conception of privacy is thus the control that people have over information, not only including things like wiretapping but also, for example, personality tests, and thereby it protects the privacy of inner thoughts [19]. The notice and consent paradigm within the GDPR is based on the idea of having control over information [6]. In every step, the consumer gets the option to agree or disagree with the privacy policies and is therefore able to exercise control. Building on this idea of privacy as control, other authors argue to shift focus from control to meaningful choice, which includes the ability of people to make decisions [6, 20]. Companies that incentivize consumers to share information about themselves do not contribute to this ability. This adapted version of Westin's definition thus conceptualizes privacy as not only having control but also having the necessary tools to control personal information.

Parker [17], focusing mainly on the physical realm, defines privacy as control over when and by whom the various parts of us can be sensed. By "sensed," Parker means: "seen, heard, touched, smelled, or tasted" ([17], p. 281). While this definition does not account for the disclosure of personal information, one's thoughts, and psychological state of mind due to its strong focus on the physical [17], it does provide an important insight, as privacy could indeed be a very physical thing. Someone watching you or sitting closely to you so they can smell you is, according to Parker, a violation of privacy.

Nissenbaum's [21] explanation of privacy as contextual integrity is also related to Westin's view of privacy as controlling information, as it is phrased in similar terminology [22]. According to Nissenbaum [21], what constitutes adequate protection

of privacy depends on the norms of the context you are in. Nissenbaum's theory is inspired by Walzer's work on spheres of justice. While it might not be an invasion of privacy to provide your doctor with your medical history, when this information is taken outside the medical sphere and provided to your boss in the sphere of labor, it becomes a privacy violation. This focus on privacy as contextual is an important contribution to the academic debate. However, Nissenbaum's work also received critique, as norms are not always easily identified and might quickly change [23].

While acknowledging the distinctions, proponents of the conception of privacy as control identify a loss of privacy as a loss of control, which is the basis of current privacy law. This is also what constitutes the main critique—one also loses privacy when voluntarily sharing information, however, the question is whether this is bad or not [18]. This underscores how this definition of privacy does not meet the criteria of neutrality. Moreover, the relationality of data renders the focus on individuals problematic, as controlling information in the current technological reality is impossible [24–26]. Consequently, while providing important insights, this definition does not fit the data.

2.2 The right to be let alone

This section describes privacy as the right to be let alone, which has its foundations in privacy law in the United States [4]. It will first introduce the work of those some consider the most important authors in the field of privacy: Warren and Brandeis [27]. After delving into their theory, the conception of privacy by Gavison [18] will be discussed, which builds on this idea of privacy as being let alone. This is followed by a discussion based on the four criteria as previously outlined.

Warren and Brandeis [27] contended that the advent of technological innovations in photography and printed newspapers necessitated the formal recognition of the right to privacy. This right to privacy as being let alone was envisioned to protect individuals from having their picture taken without consent or having their private life exposed in the newspaper [27]. Warren and Brandeis define the right to privacy in the following way: "In general, then, the matters of which the publication should be repressed may be described as those which concern the private life, habits, acts, and relations of an individual" ([27], p. 216). In essence, privacy as the right to be let alone thus means that no one should have unauthorized access to you when you are in the private sphere.

Gavison [18] critiques the conception of privacy as proposed by Warren and Brandeis, arguing that their definition of privacy as a negative right, where the government is prohibited to spy on its citizens, falls short. The right to privacy, Gavison contends, should encompass both negative and positive rights, emphasizing the state's duty to protect its citizens against intrusion by other citizens or companies [18]. Proposing an alternative conceptualization, Gavison suggests framing privacy as limited access, containing three core elements: secrecy, anonymity, and access. Secrecy pertains to information known about a person, anonymity is compromised when someone pays attention to you, and access means physical proximity. Gavison thus elevates the concept of privacy as the right to be let alone to a more detailed conception of privacy as limited access.

Whereas the definition as posed by Warren and Brandeis [27] has received substantial criticism for being both too narrow [28] and too broad [29], Gavison [18] gives the conception of privacy as being let alone more substance. Gavison's conception is simple and useful and seems to withhold from giving a normative evaluation.

However, it is a highly individualized view on privacy and does not recognize that when a person is being watched, this might not only affect this one person but could also reveal information about those in proximity or those belonging to the same group, it therefore does not meet the criteria of fitting the data. Gavison's argument that privacy is also a positive right, as well as the attention for secrecy, anonymity, and access, however, should be considered important insights.

2.3 Reductionist approach

The final traditional conception of privacy to discuss is the reductionist approach. The reductionist approach is based on a critique against the other conceptions of privacy as described in the previous sections. What is central to this approach is that the authors contend that we do not need new laws to protect privacy, as it is sufficiently protected within common law.

