Ethics and Information Technology
https://doi.org/10.1007/s10676-019-09508-z

ORIGINAL PAPER

Privacy in the digital age: comparing and contrasting individual versus social approaches towards privacy

Marcel Becker[1]

Abstract
This paper takes as a starting point a recent development in privacy-debates: the emphasis on social and institutional environments in the definition and the defence of privacy. Recognizing the merits of this approach I supplement it in two respects. First, an analysis of the relation between privacy and autonomy teaches that in the digital age more than ever individual autonomy is threatened. The striking contrast between on the one hand offline vocabulary, where autonomy and individual decision making prevail, and on the other online practices is a challenge that cannot be met in a social approach. Secondly, I elucidate the background of the social approach. Its importance is not exclusively related to the digital age. In public life we regularly face privacy-moments, when in a small distinguished social domain few people are commonly involved in common experiences. In the digital age the contextual integrity model of Helen Nissenbaum has become very influential. However this model has some problems. Nissenbaum refers to a variety of sources and uses several terms to explain the normativity in her model. The notion 'context' is not specific and faces the reproach of conservatism. We elaborate on the most promising suggestion: an elaboration on the notion 'goods' as it can be found in the works of Michael Walzer and Alisdair Macintyre. Developing criteria for defining a normative framework requires making explicit the substantive goods that are at stake in a context, and take them as the starting point for decisions about the flow of information. Doing so delivers stronger and more specific orientations that are indispensible in discussions about digital privacy.

Keywords Privacy · Autonomy · Contextual integrity · Nissenbaum

Introduction

Rethinking the concept of privacy in the digital age inevitably entangles the descriptive and the normative dimensions of this concept. Theoretically these two dimensions of privacy can be distinguished. One dimension can describe the degree of privacy people enjoy, without taking a normative stance about the desirable degree of privacy. In normative discussions, the focus is on the reasons why privacy is important for leading a fulfilling life. This distinction should not distract us from the fact that privacy is not a completely neutral concept; instead, it has a positive connotation. For example, an invasion of privacy is a *violation of* or *intrusion into* something valuable that should be protected. Discussion of the concept, however, brings into question why privacy should be cherished and protected. In the digital age, the normative dimension is the object of intense discussion. Existing dangers to privacy—because of big data applications, cloud computing, and profiling—are widely recognized, but feelings of *resignation* and *why should we bother* lie dormant. Defenders of privacy are regularly faced with scepticism, which is fueled by Schmidt's 'Innocent people have nothing to hide' (Esguerra 2009) and Zuckerberg's 'Having two identities for yourself is a lack of integrity' (Boyd 2014).

Traditionally in defences of privacy the focus has been on the individual (Rule 2015). Privacy was defined in terms of an *individual's space*, which was seen as necessary for meeting the individual's vital interests. In the last decade, however, we have seen a shift in the emphasis. A view of privacy as the norm that regulates and structures social life (the *social dimension* of privacy) has gained importance in both law and philosophical literature. For instance, the European Court of Human Rights previously stressed that data protection was an individual's right not to be interfered with. However, more and

✉ Marcel Becker
M.Becker@ftr.ru.nl

[1] Radboud University Nijmegen, Nijmegen, The Netherlands

Published online: 17 July 2019

more the Court is focusing on individuals' privacy as protection of their relationships with other human beings (van der Sloot 2014). In philosophical literature on privacy, many scholars have explicitly distanced themselves from the individual approach and instead study the *social dimensions of privacy* (Roessler and Mokrosinska 2015). Helen Nissenbaum is by far the most important spokesperson for the social approach. She has introduced the notion of *contextual integrity* as an alternative to what she describes as too much focus on individuals' rights based notions of privacy (Nissenbaum 2009). Nissenbaum criticizes the so-called interest-based approach, which defines conflicts in terms of (violated) interests of the parties involved. For instance, 'Uncontroversial acceptance of healthcare monitoring systems can be explained by pointing to the roughly even service to the interest of patients, hospitals, healthcare professionals and so on'. The problem with this approach, according to Nissenbaum, is that it sooner or later leads to 'hard fought interest brawls', which more often than not are settled to the advantage of the more powerful parties (Nissenbaum 2009, p. 8). It is necessary to create a justificatory platform to reason in moral terms. As a rights-based approach is not satisfactory, she proposes a normative approach that does more justice to the social dimension.

The distinction between a focus on the individual and privacy as social value is not only of academic importance. For policies on privacy, this makes quite a difference. On the one hand, the emphasis can be on an individual's right to decide about personal interests and transparency for *empowering the individual*, as for instance the European Data Protection Supervisor asserts (EDPS *Opinion* 2015). On the other hand, the emphasis can also be on institutional arrangements that protect social relationships. The fact that good privacy policies require measures should not be a reason to overlook their fundamental differences.

In this paper, we compare individual-based justifications of privacy with the social approach. We open with a discussion of the strengths of the individual-focused approach by relating privacy to a concept that has a strong normative sense and is most closely associated with individual-based privacy conceptions: autonomy. As we will see, a defence of privacy along these lines is both possible and necessary. In our discussion of the social approach, we focus on Helen Nissenbaum's model. A critical discussion of the normative dimension will lead to suggestions for strengthening this model.

The individual approach

The importance of privacy: autonomy

The history of justifications of privacy starts with Warren and Brandeis's (1890) legal definition of privacy as *the right to be left alone* (1890). This classic definition is completely in line with the literal meaning of privacy. The word is a negativum (related to *deprive*) of *public*. The right to privacy is essentially the right of individuals to have their *own domain*, separated from the public (Solove 2015). The basic way to describe this *right to be left alone* is in terms of *access* to a person. In classic articles, Gavison and Reiman characterize privacy as the degree of access that others have to you through information, attendance, and proximity (Gavison 1984; Reiman 1984).

