Privacy and/in the Public Sphere

Roessler, B.

DOI
10.1515/yewph-2016-0021
Publication date
2016
Document Version
Final published version
Published in
Yearbook for Eastern and Western Philosophy

Beate Roessler (Amsterdam)

19 Privacy and/in the Public Sphere

Abstract: Talking about privacy in the public prima facie seems to be a contradiction: why should privacy have to play a role within the public sphere? What could possibly be private in the public? However, quite a number of theories of privacy conceptualize privacy as a protective shield which we carry with us wherever we are: respect for privacy in public then means, for instance, not listening in on private conversations between friends on the street or in a cafe. The most important form of privacy in public, however, which has gained a lot of attention during the last decade or so, is privacy as anonymity: the form of privacy in the public sphere, online as well as offline, which means invisibility, non-traceability, not being identifiable as an individual person. Theories of privacy differ as to the possibility as well as to the desirabilty of anonymity in public contexts, online as well as offline.

In my paper, I investigate the complicated relations between privacy, anonymity, and the public sphere. I will, firstly, clarify the conceptual relation between privacy and anonymity, drawing on theories which define privacy in terms of (contextually varying) conditions enabling individual freedom and autonomy. I will also review some normatively relevant differences between the online and the offline world. In the second part, I will discuss possible normative conflicts between a moral or legal right to privacy and anonymity, and considerations of security, accountability, or moral responsibility. One of the important questions will concern the ethical consequences of the technical possibilities of identification and de-anonymization in the online world.

Introduction

Talking about privacy in public seems to involve a contradiction: what role should privacy play *in* the public sphere, when it actually constitutes the counterpart to the public sphere? Although some theorists – such as William Parent (Parent 1983) – reject the idea of the protection of privacy in the public, a range of theories of privacy endeavour to show that privacy is not to be conceptualized as a spatial sphere, in contrast to the sphere of the public, but rather as a kind of protective shield that we always carry with us, regardless of where we are – and thus also in the public realm. This can be understood when we consider that one does not listen in on but rather tries to ignore conversations at a neighbouring table in a cafe, or when we refrain from commenting on the conspicuous behaviour of others

DOI 10.1515/YEWPH-2016-0021

on the street. This is a form of respect for the privacy of others in public, a form that Goffman once described as "civil inattention" (Goffman 1959; Nagel 2002).

Another form of privacy in public that has increasingly come to the fore of discussions in recent years is privacy as *anonymity*: the idea here is that one can best protect one's own personal privacy in relation to strangers, to unspecified others, when one is nameless, not identifiable or traceable as a particular person, both in the offline and in the online world. Theories of privacy can be differentiated with regard to the question of how strongly a demand for anonymity of this kind can be justified and what exactly the relationship between privacy and anonymity is (cf. Kerr et. al. 2009; Marx 1999). In the following, I shall clarify more precisely the relation between privacy and anonymity and in doing so also consider possible conflicts between privacy and anonymity on the one hand and other rights or values such as societal security on the other hand.

I will thus first (I) say something more general about the concept of privacy and the relation between individual privacy, freedom, and autonomy. In doing so, I will also address the various dimensions of individual privacy and say a few words about the case law, at least in the EU. In a second step (II), I will explain the significance of privacy in public more precisely and discuss the concept of anonymity. Following an analysis of legal, moral and conceptual aspects, in a final step (III) I will examine possible problems and conflicts: between anonymity and freedom of expression and freedom of the press; between anonymity and security; and between anonymity and the freedoms of the free market.

1 The Concept of Privacy

The concept of privacy can be contrasted with that of the public in various ways: as the private sphere of the household in contrast to the publicity of society; as the liberal basic idea of individual freedom in contrast to state interventions; and, thirdly, as protection of information over a person from being illegitimately collected and disseminated (Weintraub 2007; Nissenbaum 1999). In the history of philosophy, the dichotomy between the public and the private has not only been described in very different ways but has repeatedly been criticized, by feminist philosophers as well as, for instance, by Hannah Arendt. Since my interest in this article is ultimately directed towards the private *in* public I will in the following primarily take the second and third of the outlined differentiations as a basis for discussion: the private as the space of freedom vis-a-vis the state in liberal-democratic societies; and the private as privacy of information as opposed to public information. The sphere of the private household will only be addressed very briefly.

