# Privacy

**Tobias Matzner**

*University Paderborn, Germany, tobias.matzner@uni-paderborn.de*

**Carsten Ochs**

*Department of Sociological Theory, Universität Kassel, Germany, carsten.ochs@uni-kassel.de*

**Abstract:** This contribution provides a short introduction into the conceptual and socio-technical development of privacy. It identifies central issues that inform and structure current debates as well as transformations of privacy spurred by digital technology. In particular, it highlights central ambivalences of privacy between protection and de-politicization and the relation of individual and social perspectives. A second section connects these issues to the influential texts and discussions on digital privacy. In particular, we will demonstrate privacy in digital societies is to be conceived in a novel way, since contemporary socio-technical conditions unsettle central assumptions of established theories: forms of perceptions, social structure or individual rights. Thus, a final third paragraph summarises theoretical innovations triggered by this situation – especially research from computer science to the social sciences and law and philosophy highlighting the requirement to take groups, social relations and broader socio-cultural contexts into account.

**Keywords:** Privacy, Contextual integrity, Autonomy, Liberalism, Sociotechnical context

*This article belongs to [Concepts of the digital society](https://policyreview.info), a special section of* Internet Policy Review *guest-edited by Christian Katzenbach and Thomas Christian Bächle.*

# PRIVACY: DEVELOPMENTS AND CONTESTATIONS

Delivering a consolidated account of privacy, even when narrowing down the focus on its informational dimension, is not an easy task given the complexity of the issue; and the vast landscape of theoretical work referring to the concept (Roessler, 2005; Solove, 2009; Nissenbaum, 2010). Nevertheless, the notion of privacy plays a central role in public as well as in scholarly controversies about the multiple transformations accompanying the advent of 'digital society'. Since privacy is implicated in one of the most basic distinctions pervading modern society, namely the distinction between the private and the public (e.g., Bobbio, 1989), it may be understood as an analytical 'probe head' potentially providing insights into the digital transformation of society at large. This entails that current developments of privacy regarding digital technology cannot be understood without considering the larger socio-historical currents that still structure practices and concepts of privacy. In consequence we will firstly present a sketch of the general outlines of this multi-layered notion, which particularly highlights the role that technologies have been playing for privacy from the very beginning. Having gained an overview, we will next briefly introduce some particularly 'digital challenges' of privacy, before moving on to a presentation of conceptual innovations having been developed by privacy scholars in response.

We may first of all note that, although some scholars have traced privacy in the most diverse geographical and historical formations (Moore, 1984) we will restrict our discussion to the modern phase of the historical West.[1] Thus, although in medieval Europe the idea and practice of keeping secrets was well-known and widespread (Assmann and Assmann, 1997) framing these practices as a *positive* institution occurs only in the post-*Ancien Régime* era: the idea of privacy as an ethical or legal right emerges with the rise of bourgeois societies in Europe. Not only does the decline of the court society (Elias, 1983) demand actors to develop novel subjectification schemes, there are also new forms of architecture and interior design that include a sense of more or less public/private rooms, e.g., the salon vs the bedroom and, for the well-off: the study (Vincent, 2016). Moreover, novel cultural techniques emerge, such as letter-writing and -sending through the novel postal system (Siegert, 1993), and diary-keeping (Koschorke, 1999), which are considered constitutive elements of the Enlightenment idea of a self-reflecting, and thus autonomous subject (Ruchatz, 2003; Rössler, 2017). Kant famously builds his claim that every human being is capable of using his own understanding by experiencing a scholarly "reading world" that publishes and discusses educated writings (Kant, 1996). Here, autonomy is tied to public exchange whereas private occupations may be limited in all kinds of regards.

In this sense, privacy, understood as a practice to forge subjectivities of self-determination emerges in an early bourgeois societal setting; and is right from the outset strongly linked to the materiality and socio-technology of its environment. It is for this reason that media and technological inventions from the 18th century onwards have constantly spurred both public debates on, and theoretical developments of, privacy. In fact, one of the most influential legal definitions of privacy, Warren and Brandeis' conceptualisation of privacy as the "right to be let alone" (Warren and Brandeis, 1890) was motivated by the emergence of instantaneous photography and the yellow press (Glancy, 1979). Nevertheless, while privacy 'is' as technological as its transformation, there is no technological determination of either aspect.

Apart from its cultural and material character, privacy has also always been 'normative', and massively contested for that matter. It has been challenged by social movements, such as

feminist (Cohen, 2004) and queer activism (Gross, 1993) in particular, as well as by more conceptual enterprises, e.g., feminist (Allen, 2003; Cohen, 2012) and communitarian (Etzioni, 1999) social theory, critical theory and other strands of Marxist thought (Althusser, 2014), surveillance studies (Stalder, 2002), media studies (Osucha, 2009), legal theory (Roberts, 1996) and so on. To illustrate the contested nature of the concept we will sketch the outline of two groups of issues that are of particular importance for understanding privacy in digital societies.