Discussion about the importance of privacy for the individual intensified in the second half of the twentieth century, as patterns of living in societies became more and more individualistic. Privacy became linked to the valued notion of autonomy and the underlying idea of individual freedom. In both literature on privacy and judicial statements, this connection between privacy and autonomy has been a topic of intense discussion. Sometimes the two concepts were even blended together, even though they should remain distinct. A sharp distinction between privacy and autonomy is necessary to get to grips with the normative dimension of privacy.

The concept *autonomy* is derived from the ancient Greek words *autos* (self) and *nomos* (law). Especially within the Kantian framework, the concept is explicated in terms of a rational individual who, reflecting independently, takes his own decisions. Being autonomous was thus understood mainly as having control over one's own life. In many domains of professional ethics (healthcare, consumer protection, and scientific research), autonomy is a key concept in defining how human beings should be treated. The right of individuals to control their own life should always be respected. The patient, the consumer, and the research participant each must be able to make his or her own choices (Strandburg 2014). Physicians are supposed to fully inform patients; advertisers who are caught lying are censured; and informed consent is a standard requirement of research ethics. In each of these cases, persons should not be forced, tempted, or seduced into performing actions they do not want to do.

When privacy and autonomy are connected, privacy is described as a way of controlling one's own personal environment. An invasion of privacy disturbs control over (or access to) one's personal sphere. This notion of privacy is closely related to secrecy. A person who deliberately gains access to information that the other person wants to keep secret is violating the other person's autonomy through information control. We see the emphasis on privacy as control over information in, for instance, Marmor's description of privacy as 'grounded in people's interest in having a reasonable measure of control over the ways in which they can present themselves to others' (Marmor 2015). Autonomy, however, does not entail an exhaustive description of privacy. It is possible that someone could have the ability to

control, yet he or she lacks privacy. For instance, a woman who frequently absentmindedly forgets to close the curtains before she undresses enables her neighbour to watch her. If the neighbour does so, we can speak about a loss of the woman's privacy. Nevertheless, the woman still has the ability to control. At any moment, she could choose to close the curtains. Thus, privacy requires more than just autonomy.

The distinction between privacy and autonomy becomes clearer in Judith Jarvis Thompson's classic thought experiment (Taylor 2002). Imagine that my neighbour invented some elaborate X-ray device that enabled him to look through the walls. I would thereby lose control over who can look at me, but my privacy would not be violated until my neighbour actually started to look through the walls. It is the actual looking that violates privacy, not the acquisition of the power to look. If my neighbour starts observing through the walls but I'm not aware of it and believe that I am carrying out my duties in the privacy of my own home, my autonomy would not be directly undermined. Not only in thought experiments, but also in literature and everyday life, we witness the difference between autonomy and privacy. Taylor refers to Scrooge in Dickens' *A Christmas Carol* who is present as a ghost at family parties. His covert observation of the intimate Christmas dinner party implies a breach of privacy, although he does not influence the behaviour of the other people. In everyday life, we do not experience an inadvertent breach of privacy (for instance, a passer by randomly picking up some information) as loss of autonomy.

These examples make it clear that there is a difference between autonomy, which is about control, and privacy, which is about knowledge and access to information. The most natural way to connect the two concepts is to consider privacy as a tool that fosters and encourages autonomy. Privacy thus understood contributes to demarcation of a personal *sphere*, which makes it easier for a person to make decisions independently of other people. But a loss of privacy does not automatically imply loss of autonomy. A violation of privacy will result in autonomy being undermined only when at least one additional condition is met: the observing (privacy-violating) person is in one way or another influencing the other person (Taylor 2002). Such a violation of privacy can take various forms. For instance, the person involved might feel pressure to alter her behaviour just because she knows she is being observed. Or a person who is not aware of being observed is being manipulated. This, in fact, occurs more than ever before in the digital age.

Loss of autonomy in the digital age

In the more than 100 years following Warren and Brandeis' publication of their definition, privacy was mainly considered to be a spatial notion. For example, the right to be left alone was the right to have one's own space in a *territorial* sense, e.g., at home behind closed curtains, where other people were not allowed. An important topic in discussions of privacy was the embarrassment experienced when someone else entered the private spatial domain. Consider, for example, public figures whose privacy is invaded by obtrusive photographers or people who feel invaded when someone unexpectedly enters their home (Roessler 2009; Gavison 1984).

The digital age is characterized by the omnipresence of hidden cameras and other surveillance devices. This kind of observation and the corresponding embarrassment that it can cause have changed our ideas about privacy. The main concern is not the intrusive eye of another person, but the constant observation, which can lead to the panopticon experience of the interiorized gaze of the other. It is self-evident that the additional conditions are now being met, viz., the person's autonomy is threatened. In situations in which the observed person feels impeded to follow his impulses (Van Otterloo 2014), the loss of privacy leads to diminished autonomy.

The loss of autonomy resulting from persistent surveillance becomes even more striking when we take into consideration the unprecedented collection and storage of non-visual information. Collecting data on individuals, such as through the activity of profiling, offers commercial parties and other institutions endless possibilities for approaching people in ways that meet the institution's own interests. Driven by invisible algorithms, these institutions temp, nudge, seduce, and convince individuals to participate for reasons that are advantageous to the institution. The widespread application of algorithms in decision-making processes intensifies the problem of loss of autonomy in at least two respects. First, when algorithms are used to track people's behaviour, there is no 'observer' in the strict sense of the word; no human (or other 'cognitive entity') actually ever checks the individual's search profile. Nevertheless, the invisibility of the watchful entity does not diminish the precision with which the behaviour is being tracked; in fact, it is quite the opposite. Second, in the digital age mere awareness of the possibility that surveillance techniques exist has an impact on human behaviour, independently of whether there is actually an observing entity. More than ever before, Foucault's (1975) addition to Bentham's panopticon model is relevant. The gaze of the other person is internalized.