Since the beginning of the more recent discussions on privacy, the focus has been on an individual right to privacy, its protection and its justification. This new beginning of the philosophical and legal debate is usually dated back to an article by Samuel Warren and Louis Brandeis in the *Harvard Law Review* in 1890 – with regard to the concept of privacy surely one of the most influential articles ever. Warren and Brandeis develop the idea of the right to privacy as a "right to be let alone", and the value of the private is accordingly justified with regard to individual rights of freedom, as later seen in numerous other theorists in differently accentuated ways (e.g. Allen 1988, Reiman 2004, Cohen 1992, Roessler 2005).

The focus on the individual right to privacy is due to the paradigm of liberalism. I believe that taking these individual rights as a point of departure is not only historically important and correct; it is also precisely this focus which enables central aspects of the meaning as well as of the *threats* to privacy to be articulated. Particularly since the technological modernizations of recent years, the problem of individual privacy of information has been in the center of debates: technological developments have led to new threats to as well as to new concepualizations of individual privacy and its protection (see, for example, Reiman 2004, Solove 2008, Nissenbaum 2010; Tangens/padeluun 2006).

Before addressing this problem more closely, however, I shall point out briefly the general normative foundations of privacy: the value of privacy in the public sphere has to be argued for along the same lines as the value of privacy in general. Why is a society without structural separations between private and public realms or dimensions so undesirable? We ultimately value privacy because we value individual liberty or autonomy and because this autonomy is not viable – at least, not in all of its aspects and certainly not in its most relevant aspects – without the protection of privacy, without the differentiation between private and public dimensions or areas of life. In terms of its value, privacy is thus functionally linked to autonomy (see for more detail Roessler 2005).

What has to be counted as private? Here, too, I can only provide an outline: the common denominator of the various forms of privacy is the idea of individual control of access: something is private and has to be respected as private, if I am capable of and entitled to control access to it – to data, to information, to homes, to decisions or to forms of action. This 'access' can, of course, be understood indirectly, for example, when it involves *access to* or interference with individual decisions (for example, which religion do I want to worship?); access can, however, be meant completely literally as access to data or access to my home. Privacy in the sense of individual control of access can thus have different meanings.

On this basis, the next step is plausible as well: in the tradition of Warren and Brandeis and the liberal paradigm of individual rights of freedom it seems reasonable to understand the complexity of privacy in such a way that one is dealing

with different dimensions. If privacy involves data and information about a person, that is, generally involves what other people know about a person, then at issue is informational privacy. If privacy involves decisions and actions (who I live with; what job I want to get), then at issue is decisional privacy, the privacy of decisions. And if the privacy of a person's home is under debate, I then speak of local privacy. In general, one can thus say that privacy protects different dimensions of the individual freedom and autonomy of persons. Persons want the protection of privacy because without this protection they cannot live their lives as freely and in as self-determining ways as possible.

In the following I will be concerned with the problem of *informational privacy*. The definition of informational privacy as enabling people to control the access to their data is nowadays relatively uncontested in the literature (see also Bok 1983: 10, Allen 1988: 15, Innes 1992: 56, 69, Allen-Castellito 1999: 723, Froomkin 2000, Roessler 2005: 23, 136-137; but see for criticism Nissenbaum 2010: 120f). Private information is (and should be) information to which persons can control the access themselves or have at any rate legitimately *reasonable expectations* about who has access to their data and in which ways they are transmitted. This idea applies to the very different contexts of personal information given to friends; given to one's doctor; or given to one's bank, and it also applies to the context of internet purchases – to name a few examples. If these different data are passed on and disseminated without the knowledge of or against the will of the persons, their privacy and thus, ultimately, as these theories argue, their autonomy will be violated. (See already Westin 1967: 32-34). So, informational privacy is concerned with information or knowledge other people might have about a person in different contexts and different relationships: in intimate relationships as well as those with colleagues or with strangers, i.e. with unspecified others (this will become specifically relevant in the online world).

Therefore, the social norms of informational privacy not only protect and enable a specific behaviour – the freedom of the person whose privacy is at stake – but also demand and stipulate a specific behaviour, namely that of the persons or institutions which have to respect privacy. The social norms of privacy protect individual informational privacy in different contexts in different ways, because the protection of information varies according to the context and relationship at stake.