*Privacy: enabling individuality vs de-politicising issues*: 'Advocates' value privacy as a 'space' where people can act without public scrutiny, and hence claim its importance for personal development: a 'space' for trying out things, for making 'mistakes' without too many consequences, etc. (Rössler, 2005, p. 144). They hold that, while societies are structured by power imbalances and the stigmatisation of both morally and legally permissible acts, privacy allows for practices to be performed and to prevail in spite of their stigmatisation. At the same time, however, critics argue that this is precisely what may become problematic, for the possibility to evade public visibility may turn into a necessity to hide: if controversial actions are restricted to the private realm, social change is stifled. Emancipatory politics quite in contrast involve public acknowledgement of issues as political ones concerning all of society (Arendt, 1970; Rancière, 1999). The relevance, or existence of, a social problem, is hard to press publicly if those being concerned are hidden in privacy. This issue forms an important context for current debates. Otherwise, digital technology is too easily conceived as a threat to privacy rather than a shift within an already ambivalent and complex relation. Similarly, without the focus on (de-)politicisation the endorsement of a more publicly visible digital life is too easily denigrated as naïve or lacking in autonomy. We return to these issues below.

*Privacy as disavowal of social contexts:* The notion of privacy, as discussed in this contribution, emerges with bourgeois society; and the latter's idea of autonomous individuals is based on a negative conceptualisation of freedom (Berlin, 2017). From this point of view, social contexts and interactions count as *limitations* to freedom, as the interests of others have to be taken care of. In private, that is, in the absence of others, such infringements are likewise absent; consequently freedom increases. Again, feminist thinkers have taken issue with such a perspective in arguing that in privacy, actually others *are* present: family, houseworkers, etc. Those others take care of providing food, organising space, they contribute emotional labour and do reproductive and care work in general, all of which enables the absence from pressing needs and demands that we cherish as privacy in the first place. In this sense, autonomy is not the absence, but the presence, of others whose contributions to one's social positioning is neglected. As subjectivity is a relational affair (Friedman, 2003; Nedelsky, 1989), the same goes for subjectivities of self-determination. As a result, the latter relates to, and at times contradicts, the valuation of others. This inherent relationality of privacy is particularly salient in recent debates and theoretical innovations for privacy in digital societies. Thus, the normative and socio-political issues sketched here form a second important context for current issues.

Both these groups of issues illustrate that privacy is to be discussed as an inherently ambivalent value. As a value it forms part of a broader societal framework of related or contravening values that are subject to constant negotiation. Moreover, most scholars one way or another do admit to its 'downsides' by granting the necessity of constraining privacy in certain cases etc., while at the same time arguing for privacy's great individual and social value.

However, what is this "individual and social value"? Regarding the former there is one group of normative theories that sees privacy's value rooted in autonomy. From this point of view, privacy is required to lead an autonomous life (Roessler, 2005). The argument pertains to both

'situations' and biographies. Under involuntary public scrutiny, the argument goes, we could not act freely. Furthermore, without privacy we could not even develop an individual character, try out things or commit errors (Reiman, 1976). Here privacy is not considered an end in itself; rather, its individual value is to be found in its being a precondition for the fostering of autonomy. A second group of theories locates privacy's value not in individuals but in societal structuring. Authors belonging to this group argue that privacy is a precondition for democratic institutions, such as elections (Regan, 1995; De Hert and Gutwirth, 2006); and is furthermore a requirement of democratic society as it enables a plurality of life forms (Roessler, 2010). Obviously, such reasoning points out privacy's potential to enable individual decisions as to how one wants to lead her life; liberal-democratic ideas, are central to classic privacy theorising, as the concept was connected to the notion of "freedom" already in mid-twentieth century privacy discourse (Westin, 1967).

In our general discussion of the concept we have thus far carved out three characteristics of privacy: its historical and cultural shaping; its material forming/transforming; and its societal contestation. What we have not touched upon so far are debates of how to define privacy. To cope with this task, we will begin by pointing out the multiple dimensions of privacy. Some scholars distinguish, e.g., informational from local and decisional privacy (Roessler, 2005), and thus knowledge related from spatial and decision-making aspects. Some theorists add still more dimensions, such as bodily and psychological privacy (Tavani, 2007), plus intellectual, communicational, associational, proprietary, and behavioural privacy with informational privacy "overlapping" all the other types of privacy (Koops et al., 2016). There are two things to note at this point: first, no matter how many dimensions any privacy theory is inclined to take into account, most or at least some of those accounted for, are only analytically distinguishable, but not so in empirical practice. This is illustrated by the trivial fact that in some circumstances closing the door might grant actors not only spatial privacy (a room for their own), but also informational (e.g., knowledge about what's going on inside) as well as bodily privacy (e.g., romantic activities). In line with these considerations Roessler (2005, p. 87) argues that bodily privacy may be realised via spatial and decisional privacy. Considering the US Supreme Court ruling in *Roe vs Wade,* where the court introduced a legal right to decisional privacy and consequently stated that abortion is a private affair, we may infer that here decisional privacy is a precondition to bodily privacy (Cohen, 2004) – in fact, both are inextricably entangled.