Thomson emerges as an important critic of the conception of privacy as the right to be let alone, asking: "where is this to end? Is every violation of a right a violation of the right to privacy?" ([28], p. 295). Thomson contends that when a right to privacy seems to be violated, some other rights have been violated as well. For instance, when security agencies spy on a married couple having a quiet fight inside their home, their right to privacy has not been violated, but their right over the person has been violated, which includes the right not to be listened to [28]. Similarly, Posner [30] takes an economic approach, arguing that while privacy can be useful for innovation, further protection will not be fruitful. According to these authors, privacy is thus sufficiently protected within common law.

Gavison [18] criticizes this reductionist approach to privacy, arguing that while other rights might simultaneously be harmed when a loss of privacy occurs, the loss of privacy remains important in itself. The plead made by the reductionist theorists leaves the doors wide open to dismiss any claim of a right to privacy. As Fried [31] notes, this work is inspired by scholars like Friedrich Hayek and Robert Nozick who maintain a hierarchy of rights where privacy is less important than other rights. Furthermore, the fast development of the digital world has changed the issues of privacy significantly, rendering it highly questionable whether the common law would still suffice in protecting it. As the reductionist approach, thus does not really propose a conception of privacy as they argue that this is not necessary, it is not entirely possible to assess it on the four criteria a definition should meet. However, there are indications that this approach does not endeavor neutrality and is a misfit with the data.

3. Challenging individualistic conceptions of privacy

Studying the traditional conceptions of privacy reveals that it is a contested concept. While the three discussed approaches highlight vastly different aspects of privacy, a common thread among them is the perspective of persons as individual atoms [7, 8]. This individualistic viewpoint is not only prevalent within academic literature, it is also the dominant perspective within EU and US privacy laws [5, 32, 33]. This section aims to scrutinize the individualistic perspective on privacy and assert its problematic nature. This entails reflecting on two issues as established in the introduction: individual versus communitarian rights and the fast development of aggregated data and the use of AI technologies.

The individualistic perspective on privacy renders it vulnerable to a communitarian critique, particularly as outlined by Etzioni [34], who argues that the individual right to privacy often takes precedent over the common good while it should instead be balanced. While this statement is contested by Cohen [13] who observes that privacy is often on the losing side of this balancing game, let us discuss Etzioni's argument shortly. Two important cases that Etzioni takes as example are those of testing infants for HIV, where the mother's privacy is put against public health, and the case of registering sex offenders, where the privacy of the offender is put against public safety. Etzioni, in these cases, argues that the common good should take precedence over the individual's right to privacy. While Etzioni's work is a highly valuable contribution to the discussion on privacy, I want to contest the idea of balancing privacy as an individual right against the common good. One possible solution might be to see privacy as important for the common good, while my analysis is not broad enough to argue it would change the outcomes of the two cases, what it would surely do is create an equal playing field. Other authors have also argued in this direction, for example, in favor of seeing privacy as an (aggregate) public good [5, 32], or as a collective value [35, 36]. Both Sætra's [5] and Regan's [36] argument is based on the idea that the privacy decisions of one person influences the privacy of others.

The idea that privacy decisions of one person have an effect that transcends beyond the individual is strengthened by the technological advancements of AI and data aggregation. The second vulnerability of the individualistic view on privacy is thus that it is no longer in line with our technological reality [33]. Especially the harvesting of data on an enormous scale poses a significant challenge to conceptualizing privacy as a matter of the individual [8, 9, 15, 32, 33, 37]. An example of consequences of the rapid harvesting and accumulation of data can be found in new AI models, which show how privacy is no longer an individual decision [33]. For AI, our data is not about an individual, but rather it categorizes us in groups; you can belong to numerous groups based on your gender, sexuality, occupation, age, race, and many more [8]. Whenever you accept tracking cookies, this thus does not only reveal something about you, it reveals something about the groups you belong to, and every person in them. Barocas and Nissenbaum [15] call this the "tyranny of the minority" as few people consenting to a privacy loss affect the privacy of everyone else. Or in other words: "*everyone's privacy depends on what others do.*" ([38], p. 558). Barocas and levy [38] explore the concept of privacy dependencies, which can be tie-based, where an observer gains information of someone because the ties they have with someone else. They can also be similarity-based or difference-based, where due to similarities or differences in known attributes, other information can be inferred [38].