This brings us to the conclusion that, despite the fact that a loss of privacy does not necessarily involve a loss of autonomy, in the digital age when privacy is under threat, the independence of individual decisions is typically also compromised.

These observations are striking when we consider that Western societies in particular focus on the individual person, whose autonomy is esteemed very highly. We can contrast the self-image and ego vocabulary that prevail in

everyday life with online situations where an individual's autonomy is lost. There are two examples of this from domains where autonomy has traditionally been considered to be very important and where it has come under threat.

Advertising

In consumer and advertising ethics, the consumer's free choice is the moral cornerstone. In the online world, this ethical value is scarcely met. Digitalisation facilitates customised advertising, which originally was presented as a service for the individual. Tailored information was supposed to strengthen a person's capacities to make choices to his own advantage. But now the procedure has become degenerated; people are placed into a filter bubble based on algorithms and corporate policies that are unknown to the target persons. Individuals' control and knowledge about the flow of information are lost. As we all are keenly aware, requiring people to agree with terms and conditions does nothing to solve the problem. In the first place, very few people even read them. This kind of autonomy is apparently too demanding for most people to exercise. Secondly, the terms and conditions do not themselves say anything about the algorithms. Today's consumer finds himself in a grey area, where he struggles between exercising autonomy and being influenced by others.

Of course, it is an empirical question as to what degree the algorithms influence customers' behaviour. The least we can say is that the wide application of algorithms suggests that they must have a substantial effect. Following the critical study of Sunstein (2009) in which he warns that the political landscape might become fragmented ('cyberbalkanization'), much research has been undertaken on the influence of algorithms on political opinions. This has resulted in a nuanced view of the widespread existence of 'confirmation bias'. For instance, it has been shown that the need for information that confirms one's opinion differs from other kinds of information and that it is stronger in those people who have more extreme political opinions. Furthermore, there turns out to be a major difference between how often individuals actively search for opinions similar to their own (what people usually do) and how often they consciously avoid noticing opinions that differ from their own (which are far more infrequent). People surfing the Internet often encounter news they were not consciously looking for, but which they nevertheless take seriously. This is called 'inadvertent' attention for news (Garret 2009; Tewksbury and Rittenberg 2009; Becker 2015, Chap. 4).

The question how online networks influence exposure to perspectives that cut across ideological lines received a lot of attention after the Brexit referendum and Trump election. Using data of 10.1 million Facebook users Bakshy et al. confirm that digital technologies have the potential to limit exposure to attitude-challenging information. The authors observed substantial polarization among hard content shared by users, with the most frequently shared links clearly aligned with largely liberal or conservative populations. But one-sided algorithms are not always of decisive importance. The flow of information on Facebook is structured by how individuals are connected in the network. How much cross-cutting content an individual encounters depends on who his friends are and what information those friends share. According to Bakshy et al. on average more than 20% of an individual's Facebook friends who report an ideological affiliation are from the opposing party, leaving substantial room for exposure to opposing viewpoints (Bakshy et al. 2015). Dubois and Blank, using a nationally representative survey of adult internet users in the UK found that individuals do tend to expose themselves to information and ideas they agree with. But they do not tend to avoid information and ideas that are conflicting. Particularly those who are interested in politics and those with diverse media diets tend to avoid echo chambers. Dubois & Blank observe that many studies are single platform studies, whereas most individuals use a variety of media in their news and political information seeking practices. Measuring exposure to conflicting ideas on one platform does not account for the ways in with individuals collect information across the entire media environment. Even individuals who have a strong partisan affiliation report using both general newssites which are largely non-partisan and include a variety of issues (Dubois and Blank 2018, see also Alcott et al.). These findings are consistent with other studies that indicate that only a subset of Americans have heavily skewed media consumption patterns (Guess et al. 2016).

Research ethics

Corporations such as Google and Facebook, as well as data brokers use people's personal information in their research activities. One disturbing example is the research that Facebook conducted in 2014. The corporation experimented on hundreds of thousands of unwitting users, attempting to induce an emotional state in them by selectively showing either positive or negative stories in their news feeds (Kramer et al. 2014; Fiske and Hauser 2014). Acquiring information by manipulating people without their informed consent and without debriefing them is a gross violation of the ethical standards that established research institutions must follow.

Such violations of people's autonomy indicate a striking contrast between the offline ideals of most users and their online practices. Whereas in the offline world we typically take autonomy as a moral cornerstone, on the Internet this ideal is not upheld. How to deal with this discrepancy in values upheld in the real world and on the Internet is one of

the central challenges in discussions about privacy. When we do not strive for more clarity and transparency in the flow of information, we relinquish autonomy, a value that is deeply embedded in Western cultures.

The social approach

We might be tempted to associate the emergence of the social approach in discussions about privacy with the digital age, as if only in these times of rapid information flow reflection on the social dimension of privacy is justified. This, however, would be a false suggestion. During the twentieth century, an important undercurrent in discussions of privacy was an emphasis on the importance of privacy for social relationships. Privacy was seen as a component of a well- functioning society (Regan 2015), in that it plays an important role in what is described as a differentiated society. Privacy guarantees social boundaries that help to maintain the variety of social environments. Because privacy provides contexts for people to develop in different kinds of relationships, respect for privacy enriches social life. Privacy also facilitates interactions among people along generally agreed patterns (Schoemann 1984). As the poet Robert Frost remarked in *Mending Wall* (1914), *Good fences make good neighbors*.