It is for this reason that in this contribution we set out to discussing privacy in general, for informational privacy in digital society is intimately connected with the dimensions and genealogies of all the other privacies that can be distinguished only for analytic purposes. The entangled nature of privacy furthermore complicates, or in fact, renders impossible, its clear-cut definition. Historians have attempted to retrace privacy's genealogy back to the notion of private property (Vincent, 2016),2 which currently re-emerges in attempts to implement data protection via a right of data ownership (Hornung and Goeble, 2015), while for other researchers privacy refers to some kind of inaccessibility, protection, shielding, or limiting of the possibilities for others to interact. A central debate in philosophy and legal theory concerns the question of whether privacy is about being inaccessible for others in some way – or about the possibility to *control* that access (DeCew, 1997; Fried, 1968; Parent, 1983). However, those long-standing discussions have not quite settled the dispute, but driven some influential scholars to rather conceive of "privacy" as the name given to the "family resemblance" of a set of practices (Solove, 2009); or to straightforwardly detach privacy from individuals and conceptualise it as a fit between information flows and appropriate social contexts (Nissenbaum, 2010).

In this paper we will not be able to provide the clear-cut definition privacy studies are lacking...

since their establishment more than hundred years ago. In fact, as we turn to the specific challenges for privacy in digital societies below, we will see that they entail shifts and re-conceptualisations among the various aspects of privacy, rather than developments that could be scrutinised from the perspective of a clear-cut definition.

Contemporary digital transformations profoundly destabilise this notion of privacy by shifting the material-technological base of society, and thus, of privacy. As a result, the normative contestation of privacy comes to the forefront again, and the precariously balanced relationship between privacy and other values gets into disorder. We will next demonstrate how this comes about by illustrating the digital challenge of privacy before specifying the way these challenges transform privacy in a networked age.

## PRIVACY IN THE DIGITAL SOCIETY: EXISTING THEORIES AND CHALLENGES

Digital technology troubles not only the informational realm, but affects other dimensions of privacy as well. For instance, when considering information related to activities within private space we may note that most people still believe such information was only accessible by third parties if actively passed along, or when third parties are granted physical access. However, given today's devices, such as smartphones or "smart speakers", we must account for imperceptible listening or watching also within private space (Ochs, 2017).

This is just one example for the way social digitisation transforms the groundwork of sociality. We will elaborate two aspects of this transformation in order to show how well-worn notions of privacy lose plausibility at least to account for the novel socio-technical situations emerging within digital society: the massive extension of the scope of perceptibility and action, on the one hand; and the uber-individuality of the resulting privacy problematics. Taking up the first point, we may set out from the observation that digital technologies shift the possibilities and boundaries of human perception and action; and that, as a result, normative questions emerge triggered by novel forms of action. A case in point is the apparently paradoxical notion of "privacy in public". Persons in public, one might argue, cannot reasonably expect privacy, for they are visible to everybody. Indeed, this has been a longstanding legal and theoretical point of view (Nissenbaum, 1998). However, "everybody" here implicitly means everyone who is present *where I am*. Thus, when I sit in a public park, everyone who happens to be in the same area is able to see and approach me. Social stratification of cities and quarters further reduces the selection of people who might possibly do so in the first place. However, with people now having gained the means to take pictures or videos of the park and to upload them to the internet, the implied notion of "everybody" changes drastically: suddenly, the park-wide audience is replaced by a potentially world-wide audience. This raises the question of whether we actually should have a right to privacy regarding that newly extended audience (Nissenbaum, 1998), especially when taking into account the dangers that using an established notion of privacy in the context of new possibilities of action and perception might have as was demonstrated by Zimmer (2010) for the case of research. The increased reach of perception and interaction through digital technology that becomes visible here is augmented by two oft-cited factors: first, digital data is easy and cheap to store, thus things that appear in data acquire permanence as digital records. Combined with effective search engines and machine learning, vast troves of data can efficiently be queried. Such developments have led to the claim for a right to be forgotten (Frantziou, 2014) that is, a claim to legal guarantees that target the longevity of data by limiting the scope of search procedures.[3] The second factor is the vast increase of sensors, for example by the proliferation of smartphones or so called "internet of things" devices, leading to a circumspect source of digital data in our vicinities (Ziegeldorf et al., 2014).