In their study, Barocas and Nissenbaum [15] provide multiple examples on how the tyranny of the minority works, which also shows the relationality of data. Jernigan and Mistree [39] show how sexual orientation can be inferred from Facebook profiles, and a study on Rice University alumni reveals that sharing personal details by only 20% of a group allows accurate inference of over 80% [40]. Furthermore, Duhigg's [41] research on Target's advertising strategy demonstrates how a fraction of pregnant women disclosing information affects all pregnant individuals shopping there, in one case leading to the unintended consequence of revealing a teen pregnancy to family members. These examples emphasize that privacy is not solely an individual matter, and the introduction of sophisticated AI systems using aggregated data will ever more correctly infer information about individuals that did not give consent [23]. What makes aggregated data even more problematic is that data accumulates across time

and across different sources [32]. The younger the child that enters the internet, the more data will be collected of them over a lifetime.

This section argued that seeing privacy as individualistic creates an unequal playing field when it is balanced against the common good, and that it no longer fits with our technological reality. The issue of tyranny of minority [15] shows how the decisions of an individual regarding their privacy have a profound impact on everyone's privacy. The next section will discuss an alternative way of viewing privacy, transforming it from individualistic to relational.

4. Group privacy

One form of privacy which does not only consider the individual is group privacy [9]. While the GDPR does not mention group privacy [8], it has been mentioned in academic literature and surprisingly even in the famous work of Westin [19]. The more recent work that this section discusses considers group privacy especially due to AI's capability to categorize data subjects into groups, based on our characteristics, like age or nationality, or behavior.

In the renowned work on privacy as control over information, Westin [19] acknowledges the need for group privacy in society. Specifically mentioning the intimate family and the community as important groups. To illustrate this point, Westin proposes that communities might have certain traditions which they would like to keep a private matter of the group. A recurring example in Westin's work regards the idea that personality tests may inadvertently lead to a standard personality based on the white men, potentially disadvantaging minority groups. While Westin offers valuable insights into the significance of privacy for groups, this regrettably does not lead to a broader conception of privacy.

Substantial early work on the topic of group privacy was done by Bloustein [42], who does not consider it as an alternative to individualistic privacy but rather as additional to the right to be let alone: "The right to be let alone protects the integrity and the dignity of the individual. The right to associate with others in confidence – the right of privacy in one's associations – assures the success and integrity of the group purpose." ([42], p. 181). Bloustein sees the group as a collection of individuals, not as a separate entity and discusses examples like the lawyer-client relationship where information is shared that should be kept private. In line with this, Bygrave and Schartum [43] consider the option of collective consent, where established groups can control their consent to data collection in a more organized way.

Further important work on group privacy is done by Floridi [9], who argues that in the digital realm, people are often not considered as individuals but as members of a group—regnant women, people living in Amsterdam, parents, or owners of a particular car. While group data has often been said to be anonymous, accumulating such data can lead back to an individual, as you are part of many groups [9, 15, 33, 44]. Anonymization of data thus is no guarantee for privacy. This leads Floridi to argue that "An ethics addressing each of us as if we were all special Moby-Dicks may be flattering and perhaps, in other respects, not entirely mistaken, but needs to be urgently upgraded. Sometimes the only way to protect a person is to protect the group to which that person belongs." ([9], p. 20).

Influenced by the work of Floridi, Mittelstadt [44] discusses the impact of AI, which creates groups that have no collective identity or agency, providing a complicated legal question on how to protect such group rights. A possible solution according to Mittelstadt

is to think of these groups as rightsholders, carrying a moral right to privacy. As these rightsholders cannot be responsible for protecting their own privacy, this should be the task of an organization. Similarly looking into the direction of external organizations for the protection of group privacy, Mantelero [35] suggests this could be done by data protection agencies. This would entail collective data protection by means of risk assessment methods, involving multiple stakeholders to balance the benefit of data collection against the collective data protection rights of groups [35].

Similarly, Loi and Christen [45] worry about AI assembled groups that have no agency. They propose "inferential privacy" to protect us from the inferences made by predictive analytics. Important to mention is that they acknowledge that such predictive analytics can be significantly beneficial for society, as for example showed by the research on increased risk of cancer after smoking [45]. While acknowledging the risks of predictive analytics for privacy, we must not lose sight of the benefits for society. Related to the logic of inferential privacy, Mühlhoff [33] discusses predictive privacy as a concept relevant for protecting both individual and group privacy. Mühlhoff suggests that predictive privacy could protect the community against predictive analytics that could potentially harm society. To effectively reach the goal of predictive privacy, Mühlhoff contends that we need to depart from the liberalist ethics of individualism. Puri [46] argues that privacy exists at multiple levels, both individual as well as of the group. Going further than the discussion on inferential privacy, which focuses on the inferences made by predictive analytics, Puri argues that the process of algorithmic grouping itself is a violation of privacy.