We can now understand the general thesis demonstrating the value of informational privacy in liberal democracies in yet a different way: the protection of informational privacy is constitutive for individuals because having control over their self-representation in different relations in different ways is constitutive for their self-understanding as autonomous persons. Schoeman refers to this as the right to 'selective self-disclosure' (Schoeman 1984). Depending on the person's

role and social relationship – for instance as friend, mother, teacher – the other persons involved will know different things about her, will have to have different information about her. These roles represent different aspects of a person's identity and personality, different dimensions of her life, different expressions of her autonomy. All of this is regulated through social, moral or legal norms of informational privacy.

The respect for the privacy of persons is thus the respect for them as autonomous subjects. Let me briefly point out that it is this basic idea of informational privacy which is also evident in European law. The German Constitutional Court argued as early as 1983 for the *right to informational self-determination* in 1983. Since 1995 there has also been an EU directive on data protection through which the control of the dissemination of one's own personal data and the access that others have to it is regulated. By now, not only does the EU *Convention of Human Rights* protect the private sphere (Article 8), so, too, does the *European Charta of Fundamental Rights and Freedoms*, which draws a distinction between the protection of private life and the protection of personal data. (Article 7 *Respect for private and family life*;[1] Article 8 *Protection of personal data*[2]).

2 Privacy and Autonomy

Let us now turn to the question of how privacy in public can be conceptualized more precisely. This idea of privacy, too, can assume various forms: we already saw that the privacy of a conversation in a cafe is to be respected, as is the behaviour of persons on the street. Here a person is private in the sense of being nameless, not known, not identifiable as a particular person with a name, biography etc. The person can be seen – and possibly spoken to – but the social norms of informational privacy in this context demand that the persons are respected in their anonymity and 'let alone' (Warren and Brandeis 1980).

In the offline world, being nameless can suffice for not being identifiable. This was already suggested by Alan Westin in his groundbreaking 1967 study *Privacy and Freedom*, in which he differentiates between various states of privacy.

---

1 "Everyone has the right to respect for his or her private and family life, home and communications".

2 "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority".

Following the first state, solitude, and the second one, intimacy, in which he includes friendship and family, as well as work colleagues, he describes the third state: "The third state of privacy, anonymity, occurs when the individual is in public places or performing public acts but still seeks and finds, freedom from identification and surveillance. He may be riding a subway, attending a ball game, or walking the streets; he is among people and knows that he is being observed; but unless he is a well known celebrity, he does not expect to be personally identified and held to the full rules of behaviour and role that would operate if he were known to those observing him. In this state the individual is able to merge into the "situational landscape". Knowledge or fear that one is under systematic observation in public places destroys the sense of relaxation and freedom that men seek in open spaces and arenas." (Westin 1967, 31f) Westin himself refers to the affinity of his theory with Georg Simmel's description of the stranger and the relationship we have to strangers, for example, on a train: when we respect them as nameless individuals and are respected by them in our own namelessness and anonymity (Westin 1967).

Westin makes out a further form of anonymity, namely the anonymous publication of ideas: "Here the individual wants to present some idea publicly to the community or to a segment of it, but does not want to be universally identified as the author at once – especially not by the authorities who may be forced to take action if they 'know' the perpetrator. The core of each of these types of anonymous action is the desire of individuals for public privacy." (Westin 1967, 32) It is stunning that Westin developed these ideas long before the age of the internet, since it is precisely these questions that nowadays have such an impact on informational privacy. Anonymity can therefore be seen as a (moral or legal) right that is based on a right to informational privacy; anonymity can thus in the first instance be defined as a case of informational privacy in the *offline* public sphere in relation to unspecified others if the person cannot be identified or determined – is not traceable. In the *online* world, the protection of privacy as anonymity is much more complex and encounters, as for instance Kerr points out, rather different problems (2009).

Before discussing more precisely the meaning and relevance of privacy as anonymity on the internet, let me first have a brief look at the concept of anonymity and its history. In the history or philosophy there is no 'right to anonymity'. Anonymity itself is not an established philosophical concept: no philosophical dictionary has an entry on anonymity. And if we consider German everyday language and its history, we can see that even in the dictionary of the *Gebrueder Grimm* (in the first volume of 1831) no entry on anonymity can be found. Anonymity is thus not only comparatively new in the conceptual history of philosophy and law; in everyday language, too, the concept and the idea has only

played a noteworthy role since roughly one hundred years. There is, however, a context in which the concept was in fact used and relevant: in the context of the nameless, anonymous writer of letters or author of literary works. Moreover, the concept also found marginal use in the ancient world refering to those beings who only appeared and were of importance as the member of a group – such as, for example the Erinyes. Still, anonymity is not exactly a basic concept of philosophy, and in recent publications on the problem of anonymity, the category of history mostly begins around 1988.