The second aspect of digitisation for privacy that we would like to invoke is that it troubles the inherent individualism of conventional privacy theories. Such individualism is also central to most data protection legislation like the European Union General Data Protection Regulation, which relies on the notion of personal data, personally identifiable information or similar concepts.4 All of them express a clear relation between particular bits of data and specific subjects. A similar individualism can be found in most theories of privacy that relate the latter to an individual value, particularly to autonomy. This of course includes autonomy regarding one's communication, information about oneself or one's self-presentation (Roessler, 2005). However, digital data tends to be relational, e.g., information about communication processes. Furthermore, the bulk of data collected nowadays is analysed on an aggregate level. The issue is not about specific pieces of information concerning particular persons, but rather about finding new behavioural patterns (Chun, 2016). Such data analytics technologies, often discussed under the label of "Big Data" or "Machine Learning", do not disclose who you are but what you are like (Matzner, 2014). Emerging patterns are then used for all kinds of ends like credit scoring (Gandy, 2012), social sorting (Lyon, 2014), security procedures like algorithmic profiling (Leese, 2014), border controls (Jeandesboz, 2016) and many more purposes. Thus, the type of data that data protection schemes and individual notions of privacy enable us to control (personal data) and the types of data that render some corporate actors immensely powerful (aggregate/patterns of data) are not the same.

In a certain sense, privacy's contestations identified above are reoccurring here, albeit in a different form: the imperceptibility of the listening and watching within private space, as induced by the digitally increased reach of perceptibility, hides the underlying socio-technical networks challenging privacy (Stalder, 2002; Fuchs, 2011; Lyon, 2015). The socio-technical dependency of the practices constituting digital society remains thus invisible; consequently, it is extremely difficult to break the de-politicising grip of the whole constellation, for collective risks (e.g., digitally induced decline of democracy) remain extremely abstract, while individual risks are hardly felt at all. Individualistic privacy notions tend to aggravate the problematic, for framing the latter in individualistic terms de-politicises the issue right from the outset, and furthermore conceals the social dependency of the whole constellation on users' "invisible work" (Leigh Star and Strauss, 1999).

The summary offered above shows that the challenges of digital society by far exceed a narrow definition of privacy as informational privacy; and even more so the equation of privacy with data protection. In particular, they trouble the individualist notions of privacy which are also at the core of much national privacy laws as well as the European Union General Data Protection Regulation. They moreover unsettle deep-seated ideas and practices by changing perception, communication and social relations, all of which impact the various aspects or dimensions of privacy. However, there have been several theoretical innovations regarding privacy in the last twenty years that either are directly prompted by the aforementioned issues or allow to address them. We will next turn to these innovations.

## PRIVACY IN DIGITAL SOCIETY: THEORETICAL INNOVATIONS

Already in the 1970s, probably most famously voiced in Rachels' paper (1975), theories of privacy have turned away from equating the private subject with being "let alone". Particularly in the wake of Goffman's work (1959, 1977) subjects are seen as playing various roles in different social contexts. From this perspective, privacy still protects some kind of individual autonomy, as it now concerns the individual's potential to determine the information to be disclosed in any one context. There are some relations that warrant knowledge of particular pieces of information or certain forms of interaction, while the same information is to be protected in

others. Since Goffman and his successors have shown that our roles have to conform to all kinds of social expectations, which are in turn tied to power, resources and other forms of inequality, the right to privacy grants persons a claim to self-determination within these relations. In normative terms the protected autonomy of the sovereign individual gives way to the autonomy to perform identity management.

This point of view has become prevalent in the analysis of digital society. The first group of challenges mentioned above entails that different social contexts and their ensuing roles are no longer clearly separated. Thus, in addition to protecting one's information within such contexts, the latter must be protected in relation to each other. This problematic has been studied under the topic of "context collapse" in the social sciences and in media studies. In particular, social networking sites are designed to interconnect different social contexts in which we lead our social lives. Thus, information which may be voluntarily disclosed in one context and with a particular audience in mind, is now easily transported to other contexts where this might entail harm (Marwick and boyd, 2014; Wesch, 2009). This analysis is important because it counters a particular version of the de-politicising problem mentioned earlier: information that is released to adverse effects in digital media often has been voluntarily provided elsewhere. Putting the blame on the individual's original release in a specific context, however, ignores the social, cultural and technical interrelations between different contexts as a political issue. This is exemplified by former Google CEO's infamous 2009 statement that "If you have something you don't want anyone to know, maybe you shouldn't be doing it in the first place" (Esguerra, 2009), which completely lost sight of the fact that the appropriateness of disclosing information about one's doings in complex societies is not binary (disclosure/non-disclosure) but largely determined by differentiated contextual norms. Such blaming becomes particularly questionable when regarding young persons or gendered forms of interaction like non-consensual image sharing. Here the reduction of privacy issues to individual acts connects to other forms of blaming the victim (Henry and Powell, 2014; Ringrose, Harvey, Gill, and Livingstone, 2013).