This characteristic of privacy is important not only at an institutional level. In people's private lives the creation and maintenance of different kinds of relationships is possible only when subtle differences in patterns of social behaviour and social expectations are recognized (Rachels 1984, Marmor 2015). Remarkably, this subtlety becomes clearest in examples of intrusions of privacy in unoccupied public places. Consider (a) someone who deliberately attempts to sit beside lovers who are sitting together on a park bench, or (b) intrusive bystanders at the scene of a car accident. In both cases, the intrusions of the privacy of the persons involved are very important. The most trivial words and gestures can reflect a deep dedication and intense relationship between two people. In one of the first descriptions of the core of privacy, the English jurist and philosopher Stephens depicted it as an observation which is sympathetic (Schoemann 1984). Sympathetic is derived from the Greek word *sympathein*, which means being involved with the same. Indeed, in private situations, different people experience the same things as important. A small, clearly distinguished domain is created, and the events should be shared only by those who directly participate in them. The persons involved are tied together by having undergone common experiences. They have an immediate relationship to what is at stake, and in this relationship they are deeply engrossed. An outside observer who has not participated in the common experience is viewed as invading their privacy. He cannot share the meaning of what is going on because he has not been directly involved.

When understood this way the concept of privacy is helpful in explaining the difference between occasionally being noticed and being eavesdropped upon. In cases involving eavesdropping, someone participates in an indirect and corrupt way in what is going on. The participation is indirect because the person acquires knowledge without participating directly; the things that are at stake should not concern him. The participation is corrupt because the indirect participant is not genuinely interested in what is going on. He sees the others involved not primarily as people with their own sensibilities, goals, and aspirations, but as the objects of his own curiosity. When the other people become aware that they are being observed, they begin to see themselves through the eyes of the observing person, and they thereby lose spontaneity. Their direct involvement in the meaning of what is at stake is lost.

In cases like these, neither the content of the action nor the secrecy surrounding it qualifies the actions as belonging to the private sphere. The content might be very trivial, but it would be offensive to the lovers sitting on the park bench to suggest that what they are expressing to each other could be made public. The most commonplace of actions—for instance, walking with one's children down the street—can be private. Note the indignation of people in the public eye about obtrusive photographers who take photographs of public figures while they are doing ordinary things like we all do. The essence of secrecy is intentional concealment, but the private situations that we discuss here concern behaviour, inward emotions, and convictions that can be shown and experienced in various places that are accessible to everyone, as for instance in the case of the young couple we saw sitting in the park (Belsey 1992).

This characteristic of privacy in social relationships cannot be captured by the concept of autonomy in the sense of an individual independently and deliberately making his or her own choices. What is at stake in situations like these is not a lack of transparency. There is no question about the autonomy of an independent individual. The person would be deeply engrossed in precarious and delicate situations involving social relationships. An intrusion on this person's privacy would mean that he feels inhibited in being immersed in the social interaction and share the meaning at stake.

In order to do justice to this notion of privacy, other strategies for protecting privacy are required. It is not primarily an individual's mastery that must be protected; rather, it is the possibility for the individual to be properly embedded in social relationships. To answer the question of how this concept of privacy manifests itself in the digital age, we turn to

Helen Nissenbaum's *contextual integrity* model, which is an elaboration of socially embedded privacy in the digital age.

Helen Nissenbaum's contextual integrity model

After having conducted several preliminary studies, Helen Nissenbaum published *Privacy in Context* (2009), a book that became very influential in philosophical and political debates on privacy. It inspired the Obama administration in the United States to focus on the principle of respect for context as an important notion in a document on the privacy of consumer data (Nissenbaum 2015). The core idea of Nissenbaum's model is presented in the opening pages of her book: 'What people care most about is not simply *restricting* the flow of information but ensuring that it flows *appropriately*.' In Nissenbaum's view, the notion 'appropriate' can be understood to mean that normative standards are not determined by an abstract, theoretically developed default. The criteria for people's actions and the expectations of the actions of other people are developed in the context of social structures that have evolved over time, and which are experienced in daily life. As examples of contexts, Nissenbaum mentions health care, education, religion, and family. The storage, monitoring, and tracking of data are allowed insofar as they serve the goals of the context. Privacy rules are characterized by an emphasis on data security and confidentiality, in order to ensure that the flow of information is limited only to the people directly involved. The key players in the context have the responsibility to prevent the data from falling into the wrong hands.

Nissenbaum's model is well-suited for the information age. It describes privacy in terms of the flow of information, and the model is easy to apply to institutional gatekeepers who deal with data streams. At the same time, the contextual approach deviates from the classical view of autonomy. The personal control of information loses ground, and shared responsibility that is expressed through broader principles becomes more important. Nissenbaum considers it a serious disadvantage of the autonomy approach that it is usually associated with notions of privacy that are based on individuals' rights. In the articulation of justificatory frameworks in policymaking and the legal arena, we often see major conflicts among parties who insist that their rights and interests should be protected. She also distances herself from the connection between privacy and secrecy (for a recent description of this connection, see Solove 2015). Privacy is not forfeited by the fact that someone knows something about another person. Within contexts, information about persons might flow relatively freely. In line with this, Nissenbaum puts into perspective the classic distinction between the private and the public realm. Contexts might transgress borders between the public and the private. For instance, professionals in social healthcare work with information that comes from intimate spheres. As professionals, they are, however, part of the public domain. It is their professional responsibility to deal properly with the flow of information within the realm of their own activities.

Normative weakness and the threat of conservatism

Nissenbaum's rejection of autonomy as the basis for privacy raises questions about the normative strength of her model. Does she indeed deliver the justificatory platform or framework to reason in moral terms? She asserts that her model does do so when she claims that the context procures a clear orientation, which can guide policies on privacy. This claim suggests that it is completely clear what a context is, as is the way in which it delivers a normative framework. In this respect, Nissenbaum's work has some flaws.