Whereas the view on group privacy as provided by Westin [19], Bloustein [42], and Bygrave and Schartum [43] still holds a very individualistic view of the person. Later work provides a view that is a better fit with current technological reality. Whereas the novel work on group privacy thus overcomes the critique of traditional perspectives of privacy as they do not fit the data, they might be missing the foundation in normative theories that the theories of Westin and Warren and Brandeis have. The individualistic views on privacy are strongly established within liberal theory, providing a solid foundation [6]. Such a foundation in theory would be a valuable contribution to the work of group privacy [46]. Furthermore, the number of groups one is part of is difficult to grasp and is not a static fact [35]. While the work on group privacy thus made valuable contributions to the privacy debate, the static idea of groups might be holding it back. Overcoming this challenge, the subsequent section will discuss relational privacy.

5. Relational privacy

The preceding sections have established that traditional Western views on privacy are based on the individual as atomic entity. While group privacy provides an alternative view, it does not explicitly break with the Western liberal tradition of individuality. Opposed to this Western tradition, cultures such as Indian, Japanese, Buddhist, and Confucian have been posited to adopt a more relational conception of privacy [8]. While the previous sections criticized the individualistic view on privacy in the traditional conceptions, according to Kerr [47] such conceptions already have an implicit relationality in them as they do focus on "the other". However, an explicit view on relational privacy remains necessary. This section will discuss the work that has been done on conceptualizing privacy in a relational way. While not much scholarly work has been devoted to this topic, noteworthy suggestions have been made.

The term "relational privacy" has been used in multiple ways. For example, Sacharoff [48] uses the term to explain that our expectation of privacy is depended on the type of relationship we have. While we do not mind sharing information about our body with our physician, we do mind sharing such information with our boss. Thus, because we make distinctions in what information we share with someone based on the relationship we have with them, Sacharoff considers privacy to be relational. In line with this, Sloan and Warner [49] use relational privacy to describe how we navigate sharing information within different relationships. This must remind us strongly of privacy as contextual integrity from the work of Nissenbaum [21] and is thus susceptible to the same criticism—it is still an individualistic view of privacy. While recognizing the importance of relationships, these conceptions are centered around the individual and thus are not in line with the type of relational privacy this chapter is looking for.

An example of a relational approach to privacy that truly moves away from the individualistic perspective can be found in Ubuntu philosophy, which originates from multiple countries within the African continent [8]. A phrase that is central to Ubuntu philosophy is "Umuntu ngumuntu ngabantu" which can be translated to "a person is a person through other persons." ([8], p. 595). This relational view of the person leads to the conclusion that the protection of privacy should not be up to individuals but should be regulated top-down. This also entails stopping using legal frameworks for privacy that are built on the idea of informed consent [8].

Ma [7] argues for relational privacy based on the ideas from Confucianism, and connects this to views from Western feminist ethics. While there are many different perspectives within Confucianism, the person is generally constituted as situated within a specific environment [7]. The relational perspective on privacy in Confucianism is based on a relational perspective of autonomy [7]. Relational autonomy conceives of autonomy as something that can be learned, a skill that you develop, and this development happens in context of relationships [7]. While Ma does not suggest how privacy law should be established according to this view, the research shows that outside of the Western world there are more relational views on privacy.

A relational view on autonomy can also be found within feminist work, which holds that autonomy is something that can be achieved when social circumstances are supportive of it [50]. Applying such a view of autonomy to privacy, Hargraeves [50] argues that relational privacy should be seen as a "privacy blanket". With such a privacy blanket, privacy can be shared, in the sense that someone can join you under the blanket. Privacy is mobile, it can move from one place to another, leaving behind the strict dichotomy of the private and public spheres. And privacy can be weakened or strengthened [50]. A loss of privacy, in this way, occurs when "our ability to negotiate our level of exposure to or desired level of engagement with those around us" ([50], p. 476) is affected.

Although not being explicitly relational, the work of Marwick and Boyd [10] goes beyond the individual and the group to provide a networked definition of privacy. Studying the privacy experiences of teenagers, they argue that we should see privacy as constituted within relationships and networks [10]. This is a valuable insight that should be elaborated upon, and the focus on relationships will be further discussed in the subsequent section of care ethics as we further shift from an atomic view of the individual toward a relational view.

Whereas the traditional work on privacy as discussed in Section 2 contained the main issue of not fitting the data, a growing body of scholarly work in the fields of group privacy and relational privacy is especially focused on fitting the data.

However, while having its roots in reality and being applicable to novel challenges posed by AI, what these theories lack is a normative basis. This is necessary when it comes to questions of how much privacy there *should* be and when privacy loss is considered *harmful*. The ethics of care is proposed to provide a normative basis for a relational view on privacy [8] and will be discussed in the preceding section.

6. Care ethics

As suggested by the authors on Ubuntu [8] and Confucian [7] ideas on relational privacy, the feminist tradition with its view on the relational person could provide a valuable contribution to the idea of relational privacy. This section will first discuss the complicated relationship between feminism and privacy before introducing the ethics of care and especially its ideas regarding the distinction between the private and public sphere and the relational nature of the person. The goal of this section is to show how the ethics of care could be a useful theoretical foundation for a caring perspective on relational privacy.