For similar reasons, (Roessler and Mokrosinska, 2013) argue that individual privacy needs to be amended with the protection of social relations. Without such protection, the desired or required activities in these relations become defective. Recently, in particular German scholarship has radicalised this move. Rather than maintaining individual control over social relations at the core of privacy theories, critics argue that the subject whose privacy is protected needs to be understood in a more socially and/or technically embedded manner. This shifts the normative core from autonomy in the form of identity management towards particular possibilities to negotiate social positions. While there are some hints to this approach in Roessler and Mokrosinska (2013), they are still more pronounced in recent theoretical proposals that build firmly on a variety of social theories like critical theory (Seubert and Becker, 2018; Loh, 2018; Stahl, 2016), structuration theory and actor-network theory (Ochs, in press), or Arendtian political theory (Matzner, 2018).

In distinction to such approaches that see the individual value of privacy in a social context, other theorists locate the value of privacy itself on a social level. The approaches of Ochs (in press), Seubert and Becker (2018), and Stahl (2016) fuse both outlooks. Probably the most prominent approach from the latter group is Helen Nissenbaum's idea of "privacy in context" (Nissenbaum, 2010). She argues that society is divided into particular spheres, like healthcare, education, etc. All of these spheres, she explains, are defined by intrinsic values, e.g., healthcare by healing and sanity. In consequence, Nissenbaum concludes that each of these contexts is governed by norms regarding the use and circulation of information; said norms derive in turn

from the respective intrinsic aim of any given context. Accordingly, privacy in Nissenbaum's definition is tantamount to treating each piece of information according to the norms that govern the context in which it emerged. That need not entail that all information stay in the original context of emergence, as is sometimes mistakenly stated. It rather requires that all applications and flows of data must respect the fact that any data whatsoever is gathered in a particular context for a particular aim, which does not necessarily warrant the use of the same data for other aims. According to Nissenbaum it is therefore not straightforward to assume that data released in one context is "up for grabs" in another. However, the aggregate and relational use of data particularly challenges the presumed separation of contexts (Matzner, 2014). Specifically the organisation of contemporary digital services in platforms (Bucher and Helmond, 2017) blurs such distinctions. Still Nissenbaum's approach has been very influential, not the least because it has also been designed with deployment in mind. With its rather formal treatment of norms and contexts it has led to productive engagement and implementation in computer science (Benthall, Gürses, and Nissenbaum, 2017).

Quite generally, the challenges posed by privacy have led to innovations in computer science. Notions such as differential privacy (Dwork, 2008) or k-anonymity (Machanavajjhala, Kifer, Gehrke, and Venkitasubramaniam, 2007) acknowledge the importance of aggregate data, and in consequence that the meaning of a piece of data depends on the context in which it is evaluated. In this sense, these approaches define measures to determine the amount of information that can be derived about a person in the context of a specific data-base or other collection of data. Still, they are focused on privacy as prevention gathering information about a person, rather than preventing certain actions performed on this person.

This latter observation leads to recent debates on the question of regulating the usage instead of the collection of data, which so far have not born too many fruits. Instead of delving into this discussion we would like to flag the fact that the digital unsettling of privacy also at this point generates the requirement to conceptualise privacy as embedded within the sociotechnical structures of digital society. Privacy is linked up with all kinds of values, norms, institutions, and practices constituting the political economy from which it emerges – losing sight of the latter in theory breeds faint privacy notions in practice.

## CONCLUSION

Privacy has become a pervasive issue in digital societies – in political, economic, and academic discourse as well as in everyday life of many. This is not surprising, since digital technologies challenge many established notions and practices related to the concept. However, this must not be understood as a recent attack on a hitherto unproblematic value. As we have seen, a lot of the transformations under way connect to the conceptual, socio-material and cultural history of privacy. In this regard, the digital transformation sustains and adds to existing critiques from feminist and social perspectives. At the same time, digital transformations and the many privacy-related incidents it causes highlight the urge to find re-conceptualisations that sustain its value. In navigating this tension research from computer science to the social sciences and law, and philosophy have highlighted the necessity to take groups, social relations and broader socio-cultural contexts into account. Such developments of privacy can also be seen as part of existing efforts to reconceive core tenets of liberal societies in a more socio-culturally situated manner (Friedman, 2003; Roessler and Morkosinska, 2013). At the same time, strands of social and political theory beyond liberalism (understood in its broadest sense), which so far have often been rather critical towards privacy are increasingly harnessed to find novel solutions to

the digital challenge of privacy. As such, this short overview has described a concept as much as a process that doubtlessly must, and hopefully will continue in the future.