In her description of context as a structured social setting that guides behaviour, Nissenbaum refers to a wide array of scholars from social theory and philosophy. Nissenbaum (2009), for instance, reviews Bourdieu's field theory, Schatzki's notion of practice in which activities are structured teleologically, and Walzer's *Spheres of Justice*. There are, however, major differences among these authors. Schatzki focuses on action theory and the way in which people develop meaningful activities; Walzer describes the plural distribution of social goods in different spheres of human activity; and Bourdieu focuses on power relationships. When searching for a normative framework, it matters which of these approaches is being taken as the starting point. The theories also differ in their emphasis on a descriptive (Bourdieu) versus a normative (Walzer) analysis.

This vagueness about the normative framework is a serious problem because protection of privacy in the digital age requires systemic criteria to measure new developments against established customs. Nissenbaum assumes at the start that online technologies change the way in which information flows, but they do *not* change the principles that guide the flow of information. The principles by which digital information flows must be derived from the institutions as they function in the off-line world, i.e., the background social institutions (Nissenbaum 2009). Consider online banking as an example. In the digital age, contacts between costumers and banks have completely changed. Impressive buildings in which people previously made financial transactions have been partly replaced by the digital flow of information. But the core principles regarding the actions of the actors (the so called information and transmission principles) have not changed. This implies that people working within the context are familiar with the sensible issues, and

they have the final say. The only thing that must be done is to translate the principles to the new situation. In case the novel practice results in a departure from *entrenched* norms, as Nissenbaum says, the novel practice is flagged as a breach, and we have prima facie evidence that contextual integrity has been violated (Nissenbaum 2009). Indeed, Nissenbaum admits that this starting point is inherently conservative, and she flags departures from entrenched practice as problematic (2009). She leaves open the possibility that completely new developments can lead to a revision of existing standards, and she gives ample guidelines about how to implement such a revision (Nissenbaum 2015).

Nissenbaum's emphasis on existing practices must be understood in the context of a non-philosophical and non-sociological source, e.g., the notion of reasonable expectation, which plays an important role in United States jurisprudence on privacy. In the conclusion of her book, Nissenbaum (2009) describes privacy as 'a right to live in a world in which our expectations about the flow of personal information are, for the most part, met'. Reasonable expectation was the core notion in the famous case of *Katz* versus *United States*, which laid the foundation for privacy discussions in the United States. Before *Katz*, it had already been recognized that within one's own home, there was a justified expectation of privacy. *Katz* dealt with the kind of privacy situations in the public sphere that was described in the preceding paragraph. In this case, a phone call had been made from a public phone booth while enforcement agents used an external listening device to listen to the conversation. The Court considered this to be unjustified. The Fourth Amendment to the United States Constitution protects people, but not places; therefore, the actions of the enforcement agents constituted an intrusion. Regardless of location, oral statements are protected if there is a reasonable expectation of privacy. This extension of privacy was a revolutionary development, and the notion of reasonable expectation turned out to work well. For instance, in cases where the distinction between hard-to-obtain information and information that is in plain view plays an important role. In many cases, however, just because information is in plain view does not mean there is a reasonable expectation of privacy. Consider the situation where the police accidentally uncover illegal drugs concealed in an automobile. In cases like this, an appeal to privacy to protect criminals cannot be justified.

However, the normative strength of the notion reasonable expectation is weak. The notion refers to existing practices; reasonable is what in a society counts as reasonable. In many cases, this might work out well. We usually do not need polls to make it clear what reasonable means. Eavesdropping is despised, yet video surveillance in a taxi is generally accepted. Police arbitrarily invading a house is not justified; however, police actively working to find concealed drugs are justified. In times of rapid development, referring to existing practices to find ultimate normative justification is not a good strategy, for at least two reasons. First, the danger of rigid conservatism might be just around the corner. This danger was already present in Nissenbaum's idea that standards for online intrusions of privacy must be derived from the offline world. In times of technological developments new problems make their appearance, and new technologies change the effects of existing rules. Particularly in the digital age, practices and normative conceptions are under pressure; existing frameworks cannot be used unequivocally. In the times of *Katz*, the distinction between hard-to-obtain information and information in plain view was based on how easy it was to access the information, irrespective of the type of information. This distinction is out-of-date in the digital age. The revolution in techniques of surveillance makes almost all information that is in plain view information. Any development in surveillance or monitoring, if communicated well, might be placed under the umbrella of reasonable expectation. Suppose a government takes highly questionably measures (for instance, it collects all metadata on phone calls) and is completely honest about doing so. The government does not want to surprise its citizens, so it duly informs the public that this is how things are being done. Anyone who makes a phone call has the expectation that her data will be stored. We all know this is not simply a hypothetical example. The same pattern can be distinguished in the way Google and Facebook justify their practices. Thanks to Mark Zuckerberg's and Eric Schmidt's statements, Facebook and Google users do not have expectations about privacy. Ironically, the insistence on transparency, which is so often heard in debates on privacy, takes the sting out of the idea of reasonable expectation. Transparency implies that data streams can flow in all directions, as long as the responsible persons are open and honest about it (Schoonmaker 2016).

Some would suggest that the word *reasonable* (as opposed to *unreasonable*) has a certain normative strength. The word refers to standards that have a certain degree of plausibility and are widely shared. Again, however, in order to guarantee protection of privacy, we need more guidance about what these standards mean, for the concept itself does not provide this guidance. The matter is turned upside down when we search for normative strengths simply by referring to current practices.

The threat of conservatism in the digital age and the failure of the notion reasonable expectation lead us to the conclusion that strong anchors, which meet certain criteria, are needed. This is first of all apparent in the conservative-progressive dimension. The standards must be related to existing frameworks; alienation from these hampers acceptance. On the other hand, they shouldn't be so rigid that promising new developments are impeded. Second, it is apparent in the general-specific dimension. To motivate people, they must be so general that a wide

range of applications is possible. Nevertheless, they should not be too vague; they must be specific enough to contain guidelines for action.