Using a feminist theory for a new conception of privacy is an interesting undertaking, as the feminist tradition has been an important critic of the right to privacy [20, 26, 51, 52]. According to early feminist scholarly work, the right to privacy and the division of the public and private sphere have served as legitimization for the oppression of women inside their homes [20, 26, 52]. This resulted in the famous phrase "the personal is political." According to Allen and Mack [53], traditional conceptions of privacy were developed from a position of privilege, ignoring women's perspective on privacy. However, privacy has also been a partner for the feminist tradition, as the right to abortion in the United States relates to the right to privacy [20, 53, 54]. Feminist ethics thus provides a valuable and multifaceted approach to the topic of privacy.

The feminist perspective that this chapter discusses is the ethics of care [55]. Combining the central features of care ethics that Held [56] and Preston and Wickson [57] point out, the five most important features of an ethics of care are that: (1) it recognizes care as a moral value; (2) it values emotions; (3) it considers context; (4) it reconceptualizes the public and private sphere; and (5) it has a relational conception of the person. While all these aspects can provide interesting insights for privacy, this section will limit the discussion to the final two. This will show the great potential of using ethics of care in the debate on privacy, while leaving the details up to future research.

Regarding the distinction between the public and the private sphere, feminist ethics in general and care ethics specifically have had different, but complementary, perspectives. Whereas early feminists argued that the law should be introduced in the domain of the private sphere, the home, care ethics posits that relational care inherent in the private sphere should transcend into the public sphere [58]. In other feminist work, the distinction between the private and public sphere is altogether questioned [16, 50, 53, 59]. Given the evolving technological landscape, it is indeed questionable whether the distinction of spheres is still relevant, as products of firms in the public sphere invade our private homes. The work of Ford [60] provides a valuable contribution as it argues that rather than a dichotomy, the private and public should be seen as a continuum, with private on the one end and public on the other. Whereas this is a good solution to the issue of the public/private divide for now, future work should question whether a divide is necessary altogether or whether the idea of different spheres could be abandoned.

The relational conception of the person as described in care ethics is especially interesting for the relational conception of privacy this chapter is exploring. Care ethics sees the relationships we have with others as what defines us; the caring person is a relational self: "Noticing interdependencies, rather than thinking only or largely in terms of independent individuals and their individual circumstances is one of the central aspects of an ethics of care." ([56], p. 53). A person is not conceived of as a single unit, an atom, but as a being that is embedded within relationships with others [16]. As we are thus embedded within relationships, so is information about us, and so is privacy.

This section discussed the ethics of care as a possible theoretical foundation for a caring, relational conception of privacy. The first key takeaway is that caring for privacy can be applicable to both the private and the public sphere in different degrees, as they constitute a continuum rather than a dichotomy. The second is that we should not see individuals as singular atoms but as constituted within a network of relationships.

7. A caring definition of privacy

This section will propose a caring perspective on privacy, drawing upon all the takeaways from the previous sections. Privacy has been defined in different ways: as a right [27] or as a claim [19], but to make its definition more neutral, I will describe it here as a situation. A situation of privacy can thus be a good thing or a bad thing; sometimes it is necessary to lose some privacy, and sometimes losing privacy is harmful. This section makes a first suggestion of how caring privacy could look like, based on the ethics of care and on all the valuable insights of previous work on privacy.

To have a situation of caring for privacy, the following conditions should be in place:

- What is known about persons is minimized;
- We see persons as embedded in relationships;
- The private and public spheres are seen as a continuum rather than a dichotomy;
- There is no distinction between personal data and general data;
- Information is considered to be contextual;
- Personal space is respected;
- And, everyone has it.

While the first point may come as a surprise, a situation of privacy is not a situation of full seclusion, when nothing is known about a person. It is a situation where what is known is limited to what is strictly necessary for the particular relationship. This relates to the second point, which is that we consider people to be relational; they are not singular atoms; they are networked within relationships. Furthermore, the distinction between the public and private spheres is rephrased, and the distinction between personal data and general data is no longer recognized, as all information

can be inferred from aggregating data [23, 33, 61]. Furthermore, as Nissenbaum [21] argued, information is contextual; while sharing certain information in a specific situation may not be a harmful loss of privacy, when this information is taken out of context, the loss might be harmful. Inspired by Gavison's [18] insightful remarks on access and proximity, respect for personal space is also part of a situation of privacy. The final and most important point is that a situation of privacy can only exist as long as everyone has it: a privacy loss for one is a privacy loss for all.