Of greater interest than these facts, however, is a change in the evaluative meaning of the concept: the idea of anonymity, of namelessness, of being unknown used to have exclusively pejorative connotations. It was associated only with non-accountabilty of dubious or maybe even criminal minds. Nowadays, however, the unnamed individual whose identity cannot be established is seen as something positive. It would otherwise not make sense to speak of a *right* to anonymity. The possibility of anonymity is now understood as actually one of the preconditions for being able to live one's own freedom, is understood as a precondition for an independent life, without the constant control of society or the state.

Yet an ambivalence remains: for, on the one hand, the anonymity of a person still can have negative connotations referring to those who do not want to take responsibility for what they have done; and on the other hand, the right to anonymity is being defended as a right to freedom. The conflicts between claiming non-identifiability and possible moral or legal duties of accountability for actions are, currently, politically deeply coded, when, for example, a right to anonymity on the internet is denied with reference to state security interests.

The re-evaluation of the idea of anonymity is, I have argued, due to the modern idea of freedom. The right to anonymity then has to be conceived of as a privacy right, and therefore, as a right to liberty. Yet *where* is anyone really anonymous? Anonymity thus seems to be a problem of privacy in public because we want to move around in public, as if we were unknown, as if we were nameless, as if we were living among strangers. "The core of … anonymous action is the desire of individuals for public privacy", as Westin described it (Westin 1967, 32). However, this privacy cannot be expected in every public space – the possibility of being suddenly de-anonymized and identified must be reckoned with in the *offline* world, too.

However, let us look more closely at the *online world*, in which the protection of privacy is particularly important and particularly difficult. Helen Nissenbaum (Nissenbaum 1999) points in the first instance to the necessity of anonymity: "for situations that we judge anonymity acceptable or even necessary we do so because anonymity offers a safe way for people to act, transact and participate without

accountability, without others 'getting at' them, tracking them down or even punishing them." Yet Nissenbaum, too, argues that in the *online* world, mere namelessness is no longer sufficient for the protection of anonymity; being anonymous online requires a different category of protection: "In all these cases, the value of anonymity lies not in the capacity to be unnamed, but in the possibility of acting or participating *while remaining out of reach, remaining unreachable*." (My emphasis B.R.) The core of privacy as anonymity is therefore the impossibility of identifying persons on the internet, tracking them down, pursuing them. What might be sufficient for the offline world is insufficient for the online world.

It is interesting (and this is also remarked upon by, for example, Gary Marx (1999)) that anonymity, just like privacy, is a fundamentally *social* concept: just like the concept of privacy, it is only meaningful in a social world in which a person's inability to be reached, their inaccessibility, must be regulated with the means of social norms. In the social world, anonymity is supposed to protect and enable privacy and freedom of a person in public social contexts.

Thus far I have attempted to outline a general concept of privacy and to demonstrate the relation between privacy and individual freedom and autonomy. A right to privacy is referred to not only in moral but also in legal terms – for example, in the EU *Convention* and *Charta* – alongside other rights of freedom. In a second step, I attempted to clarify the meaning of anonymity offline and online and the relationship between anonymity and a right to privacy: anonymity is to be conceived as a form of privacy. The right to privacy therefore encompasses a right to anonymity, which, not surprisingly and in the same way as other rights, does not apply absolutely, but must be traded off against other rights depending on the case and context (cf. Zarsky 2003, 1024ff).

However, before I turn to possible conflicts between the right to anonymity and other rights, let me mention a rather fundamental problem of anonymity: the fact that due to the technical possibilities of de-anonymization, anonymity on the internet is becoming technically increasingly impossible. As Mayer-Schoenberger and Cukier write: "A technical approach to protecting privacy – anonymization – also doesn't work effectively in many cases. Anonymization refers to stripping out from datasets any personal identifiers, such as name, address, credit card number, date of birth, or Social Security number." (Mayer-Schoenberger und Cukier 2013, 154). They argue that this had already been difficult in the world *before* Big Data, but is now in many cases completely illusory. Only two or three different *data* are needed to de-anonymize a person, as the authors convincingly demonstrate in a series of examples (2013, 154 ff.; cf. also Koot 2012; also Marx 1999 and his differentiation between different types of 'identity-knowledge'). But the fact that a right to anonymity is difficult to technically implement merely shows how easily threatened and violated privacy is in the digital world.