A variety of notions that describe normative standards accompany Nissenbaum's reference to various philosophical and sociological sources. As far as the dimension conservative-progressive is concerned, she switches, on the one hand, between internal logic of and settled rationale for social systems, and she pleads, on the other hand, for the moral superiority of new practices (Lever 2015). Nissenbaum also speaks about ultimate criteria as delivered by the purposes and ends of the context. This description is too concrete in times of rapid technological developments. Today's targets become outmoded tomorrow. Some more general notion is required. In a recent refinement of her model, Nissenbaum (2015) provides more clarity. For example, she mentions a few domains of cooperative activities that need not count as context per se. The business model for instance does not count as context, because in business the core value is earning money. When everything is for sale, it is impossible to develop independent, substantive landmarks. She also makes it clear that a describing context as a technological system is highly problematic. It leads to technological determinism, and therefore is a *petitio principi*. Normative standards about how to deal with technological problems are derived from technological developments. A proper context can count as what she describes as a social domain. Remarkably, she hardly considers this notion.

The search for independent substantive landmarks might be guided by the expression norms and values, which Nissenbaum uses in her book. Norms are fixed standards. Usually they are concrete descriptions of particular things that must be realised or derived. Norms are necessary for guiding actions, but in times of fast changes they are too rigid. Values, on the other hand, are very general, even though they are not vague. Values such as justice, responsibility, and efficiency are used in a wide variety of contexts. This is especially true for the group of values (e.g., justice, respect, integrity, decency) that is concerned with the way in which we treat other people. These values surpass the context; they are important in society as a whole. They are, therefore, too general to deliver a normative orientation for actions within a context. One way to solve this problem would be to rewrite the values in a context-specific sense. This requires orientation points that refer to characteristics of the contexts.

At the end of her book, Nissenbaum admits that her description of context is deficient; she acknowledges that further research on the concept is necessary. We suggest following a suggestion that Nissenbaum herself made. In a short paragraph in *Privacy in context*, she refers to Michael Walzer's conception of goods as constitutive for contexts. It is the only notion to which she devotes a full paragraph; intriguingly, however, she does not elaborate on this concept in her later work. This notion could be very useful for making more explicit the underlying normativeness in contexts.

The concept of substantial goods

In his famous *Spheres of Justice*, Walzer (1983) stresses that he does not include material objects of transaction in his definition of goods. Instead, he uses a broader and more abstract notion of goods. They are immaterial qualities that people conceive and create in the course of their actions. In his book, he comments on goods such as security, education, health, kinship, and life. While performing an action, people are oriented towards goods such as these. The goods come into people's minds before they come into their hands. Goods are, moreover, crucial for social relationships (Walzer 1983). The development of goods takes place in social contexts. For people to be able to live together, they must have more or less shared conceptions about the meaning of vital goods. The main goal of Walzer's book is to show that different spheres of actions are characterized by different conceptions of goods, and subsequently different distributions of principles. The book turned out to be a very important expression of an idea that became very influential in determining standards for professional conduct: When human beings closely share an orientation on good actions with other human beings, this leads to a proper professional life. Only when goods are determined is it possible to adjust the standards. Without going into detail, we can point to two lines of thought that have contributed to elucidation and specification of the notion *good*.

Both Charles Taylor and Bernard Williams have distinguished goods from objects of impulsive desires and wishes by explaining that goods have an impact on a deep level of motivation. Goods 'are judged as belonging to qualitatively different modes of living' (Taylor 1999). They are the fulfilment of deeper commitments and engagements. Not the intensity of the desire but the sense of worth that makes life meaningful is characteristic of human attitudes towards goods. Attachment to and engagement with goods extend over a longer period and lead to a deeper fulfilment when satisfied. Goods give meaning to professional life (Williams 1981).

For professional ethics, Alisdair MacIntyre's contributions have been of great importance. He elaborated on a distinctive characteristic of the concept good, which professionals have very often used in dealing with moral dilemmas. In socially established cooperative activities—MacIntyre mentions various examples of these, such as chess, portrait-painting, and education—people are guided by internal goods, which are defined as abstract qualities that are realised in the course of an active life. MacIntyre distinguishes between internal goods and external goods such as money,

power, and prestige. External goods are necessary only for maintaining organizations and institutions, so that the kernel for a practice exists in realising internal goods. The distinction between internal and external goods can be made along two lines. First, external goods are called external as they also can be acquired through activities that are not restricted to the practice. This is true in the sense that in activities outside the practices money, power, and prestige play a role, but it is also true in the sense that within practices it is possible to acquire money, power, and prestige through dishonest means. In opposition to this internal goods can be acquired only by excelling in activities that belong to the practice. Secondly, external goods are always in some individual's possession. The more someone has of them, the less there is for other people. They are always objects for competition. Internal goods, on the other hand, are not in short supply. Their achievement is good for the whole community whose members participate in the practice; they can be shared in the full sense of the word. Many people can be orientated towards acquiring them without being in conflict with one another. In fact, a common orientation strengthens the motivation of each member of the community.

The differences among these authors do not invalidate their common focus. The distinctions they make are insightful for understanding how certain kinds of activities contribute to a meaningful life. We describe them under the heading 'substantial goods', which furnish us with a normative framework that can be used to evaluate activities. During recent decades, this line of thought has played an important role in public administration (Becker and Talsma 2015), journalism (Borden 2007), business (Solomon 1992), healthcare (Day 2007), and science. It has been particularly helpful to distinguish between qualities that are related to the content of a work and institutional and external pressures. For instance, the appropriate task for a variety of professions that stress quantitative performance measures can be elucidated using the emphasis on substantial goods; they include journalists working in a democracy, scientists working in academic institutions, and public administrators who must answer to higher-level management. The ultimate goal of their actions does not lie in complying with external standards, but in realising goods that are themselves recognized as being of substantive importance.