Returning to the criteria a definition of privacy should meet as described in section two, it should be fitting, simple, useful, and endeavor neutrality. Whereas the conceptions of privacy as discussed in Section 2 were problematic in the sense that they did not fit the data, the caring definition of privacy solves this issue by approaching it from a relational perspective. The definition is as simple as possible regarding the difficulty of the topic. It is useful due to its clear imperative that privacy should not be an individual decision but governmental. It endeavors neutrality because to have privacy can be good or bad, and to have a loss of privacy can also be good or bad. It is up to the political community to decide when a loss of privacy is harmful. The caring definition of privacy should be all-encompassing, not only considering informational privacy but also decisional- and physical privacy. While this chapter only slightly lifts the veil of what a caring perspective of privacy has to offer, it clearly shows its potential.

8. Conclusion

> *"We can achieve a sort of control under which the controlled, though they are following a code much more scrupulously than was ever the case under the old system, nevertheless feel free. They are doing what they want to do, not what they are forced to do. That's the source of the tremendous power of positive reinforcement – there's no restraint and no revolt. By a careful cultural design, we control not the final behavior, but the inclination to behave – the motives, the desires, the wishes." ([62], pp. 246-247)*

As many other authors, I started my chapter with a quote from Owell's dystopian book *1984.* However, after the findings of this chapter, it seemed more appropriate to finish with a quote from Skinner's [62] *Walden Two,* where, while having a lot of personal freedom in decision-making, the behavior of the people in this imagined society is slowly modified. While the conceptions of privacy that see it as a personal right were great answers to the threat, as described by Orwell, of a government spying on its people, the situation as described by Skinner provides alternative challenges. These challenges are all too real in our current world, where accumulated data can be used for predicting and influencing consumers behavior or political opinions. Our current technological reality of accumulated data collection and the use of it in AI challenges the conceptions of privacy based on an individualistic perspective and calls for novel approaches to privacy.

This chapter shows how the traditional perspectives on privacy contain an individualistic approach. This individualistic perspective on privacy has also been the dominant paradigm within EU and US privacy law. As well as in the GDPR's focus on notice and consent. This chapter challenges the individual conception of privacy based on two arguments. First, considering privacy as an individual matter constitutes an

unequal playing field as it is often balanced against communal rights such as national security. Second, and most important for this chapter, information that one person might consensually give away can have a profound impact on others that did not give such consent. The current paradigm on treating privacy as control over information is thus lacking and is construing a dangerous process of desensitization of societies' value for privacy [24]; a different conceptualization of privacy is therefore urgent.

To provide a first glimpse of what an alternative perspective on privacy could entail, this chapter used the ethics of care as a theoretical basis. While not providing a final definition of caring privacy, this chapter suggests that a situation of caring privacy should entail the following criteria: (1) what is known about persons is minimized; (2) we see persons as embedded in relationships; (3) the private and public spheres are seen as a continuum; (4) there is no distinction between personal data and general data; (5) information is considered to be contextual; (6) personal space is respected; and (7) everyone has it. While not downplaying the other points, the most important contribution of the caring perspective of privacy is that when there is a loss of privacy for one, this affects the privacy of all. Furthermore, while a loss of privacy for one might not be harmful, as sharing information strengthens a particular relationship, it may end up being harmful for others, as the data could be used in predictive models.

What this entails for privacy legislation is that the basis of privacy protection should not be consent of the individual. The government should have an increased role in protecting citizens' privacy. While some might suggest that to give governments this increased power would be undemocratic, I would argue the opposite. As the example of Target [41] showed, within current privacy law, a small group can impact the privacy of all, which is profoundly undemocratic. Governments must change their individualistic perspectives on privacy even though this might in some sense reduce freedom of choice: "People's liberty to dismiss their own privacy is not reduced in order to protect themselves, but in order to prevent them from inflicting harm on others." ([5], p. 8).

As this is a preliminary exploration of combining the ethics of care with the concept of privacy, several topics remain deserving of more attention. These include, but are not limited to; the division between the private and public spheres, the role of emotions in privacy, and the question of what future technological developments could mean for the conception of privacy. Furthermore, the suggestion made by Dourish and Anderson [63] to combine the concepts of privacy and security should be further studied by applying care ethics. Additionally, future scholarly work should further study the ideas on privacy in non-Western philosophy. As this study highlights the valuable ideas from Ubuntu philosophy and Confucianism, there is a lot of work that Western researchers might be overlooking by primarily focusing on Western intellectual heritage.

The right to privacy has been significantly challenged by emerging technologies, and given the early stages of large AI language models at the time of writing, the future might bring even more severe challenges to privacy. Proposing a caring approach to the idea of relational privacy might not seem like a straightforward solution. However, since the individualistic paradigm has reached its expiration date, there is a need for innovative ways of approaching privacy. A caring approach to privacy can overcome the challenges of the individualistic paradigm and provide a solution that fits the data. The future is relational, as a privacy loss for one is a privacy loss for all.