3 Conflicts

In the following, concluding part, I would like to address a range of problems in order to demonstrate that although a right to anonymity cannot apply absolutely, it is nevertheless central to our freedom in the public realm and is under threat not only for technical, but also for political reasons. There are very many different respects and contexts in which the moral or legal right to anonymity conflicts with other values or rights; I can only touch on some of these. In principle, the right to anonymity may conflict with societal, state or economic interests; I will therefore present examples from these three areas.

1) Anonymity as privacy vs. freedom of the press and freedom of opinion

This first conflict involves the protection of privacy as anonymity vis-a-vis the societal right to information, as, for example, expressed in the freedom of the press. A point of conflict is a general public right to knowledge and *publicity* on the one hand, and, on the other hand, the individual right to the protection of *privacy*. The protection of privacy can lead to the demand that particular data of 'identity-knowledge' be anonymized (cf. again Marx' different types of this identifying knowledge in Marx 1999; also Coleman 2014). The example that I shall discuss here is the case of Mario Costeja Gonzales: the Spanish lawyer filed a suit against Google Spain in order to have links to particular pages removed from a newspaper in which references were made to some dubious financial transactions that had taken place in the past. In its ruling, Case C 131-12, the *Court of Justice of the EU* decided in favour of Gonzales; Google was to delete the incriminating links because individual persons have a right to be forgotten by and in the public, and to be able to conceal specific data or parts of their biography.

Thus the problem is, as Borgesius and Kulk write: "In cases where somebody wants search results to be delisted, a balance must be struck between the right to freedom of expression, the right to privacy, and the right to data protection." Borgesius and Kulk (2014) discuss the ruling quite critically. They argue that even when the right to privacy – in this case the right to have one of the items of 'identity knowledge' for the identification of a person deleted – is shown respect on a case by case basis, in this case the freedom of the press should have won. The court did not take this freedom of the press sufficiently seriously. According to Borgesius and Kolk, the CJEU follows the rule that the right to data protection necessarily and always trumps other rights or interests, including the right of the public to information. The authors find this regrettable: "That 'rule' is an unfortu-

nate departure from the doctrine developed by the European Court of Human Rights. The CJEU should have given equal weight to the right to freedom of expression (which includes the right to receive information), the right to privacy, and the right to data protection." The CJEU thus deviates here from the case-law of the ECHR in order to better protect private interests (data protection interests). The conflict is clear: the interests of the public in having unfiltered information weigh more for Borgesius and Kulk, than the right to protection of personal information. I think, however, that the court ruled correctly in this case, since the ruling also involved restricting Google's power as a 'controller'. But I do not want to provide an exhaustive defence of this here. My concern here was only to demonstrate how a right to privacy *in* public, i.e. a right to anonymity, may conflict with rights *of* the public.

2) Anonymity as privacy vs. security

The conflict between social and state interests of security on the one hand and individual rights to privacy on the other, is doubtless the conflict most debated in the public today. It is often claimed that anonymity articulates a form of privacy in public that is particularly dangerous for society since anonymity means that persons cannot be held accountable for their actions. Thus, Zarsky writes: ".. anonymity will come at a high price to society. Anonymity adversely affects society by causing the loss of accountability." (Zarsky 2003,1028) This conflict involves the interests of the state in guaranteeing the security of its citizens and preventing privacy or anonymity from being 'abused' (as Zarsky argues) to achieve aims that violate the interests of the general public. The surveillance of citizens through the secret services, primarily the NSA, has demonstrated the way in which individual interests of privacy can be pushed aside when alleged interests of state are regarded as decisive (see Solove 2011; also Coleman 2014).