Substantial goods in Helen Nissenbaum's model

In the application of this line of thought to Helen Nissenbaum's model, we make explicit the goods that are at stake in a context, and we take them as the starting point for decisions about the flow of information. This strategy can contribute to the solution of several problems that currently stand in the way of further applying Nissenbaum's model.

A more explicit articulation of the goods at stake will be helpful in solving the problem of conservatism. We have discussed how the notion of 'reasonable expectation' and Nissenbaum's model might evoke the reproach of someone with a conservative orientation to fixed standards that do not do justice to new developments. The notion of substantial goods enables us to describe activities under a normative perspective without being restricted to certain activities. The meaning of goods can be translated in various activities. New developments lead to new interpretations of the goods involved, which, in turn, facilitate innovation. Take, for instance, education. Under the umbrella of having a good education, a wide variety of patterns of education can be developed, and new trends can be incorporated.

Another advantage of elaboration of the notion of goods is that it contributes to a sharper context-specific meaning of broad, general values, such as justice, respect, and integrity. These values are very important throughout society as a whole. But the price they have to pay for the overall appreciation is that they are vague and abstract. A more precise meaning requires them to be applied in concrete contexts. This is exactly what Michael Walzer does with the value 'justice' in *Spheres of Justice*. He shows that the criteria for distribution are dependent on standards that differ from one context to another. Likewise, a precise description of the meaning of the notion 'respect' in education (i.e. respect for the student or the teacher) differs from respect as understood in healthcare (i.e. respect for the patient). Knowledge of the substantial goods at stake is helpful when it comes to concretizing these broad notions. And this is not simply a superfluous luxury in the digital age. For instance, in healthcare explicit awareness of the meaning of 'respect' for the patient helps to determine the appropriate flow of information that benefits the patient's health. It is, therefore, helpful in protecting the interests of the patient from institutional pressures or pressures from special interest groups.

In addition to these merits, an articulation of the substantial goods delivers a welcomed intervention in an otherwise awkward debate about the different roles that privacy can play. Privacy is not exclusively positive. It can, for instance, be used to conceal poor practices. Hiding information is a central feature of deception. For instance, feminists have stated that privacy is the enemy of equality… placing ordinary people at the mercy of powerful people (Marx 2015). For criminals, privacy is a cover-up for their activities. Relating privacy to the substantial goods it serves is helpful in these debates, in which privacy seems to be a double-edged sword. When it is clear which kinds of goods privacy serves (e.g. goods of particular interest groups; emancipation; the common good), a context-specific discussion on the value of privacy is possible.

Finally, the notion of goods importantly contains a normative orientation, which is distinguished from, for instance,

economic imperatives. After all, commercial interests are increasingly hampering privacy. A stronger awareness of the substantial goods at stake strengthens arguments against commodification. This is even more important as privacy is increasingly encroached upon in terms of trade-offs. People are being seduced to choose between, for instance, more privacy versus more customized offers from corporations or more privacy versus paying a lower insurance premium. In such trade-offs, privacy is described as a luxury that only wealthy people can afford (Criado and Such 2015). How far can we go without spoiling what is vital for leading a good life? A strong articulation of substantive goods will be helpful placing a barrier between commercial pressures and leading a good life.

Conclusions

During the past decade, we have witnessed the emergence of the so-called social approach to privacy. This approach must be clearly distinguished from an autonomy approach. These two approaches rely on different normative frameworks and different justification strategies. Both of them have their merit in the digital age. Changing technologies threaten autonomy, and autonomy is indispensable for making clear what is at stake in discussions of privacy. Neglecting autonomy and the processes that threaten to undermine it is harmful for individuals. The social approach, which has been an undercurrent for decades, gains importance in the digital age. When privacy is defined in terms of control over flows of information, an approach is required that surpasses the perspective of the individual. The right to privacy provides protection in relationships with other human beings and with institutions, where the fulfilment and development of one's personal identity can be realised. The normative strength of this approach can be improved by a more explicit elaboration of the goods that are at stake.

References

Bakshy, E., Messing, S., & Adamic, L. (2015). Exposure to ideologically diverse news and opinion on Facebook. *Science, 348*(6239), 1130–1132.

Becker, M. (2015). *Ethiek van de digitale Media*. Amsterdam: Boom.

Becker, M., & Talsma, J. (2015). Adding colours to the shades of grey: Enriching the integrity discourse with virtue ethics concepts. In A. Lawton, Z. Van der Wal, & L. Huberts (Eds.), *Ethics in public policy and management: A global Research companion* (pp. 33–49). London & New York: Routlegde.

Belsey, A. (1992). Privacy, publicity and politics. In A. Belsey & R. Chadwick (Eds.), *Ethical issues in journalism and the media* (pp. 77–92). London: Routledge.

Borden, S. (2007). *Journalism as a practice: Macintyre, virtue ethics and the press*. Farnham: Ashgate.

Boyd, D. (2014). *It's complicated: The social Lives of networked Teens*. New Haven, London: Yale University Press.

Criado, N., Such, J. M. (2015). Towards implicit contextual integrity. The Second International Workshop on Agents and CyberSecurity (ACySE), pp. 23–26.

Day, L. (2007). Courage as a virtue necessary to good nursing practice. *American Journal of Critical Care, 16*(6), 613–616.

Dubois, E., & Blank, G. (2018). The echo chamber is overstated: The moderating effect of political interest and diverse media. *Information, Communication & Society, 21*(5), 729–745.

Esguerra, R. (2009). Google CEO Eric Schmidt dismisses the importance of privacy. Blog Posting. Electronic Frontier Foundation. Retrieved January 10, 2014 from https://www.eff.org/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy.