Acknowledgements

This work was funded by NWO (the Dutch Research Council) (grant number NWA.1215.18.008) and is part of the Dutch Research Agenda 2018: *Cyber security – towards a secure and reliable digital domain*.

IntechOpen

Author details

Jasmijn Boeken[1,2]

1 Institute of Security and Global Affairs (ISGA), Leiden University, The Hague, The Netherlands

2 Centre of Expertise Cyber Security, The Hague University of Applied Sciences, The Hague, The Netherlands

*Address all correspondence to: j.boeken@fgga.leidenuniv.nl

IntechOpen

© 2024 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] Orwell G. George Orwell 1984. London, UK: Penguin Classics; 2008

[2] Ellis MS. Losing our right to privacy: How far is too far. Birkbeck Law Review. 2014;**2**:173

[3] Lear S. The fight over encryption: Reasons why congress must block the government from compelling technology companies to create backdoors into their devices. Cleveland State Law Review. 2017;**66**:443

[4] Kramer IR. The birth of privacy law: A century since Warren and Brandeis. Catholic University Law Review. 1989;**39**:703

[5] Sætra HS. Privacy as an aggregate public good. Technology in Society. 2020;**63**:101422

[6] Austin LM. Re-reading Westin. Theoretical Inquiries in Law. 2019;**20**:53-81

[7] Ma Y. Relational privacy: Where the east and the west could meet. Proceedings of the Association for Information Science and Technology. 2019;**56**:196-205

[8] Reviglio U, Alunge R. "I am datafied because we are datafied": An Ubuntu perspective on (relational) privacy. Philosophy & Technology. 2020;**33**:595-612

[9] Floridi L. Group privacy: A defence and an interpretation. In: Group Privacy: New Challenges of Data Technologies. Cham: Springer International Publishing AG; 2017. pp. 83-100

[10] Marwick AE, Boyd D. Networked privacy: How teenagers negotiate context in social media. New Media & Society. 2014;**16**:1051-1067

[11] Kröger JL, Lutz OH-M, Ullrich S. The myth of individual control: Mapping the limitations of privacy self-management. 7 Jul 2021. Available at SSRN 3881776

[12] Solove DJ. Introduction: Privacy self-management and the consent dilemma. Harvard Law Review. 2013;**126**:1880-1903

[13] Cohen JE. What privacy is for. Harvard Law Review. 2012;**126**:1904

[14] Mell P. Big brother at the door: Balancing national security with privacy under the USA PATRIOT act. Denver Law Review. 2002;**80**:375

[15] Barocas S, Nissenbaum H. Big data's end run around anonymity and consent. In: Privacy, Big Data, and the Public Good: Frameworks for Engagement. Vol. 1. New York, NY: Cambridge University Press; 2014. pp. 44-75

[16] Sevenhuijsen S. Citizenship and the Ethics of Care: Feminist Considerations on Justice, Morality and Politics. London: Routledge; 2003

[17] Parker RB. A definition of privacy. Rutgers Law Review. 1973;**27**:275

[18] Gavison R. Privacy and the limits of law. The Yale Law Journal. 1980;**89**:421-471

[19] Westin AF. Privacy and Freedom. New York: Atheneum; 1967

[20] Allen AL. Coercing privacy. William & Mary Law Rev. 1998;**40**:723

[21] Nissenbaum H. Privacy as contextual integrity. Washington Law Review. 2004;**79**:119

[22] Nissenbaum H. Protecting privacy in an information age: The problem

of privacy in public. In: The Ethics of Information Technologies. London: Routledge; 2020. pp. 141-178

[23] Skeba P, Baumer EP. Informational friction as a lens for studying algorithmic aspects of privacy. Proceedings of the ACM on Human-Computer Interaction. 2020;**4**:1-22

[24] Sloan RH, Warner R. Beyond notice and choice: Privacy, norms, and consent. Journal of High Technology Law. 2014;**14**:370

[25] Solove DJ. Conceptualizing privacy. California Law Review. 2002;**90**:1087-1155

[26] Suárez-Gonzalo S. Personal data are political. A feminist view on privacy and big data. Recerca: Revista de pensament i anàlisi. 2019;**24**(2):173-192

[27] Warren SD, Brandeis LD. The right to privacy. Harvard Law Review. 1890;**4**:193-220

[28] Thomson JJ. The right to privacy. Philosophy & Public Affairs. 1975;**4**:295-314

[29] Allen AL. Uneasy Access: Privacy for Women in a Free Society. Totowa, NJ: Rowman & Littlefield; 1988