The classic model here, however, is still the nowadays almost old-fashioned-seeming camera surveillance: persons are observed and monitored and camera surveillance is structurally employed in order to guarantee public security at the cost of violating privacy interests of the persons under surveillance. In the trade-off between societal interests and the protection of individual privacy, the latter is almost always considered to be less relevant (see in more detail Waldron 2003, Muller et al 2007; Spaink 2005). Camera surveillance and the structural observation of persons' internet behaviour are the means by which states (whether the United States or European states) assert their security interests. What is problematic here for the idea of privacy and anonymity is not so much the fact and assertion of state security interests, but the seemingly complete absence of

efficient legal protection for the individual persons privacy right vis-a-vis these state interests. This can be seen, for instance, in the way the NSA dealt with the group *Anonymous*. On the basis of the data made accessible by Edward Snowden, Glenn Greenwald describes this as follows: "The treatment of *Anonymous* as well as the vague category of people known as "Hacktivists" is especially troubling and extreme. That's because *Anonymous* is not actually a structured group but a loosely organized affiliation of people around an idea. Someone becomes affiliated with *Anonymous* by virtue of the positions they hold. (…) That the NSA targets such broad categories of people is tantamount to allowing it to spy on anyone anywhere, including in the United States, whose ideas the government finds threatening." (Greenwald 2014, 189f; for a detailed examination of the group *Anonymous* cf. Coleman 2014).

This example is important as an illustration because the group calls itself *Anonymous* and anonymity in the public sphere, as we have seen, can be understood as a right to privacy. The surveillance of the NSA has demonstrated how precarious the protection of individual privacy has become and how easy it is to identify persons and to observe them, to structurally subject them to surveillance. The public that has to be protected from suspicious persons seems in this case not so much to be the societal public, the social public sphere, but the public that is represented exclusively by (secret) state actors. The fact that access to personal data is technically possible for any person or state institution is a threat to the protection of privacy in public that can hardly be overestimated.

3) Anonymity as privacy vs the free market

This brings me to my final example: markets in personal data form one of the most lucrative markets in the world. The data concern every bit of digital information about persons and their internet behaviour. Companies like Acxiom which buy and sell personal data from and to other companies are dependent on customers remaining precisely identifiable – not necessarily as an individual person but as a customer that belongs to the group of people that have bought – say – books, backpacks, hiking shoes and holidays. These companies make money based on the idea of *behavioural targeting*: each advertisement is tailored as precisely as possible to a customer's internet-profile (based on data from search machine entries, social media, former purchases, general browsing behaviour, etc) so that every advertisement placed on a person's sites will register as many hits and ultimately as many purchases as possible. Personal data are thus invaluable: the more personal data are available, the more the companies know about their customers – the 'targets' – the more selectively they can advertise to their custo-

mers, and the higher the sales are. If, however, all or even only a large part of customer data were anonymized – deleted or made non-accessible in some other way – because customers want to protect their privacy against the 'economic public' of unspecified others, the companies would have to accept heavy losses, and, as they argue, economic interests would be greatly harmed. Nissenbaum (2010, 46f), for instance, provides a series of examples of companies that buy, collect, and mine personal data; companies that would not be able to operate if customers could structurally and effectively push through their demand to delete their personal data, make them non-accessible. At the beginning, we saw that the right to informational privacy can also be asserted against unspecified others, against strangers; precisely for this reason, the case of the conflict between the economic interests of actors in the free market on the one hand and the interests of customers in privacy on the other hand is a conflict that affects privacy *in* public. However, here, too, I can do no more than outline the conflict and to point out the pressure on the right to privacy as the right to anonymity under the technological conditions of the digital society (see more detailed on this problem Roessler 2015).

This brings me to my conclusion: under conditions of modern technology, privacy in public is specifically relevant as anonymity on the internet. We can thus see that the right to anonymity is a modern right in the true sense, since it gets its specific meaning under conditions of highly advanced information and communication technologies. Under these conditions, anonymity becomes particularly urgent and at the same time, from a technological perspective, particularly difficult to implement. The right to privacy as the right to anonymity is a right derived from the right to liberty: it is one of the rights that are necessary to make liberty-rights, and thus also political rights of democratic self-determination, concrete and viable. Democratic self-determination is not possible without the guarantee of individual rights to freedom, of freedom from surveillance, of the freedom to anonymously act in public – *online* and *offline*. Hence, with the right to privacy in public not only the protection of individual autonomy is at stake, but also the possibility of collective autonomy, of democratic self-determination.

Bibliography

Allen, Anita L.: "Coercing Privacy," in: *William and Mary Law Review*, Vol. 40, 1999, pp. 723–757.

Allen, Anita L.: *Uneasy Access: Privacy for Women in a Free Society*, Totowa, N. J.: Rowman and Littlefield, 1988.

Bok, Sisela, Secrets: *The Ethics of Concealment and Revelation*, New York: Vintage Books, 1983.