## REFERENCES

Allen, A. L. (2003). *Why Privacy Isn't Everything: Feminist Reflections on Personal Accountability*. Lanham: Rowman & Littlefield.

Althusser, L. (2014). *On the Reproduction of Capitalism: Ideology and Ideological State Apparatuses*. London: Verso.

Arendt, H. (1970). *On violence*. New York: Harcourt, Brace & World.

Arendt, H. (1998). *The Human Condition* (2nd ed.). Chicago: University of Chicago Press.

Assmann, A., & Assmann, J. (1997). *Geheimnis und Öffentlichkeit* [Secret and Public]. München: Fink.

Bhandar, B. (2014). Critical Legal Studies and the Politics of Property. *Property Law Review*, *3*(3), 186–194.

Benhabib, S. (2003). *The reluctant modernism of Hannah Arendt*. Lanham: Rowman & Littlefield.

Benthall, S., Gürses, S., & Nissenbaum, H. (2017). Contextual Integrity through the Lens of Computer Science. *Foundations and Trends in Privacy and Security*, *2*(1), 1–69. doi:10.1561/3300000016

Berlin, I. (2017). Two Concepts of Liberty. In D. Miller (Ed.), *The Liberty Reader* (pp. 33–57). London: Routledge. doi:10.4324/9781315091822-3

Bobbio, N. (1989). *Democracy and Dictatorship: The Nature and Limits of State Power*. Minneapolis: University of Minnesota Press.

Bucher, T. and Helmond, A. (2017). The affordances of social media platforms. In J. Burgess, A. Marwick, & T. Poell (Eds.), *The SAGE handbook of social media* (pp. 223–253). London: Sage.

Chun, W. H. K. (2016). *Updating to remain the same: habitual new media*. Cambridge, MA: The MIT Press.

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

Cohen, J-L. (2004). *Regulating intimacy: a new legal paradigm*. Princeton, NJ: Princeton University Press.

DeCew, J. W. (1997). *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithaca: Cornell University Press.

Dwork, C. (2008). Differential Privacy: A Survey of Results. In M. Agrawal, D. Du, Z. Duan, & A. Li (Eds.), *Theory and Applications of Models of Computation* (pp. 1–19). doi:10.1007/978-3-540-79228-4_1

Elias, N. (1983). *The Court Society*. Oxford: Blackwell.

El Guindi, F. (1999). *Veil: modesty, privacy, and resistance*. Oxford; New York: Berg.

Esguerra, R. (2009). Google CEO Eric Schmidt Dismisses the Importance of Privacy. Retrieved from Deeplinks Blog: https://www.eff.org/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy

Ess, C. (2005). "Lost in Translation"?: Intercultural Dialogues on Privacy and Information Ethics (Introduction to Special Issue on Privacy and Data Privacy Protection in Asia). *Ethics and Information Technology*, *7*(1), 1–6. doi:**10.1007/s10676-005-0454-0**

Etzioni, A. (1999). *The Limits of Privacy*. New York: Basic Books.

Fuchs, C. (2011). Towards an alternative concept of privacy. *Journal of Information, Communication and Ethics in Society*, *9*(4), 220–237. doi:**10.1108/14779961111191039**

Frantziou, E. (2014). Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos. *Human Rights Law Review*, *14*(4), 761–777. doi:**10.1093/hrlr/ngu033**

Fried, C. (1968). Privacy. *The Yale Law Journal*, *77*(3), 475–493.

Friedman, M. (2003). Autonomy and Social Relationships: Rethinking the Feminist Critique. In *Autonomy, Gender, Politics* (pp. 81–97). Oxford: Oxford University Press.

Gandy, O. H. (2012). Statistical Surveillance: Remote Sensing in the Digital Age. In K. H. Kirstie Ball & D. Lyon (Eds.), *Handbook of Surveillance Studies* (pp. 125–132). New York: Routledge.

Glancy, D. J. (1979). The Invention of the Right to Privacy. *Arizona Law Review*, *21*(1), 1–39. Available at https://digitalcommons.law.scu.edu/facpubs/317/

Goffman, E. (1959). *The presentation of self in everyday life*. New York: Doubleday.

Goffman, E. (1977). *Relations in public: microstudies of the public order*. New York: Harper & Row.

Gross, L. P. (1993). *Contested closets: the politics and ethics of outing*. Minneapolis: University of Minnesota.