[30] Posner RA. Privacy, secrecy, and reputation. Buffalo Law Review. 1978;**28**:1

[31] Fried C. Privacy: Economics and ethics: A comment on Posner. Georgia Law Review. 1977;**12**:423

[32] Fairfield JA, Engel C. Privacy as a public good. Duke Law Journal. 2015;**65**:385

[33] Mühlhoff R. Predictive privacy: Collective data protection in the context of artificial intelligence and big data. Big Data & Society. 2023;**10**:20539517231166886

[34] Etzioni A. The Limits of Privacy. New York: Basic Books; 1999

[35] Mantelero A. From group privacy to collective privacy: Towards a new dimension of privacy and data protection in the big data era. In: Group Privacy: New Challenges of Data Technologies. Cham: Springer International Publishing AG; 2017. pp. 139-158

[36] Regan PM. Privacy and the common good: Revisited. In: Social Dimensions of Privacy: Interdisciplinary Perspectives. Cambridge: Cambridge University Press; 2015. pp. 50-70

[37] Taylor L. Safety in Numbers? Group Privacy and Big Data Analytics in the Developing World. Cham: Springer International Publishing AG; 2017

[38] Barocas S, Levy K. Privacy dependencies. Washington Law Review. 2020;**95**:555

[39] Jernigan C, Mistree BF. Gaydar: Facebook friendships expose sexual orientation. First Monday. 2009;**14**(10)

[40] Mislove A, Viswanath B, Gummadi KP. You are who you know: Inferring user profiles in online social networks. In: Proceedings of the Third ACM International Conference on Web Search and Data Mining. 4 Feb 2010. pp. 251-260

[41] Duhigg C. How companies learn your secrets. In: The Best Business Writing 2013. New York: Columbia University Press; 2013. pp. 421-444

[42] Bloustein EJ, Pallone NJ. Individual and group privacy. New York: Routledge; 2019

[43] Bygrave LA, Schartum DW. Consent, proportionality and collective power. In: Reinventing Data Protection? Cham: Springer International Publishing AG; 2009. pp. 157-173

[44] Mittelstadt B. From individual to group privacy in big data analytics. Philosophy & Technology. 2017;**30**:475-494

[45] Loi M, Christen M. Two concepts of group privacy. Philosophy & Technology. 2020;**33**:207-224

[46] Puri A. A theory of group privacy. Cornell Journal of Law and Pub Policy. 2020;**30**:477

[47] Kerr I. Schrödinger's robot: Privacy in uncertain states. Theoretical Inquiries in Law. 2019;**20**:123-154

[48] Sacharoff L. The relational nature of privacy. Lewis & Clark Law Review. 2012;**16**:1249

[49] Sloan RH, Warner R. Relational privacy: Surveillance, common knowledge, and coordination. University of St Thomas Journal of Law & Public Policy. 2017;**11**:1

[50] Hargreaves S. Relational Privacy & Tort. William & Mary Journal of Women & the Law. 2016;**23**:433

[51] Allen A. Unpopular Privacy: What Must we Hide? New York: Oxford University Press; 2011

[52] DeCew JW. The feminist critique of privacy: Past arguments and new social understandings. Social Dimensions of Privacy: Interdisciplinary Perspectives. 2015;**85**:90

[53] Allen AL, Mack E. How privacy got its gender. Northern Illinois University Law Review. 1989;**10**:441

[54] Regan PM. Legislating Privacy: Technology, Social Values, and Public Policy. Chapel Hill: The University of North Carolina Press; 1995

[55] Gary ME. From care ethics to pluralist care theory: The state of the field. Philosophy Compass. 2022;**17**:e12819

[56] Held V. The Ethics of Care: Personal, Political, and Global. New York: Oxford University Press on Demand; 2006

[57] Preston CJ, Wickson F. Broadening the lens for the governance of emerging technologies: Care ethics and agricultural biotechnology. Technology in Society. 2016;**45**:48-57

[58] Ruddick S. Injustice in families: Assault and domination. Justice and Care. 1995;**1995**:203-224

[59] Tronto JC. Caring Democracy: Markets, Equality, and Justice. New York: New York University Press; 2013

[60] Ford SM. Reconceptualizing the public/private distinction in the age of information technology. Information, Communication & Society. 2011;**14**:550-567

[61] Hildebrandt M. Who is profiling who? Invisible visibility. In: Reinventing Data Protection? Cham: Springer International Publishing AG; 2009. pp. 239-252

[62] Skinner BF. Walden two. Indianapolis: Hackett Publishing; 2005

[63] Dourish P, Anderson K. Privacy, security… And risk and danger and secrecy and trust and morality and identity and power: Understanding collective information practices. ISR Technical Report UCI. 2005:1-19. Report No.: UCI-ISR-05-1