European Data Protection Supervisor (EDPS) *Opinion* 4/2015 'Towards a new digital Ethics'.

Fiske, S., & Hauser, R. M. (2014). Protecting human research participants in the age of big data. *PNAS, 111*(38), 1375–1376.

Foucault, M. (1975). *Surveiller et Punir. Naissance de la Prison*. Paris: Gallimard.

Frost, R. (1914). Mending Wall. Poem in online collection. Retrieved March 13, 2014 from http://writing.upenn.edu/~afilreis/88/frost-mending.html.

Garrett, G. (2009). Echo chambers online? Politically motivated selective exposure among internet news users. *Journal of Computer-mediated Communication, 14,* 265–285.

Gavison, R. (1984). Privacy and the Limits of Law. In F. A. Schoemann (Eds.), *Philosophical Dimensions of Privacy: An Anthology* (pp. 347–402). Cambridge: Cambridge University Press. (Repr. From Gavison, R. (1980). Privacy and the limits of law. The Yale Law Journal, 89(3), 421–471).

Guess, A., Brendan, N., Reifler, J. (2016). Selective exposure to misinformation: Evidence from the consumption of fake news during the 2016 U.S. presidential campaign. Paper European Research Council, https://www.dartmouth.edu/~nyhan/fake-news-2016.pdf.

Kramer, A. D. I., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *PNAS, 111*(24), 8788–8790.

Lever, A. (2015). Privacy, democracy and freedom of expression. In B. Roessler & D. Mokrosinska (Eds.), *Social dimensions of privacy: Interdisciplinary perspectives* (pp. 162–183). Cambridge: Cambridge University Press.

Marmor, A. (2015). What is the right to privacy? *Philosophy & Public Affairs, 43*(1), 4–26.

Marx, G. T. (2015). Coming to terms: The kaleidoscope of privacy and surveillance. In B. Roessler & D. Mokrosinska (Eds.), *Social dimensions of privacy: Interdisciplinary perspectives* (pp. 32–49). Cambridge: Cambridge universiy Press.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy and the integrity of social life*. Stanford: Stanford University Press.

Nissenbaum, H. (2015). Respect for context as a benchmark for privacy online: What it is and isn't. In B. Roessler & D. Mokrosinska (Eds.), *Social dimensions of privacy: Interdisciplinary perspectives* (pp. 278–302). Cambridge: Cambridge University Press.

Rachels, J. (1984). Why privacy is important. In F. A. Schoemann (Ed.), *Philosophical dimensions of privacy: An anthology* (pp. 290–294). Cambridge: Cambridge University Press.

Regan, P. (2015). Privacy and the common good: Revisited. In B. Roessler & D. Mokrosinska (Eds.), *Social dimensions of privacy:*

Interdisciplinary perspectives (pp. 50–70). Cambridge: Cambridge University Press.

Reiman, J. (1984). Privacy, intimacy and personhood. In F. A. Schoemann (Ed.), *Philosophical dimensions of privacy: An anthology* (pp. 300–316). Cambridge: Cambridge University Press.

Roessler, B. (2009). De glazen samenleving en de waarde van privacy. *Filosofie & Praktijk, 30*(5), 20–29.

Roessler, B., & Mokrosinska, D. (2015). Introduction. In B. Roessler & D. Mokrosinska (Eds.), *Social dimensions of privacy: Interdisciplinary perspectives* (pp. 1–8). Cambridge: Cambridge University Press.

Rule, J. B. (2015). Privacy: The longue durée. In B. Roessler & D. Mokrosinska (Eds.), *Social dimensions of privacy: Interdisciplinary perspectives* (pp. 11–31). Cambridge: Cambridge University Press.

Schoeman, F. A. (1984). Privacy: Philosophical dimensions of the literature. In F. A. Schoemann (Ed.), *Philosophical dimensions of privacy: An anthology* (pp. 1–33). Cambridge: Cambridge University Press.

Schoonmaker, J. (2016). Proactive privacy for a driverless age. *Information & Communications Technology Law, 25*(2), 96–128.

Solomon, R. (1992). *Ethics and excellence: Cooperation and integrity in business*. New York: Oxford University Press.

Solove, D. J. (2015). The meaning and value of privacy. In B. Roessler & D. Mokrosinska (Eds.), *Social dimensions of privacy: Interdisciplinary perspectives* (pp. 71–82). Cambridge: Cambridge University Press.

Strandburg, K. (2014). Monitoring, datafication and consent: Legal approaches to privacy in the big data context. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, big data and the public good: Frameworks for engagement*. Cambridge: Cambridge University Press.

Sunstein, C. (2009). *Republic 2.0*. New Jersey: Princeton University Press.

Taylor, C. (1999). *Human agency and language: Philosophical papers 1*. Cambridge: Cambridge University Press.

Taylor, J. S. (2002). Privacy and autonomy: A reappraisal. *Southern Journal of Philosophy, 40*(4), 587–604.

Tewksbury, D., & Rittenberg, J. (2009). Online news creation and consumption. Implication for modern democracies. In A. Chadwick & P. Howard (Eds.), *The Routledge handbook of internet politics* (pp. 186–200). London: Routledge.

van der Sloot, B. (2014). Privacy as human flourishing: Could a shift towards virtue ethics strengthen privacy protection in the age of Big Data? *Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 5*(3), 230–244.

van Otterlo, M. (2014). Automated experimentation in Walden 3.0: The next step in profiling, predicting, control and surveillance. *Surveillance and Society, 12,* 255–272.

Walzer, M. (1983). *Spheres of justice: A defence of pluralism and equality*. Oxford: Blackwell.

Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193–220.

Williams, B. (1981). Persons, character and morality. In J. Rachels (Ed.), *Moral luck*. Cambridge: Cambridge University Press.