De Hert, P., & Gutwirth, S. (2006), Privacy, data protection and law enforcement: opacity of the individual and transparency of power. In E. Claes, S. Gutwirth, & A. Duff (Eds.), *Privacy and the Criminal Law* (pp. 61–104). Antwerp: Intersentia.

Henry, N., & Powell, A. (2014). Beyond the 'sext': Technology-facilitated sexual violence and harassment against adult women. *Australian & New Zealand Journal of Criminology* 48(1), 104–118. doi:**10.1177/0004865814524218**

Hornung, G., & Goeble, T. (2015). „Data Ownership" im vernetzten Automobil. *Computer Und Recht*, *31*(4), 265–273. doi:**10.9785/cr-2015-0407**

Jeandesboz, J. (2016). Smartening border security in the European Union: An associational inquiry. *Security Dialogue*, *47*(4), 292–309. doi:**10.1177/0967010616650226**

Kant, I. (1996). An Answer to the Question: What is Enlightenment? In J. Schmidt (Ed. & Trans.), *What is Enlightenment? eighteenth-century answers and twentieth-century questions* (pp. 58–65). Berkeley: University of California Press.

Koschorke, A. (1999). *Körperströme und Schriftverkehr: Eine Mediologie des 18. Jahrhunderts* [Body currents and written correspondence: a mediology of the 18th century]. München: Fink.

Leese, M. (2014). The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union. *Security Dialogue*, *45*(5), 494–511. doi:**10.1177/0967010614544204**

Leigh Star, S., & Strauss, A. (1999). Layers of Silence, Arenas of Voice: The Ecology of visible and Invisible Work. *Computer Supported Cooperative Work*, *8*(1–2), 9–30. doi:**10.1023/A:1008651105359**

Loh, W. (2018). A Practice–Theoretical Account of Privacy. *Ethics and Information Technology*, *20*(4), 233–247. doi:**10.1007/s10676-018-9469-1**

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, *1*(2). doi:**10.1177/2053951714541861**

Machanavajjhala, A., Kifer, D., Gehrke, J., & Venkitasubramaniam, M. (2007). L-diversity: Privacy beyond k-anonymity. *ACM Transactions on Knowledge Discovery from Data*, *1*(1). doi:**10.1109/ICDE.2006.1**

Marmor, A. (2015). What Is the Right to Privacy? *Philosophy & Public Affairs*, *43*(1), 3–26. doi:**10.1111/papa.12040**

Marwick, A. E., and boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*(7), 1051–1067. doi:**10.1177/1461444814543995**

Matzner, T. (2014). Why privacy is not enough privacy in the context of "ubiquitous computing" and "big data". *Journal of Information, Communication and Ethics in Society*, *12*(2), 93–106. doi: **10.1108/JICES-08-2013-0030**

Matzner, T. (2018). Der Wert informationeller Privatheit jenseits von Autonomie [The value of informational privacy beyond autonomy]. In S. Burk, M. Hennig, B. Heurich, T. Klepikova, M. Piegsa, M. Sixt, & K. E. Trost (Eds.), *Privatheit in der digitalen Gesellschaft* (pp. 75–94). Berlin: Duncker & Humblot.

Moore, B. (1984). Privacy: Studies in social and cultural history. Armonk; London: M.E. Sharpe, Inc.

Nedelsky, J. (1989). Reconceiving Autonomy: Sources, Thoughts and Possibilities. *Yale Journal of Law & Feminism*, *1*(1), 7–36. Retrieved from https://digitalcommons.law.yale.edu/yjlf/vol1/iss1/5/

Nissenbaum, H. (1998). Protecting privacy in an information age: The problem of privacy in public. *Law and Philosophy*, *17*(5–6), 559–596. doi:**10.2307/3505189**

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford: Stanford Law Books.

Ochs, C. (in press). Privacies in Practice. In U. Bergermann, M. Dommann, E. Schüttpelz, & J. Stolow (Eds.), *Connect & Divide. The Practice Turn in Media Studies*. Zürich: Diaphanes.

Ochs, C. (2017). Rechnende Räume. Zur informationellen Transformation räumlicher

Privatheiten [Spaces that compute. On the informational transformation of spatial private spheres]. In A. Henkel, H. Laux, & F. Anicker (Eds.), *Zeitschrift für Theoretische Soziologie: Sonderband 4. Raum und Zeit: Soziologische Beobachtungen zur gesellschaftlichen Raumzeit* (pp. 188–211). Weinheim; Basel: Beltz.