Cohen, Jean L.: "Redescribing Privacy: Identity, Difference and the Abortion Controversy," in: *Columbia Journal of Gender and Law*, Vol. 3, 1992, pp. 43–117.

Coleman, Gabriella. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*, New York: Verso Books, 2014.
Froomkin, Michael A.: "The Death of Privacy," in: *Stanford Law Review*, Vol. 52, 2000, pp. 461–543.
Goffman, Erving: *The Presentation of Self in Everyday Life*, Garden City, N.Y.: Doubleday & Company, 1959.
Greenwald, Glenn: *No Place to Hide: Edward Snowden, the NSA, and the U.S*. Surveillance State, New York: Metropolitan Books, 2014.
Inness, Julie, Privacy: *Intimacy and Isolation*, Oxford: Oxford University Press, 1992.
Kerr, Ian, Valerie Steeves und Carole Lucock (eds.): *Lessons From the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, Oxford: Oxford University Press, 2009.
Koot, Matthijs: *Measuring and Predicting Anonymity* (PhD thesis University of Amsterdam 2012) <https://cyberwar.nl/d/PhD-thesis_Measuring-and-Predicting-Anonymity_2012.pdf> accessed 1 May 2014.
Kulk, Stefan und Frederik Zuiderveen Borgesius: "Google Spain v. González: Did the Court Forget about Freedom of Expression?," in: *European Journal of Risk Regulation*, Vol. 3, 2014, pp. 389–398.
Marx, Gary T.: "What's in a Name? Some Reflections on the Sociology of Anonymity," in: *The Information Society*, Vol. 15, 1999, pp. 99–112.
Mayer-Schoenberger, Viktor und Kenneth Cukier: *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Boston: Houghton Mifflin Harcourt, 2013.
Muller, Erwin, R. / Kummeling, Hendrikus, R. / Bron, Roland, P.: *Veiligheid en Privacy. Een zoektocht naar een nieuwe balans*. Boom Juridische Uitgevers, The Hague, 2007.
Nagel, Thomas: *Concealment and Exposure and Other Essays*, Oxford: Oxford University Press, 2002.
Nissenbaum, Helen: "The Meaning of Anonymity in an Information Age," in: *The Information Society*, Vol. 15, 1999, pp. 141–144.
Nissenbaum, Helen: *Privacy in Context: Technology, Policy, and Integrity of Social Life*, Stanford: Stanford University Press, 2010.
Parent, William: "Privacy, Morality, and the Law," in: *Philosophy and Public Affairs*, Vol. 12, 1983, pp. 269–288.
Reiman, Jeffrey: "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Information Technology of the Future," in: *Privacies: Philosophical Evaluations*, ed. by Beate Roessler, Stanford: Stanford University Press, 2004.
Roessler, Beate: *The Value of Privacy,* Cambridge: Polity Press, 2005.
Roessler, Beate: "Should Personal Data be a Tradable Good? On the Moral Limits of Markets in Privacy", in: *Social Dimensions of Privacy. Interdisciplinary Perspectives*, ed. by Beate Roessler & D. Mokrosinska, Cambridge: University Press, 2015.
Schoeman, Ferdinand: "Privacy: Philosophical Dimensions," in: *American Philosophical Quarterly*, Vol. 21, 1984, pp. 199–213.
Solove, Daniel: *Nothing to Hide: The False Tradeoff between Privacy and Security*, New Haven: Yale University Press, 2011.
Solove, Daniel: *Understanding Privacy*, Cambridge: Cambridge University Press, 2008.
Spaink, Karin: *Medische geheimen: de risico's van het elektronisch patiëntendossier*, Amsterdam: Nijgh & Van Ditmar, 2005.
Tangens, Rena & padeluun (ed.): *Schwarzbuch Datenschutz: Ausgezeichnete Datenkraken der Big Brother Awards,* Hamburg: Edition Nautalis, 2006.

Waldron, Jeremy: "Security and Liberty: The Image of Balance," in: *Journal of Political Philosophy*, Vol. 11, 2003, pp. 191–210.
Warren, Samuel D. und Louis D. Brandeis: "The Right to Privacy," in: *Harvard Law Review*, Vol. 4, 1890, pp. 193–220.
Westin, Alan F.: *Privacy and Freedom*, New York: Atheneum Press, 1967.
Zarsky, Tal Z.: "Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the internet Society," in: *Miami Law Review*, Vol. 58, 2003, pp. 991–1044.