Osucha, E. (2009). The Whiteness of Privacy: Race, Media, Law. *Camera Obscura*, *24*(1), 67–107. doi:**10.1215/02705346-2008-015**

Parent, W. A. (1983). Privacy, Morality, and the Law. *Philosophy & Public Affairs*, *12*(4), 269–288. Retrieved from **https://www.jstor.org/stable/2265374**

Pateman, C. (1988). *The Sexual Contract*. Stanford: Stanford University Press.

Rachels, J. (1975). Why Privacy is Important. *Philosophy & Public Affairs*, *4*(4), 323–333. Retrieved from **https://www.jstor.org/stable/2265077**

Rancière, J. (1999). *Disagreement: politics and philosophy*. Minneapolis: University of Minnesota Press.

Regan, P.M. (1995). *Legislating Privacy*. Chapel Hill: University of North Carolina Press.

Reiman, J. H. (1976). Privacy, Intimacy, and Personhood. *Philosophy & Public Affairs*, *6*(1), 26–44. Retrieved from **https://www.jstor.org/stable/2265060**

Ringrose, J., Harvey, L., Gill, R., & Livingstone, S. (2013). Teen girls, sexual double standards and 'sexting': Gendered value in digital image exchange. *Feminist Theory*, *14*(3), 305–323. doi:**10.1177/1464700113499853**

Roberts, D. E. (1996). Punishing Drug Addicts Who Have Babies: Women of Color, Equality, and the Right of Privacy. In K. Crenshaw, N. Gotanda, G. Peller, & K. Thomas (Eds.), *Critical Race Theory – The Key Texts that Formed the Movement* (pp. 384–426). New York: The New Press.

Roessler, B., & Mokrosinska, D. (2013). Privacy and social interaction. *Philosophy & Social Criticism*, *39*(8), 771–791. doi:**10.1177/0191453713494968**

Rössler, B. (2005). *The Value of Privacy*. Cambridge: Polity.

Rössler, B. (2017). *Autonomie: ein Versuch über das gelungene Leben* [Autonomy: a conjecture on successful life] (2nd Edition). Berlin: Suhrkamp.

Ruchatz, J. (2013). Vom Tagebuch zum Blog. Eine Episode aus der Mediengeschichte des Privaten [From the diary to the blog. An episode in the media history of the private]. In Stefan Halft & Hans Krah (Eds.), *Privatheit. Strategien und Transformationen*. Passau: Karl Stutz.

Seubert, S., & Becker, C. (2018). Verdächtige Alltäglichkeit. Sozialkritische Reflexionen zum Begriff des Privaten [Suspicious banality. Socially critical reflections on the concept of the private]. *Figurationen*, *19*(1), 105–120. doi:**10.7788/figurationen-2018-190111**

Siegert, B. (1993). *Relais: Geschicke der Literatur als Epoche der Post* [Relays: The fates of literature as the era of mail]. Berlin: Brinkmann & Bose.

Stalder, F. (2002). Privacy is not the Antidote to Surveillance. *Surveillance & Society*, *1*(1),

120–124. doi:**10.24908/ss.v1i1.3397**

Stahl, T. (2016). Indiscriminate Mass Surveillance and the Public Sphere. *Ethics and Information Technology* 18(1), 33–39. doi:**10.1007/s10676-016-9392-2**

Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy*, *38*(1), 1–22. doi:**10.1111/j.1467-9973.2006.00474.x**

Vincent, D. (2016). *Privacy: a short history*. Cambridge; Malden, MA: Polity.

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193–220. doi:**10.2307/1321160**

Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum.

Wesch, M. (2009). Youtube and you: Experiences of self-awareness in the context collapse of the recording webcam. *Explorations in Media Ecology*, *8*(2), 19–34. Available at https://core.ac.uk/download/pdf/5170117.pdf

Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks*, *7*(12), 2728–2742. doi:**10.1002/sec.795**

Zimmer, M. (2010). But the data is already public: on the ethics of research in Facebook. *Ethics and Information Technology*, *12*(4), 313–325. doi:**10.1007/s10676-010-9227-5**

**FOOTNOTES**

**1.** While there are regulations and norms regarding visibility or spatial access in many cultures (e.g., in Middle Eastern Muslim countries, see El Guindi, 1999; or Confucian traditions, see Ess, 2005) that resemble central European privacy practices, great care has to be taken comparing these. To avoid lengthy discussion of this issue we take an agnostic stance here and restrict our treatment to the 'historical West'.

**2.** This normative and conceptual legacy of private property has been examined critically only recently, for example Bhandar has shown that having property and being able to appropriate has been an essential element in the emergence of liberal political subjectivity, which was particularly visible in the colonies (Bhandar, 2014).

**3.** It has to be added though, that reliable long-term storage of data (where it is desired) is a complex problem.

**4.** Arguing from "an European point of view" we narrowly focus on the EU GDPR here.