Chapter 2
Privacy 3.0

Anton Vedder

Contents

2.1 Introduction ................................................................................................................ ....... 17
2.2 The Public Debate ............................................................................................................ 18
2.3 The Meaning of Privacy as a State of Affairs .................................................................. 19
2.4 The Meaning of Privacy as a Value .................................................................................. 22
2.5 Normative Impact of Ambient Intelligence and Converging Technologies .......... 23
2.6 Conclusion .................................................................................................................. ...... 25
References .................................................................................................................................. 26

2.1 Introduction

‘Dead or as good as dead.’ Not so long ago articles and essays on privacy often started with a statement like this one. Unfortunately, those announcing the end of privacy often did not indicate what exactly was going on. Is our privacy indeed coming to an end? Can we no longer hide things from the eyes of our all-seeing neighbors, companies, and public bodies? Or perhaps nobody, including pro-privacy advocates, is really convinced of the value of privacy? As far as the recognition of the importance of privacy is concerned, there seems to be no justification for pessimism. In spite of the prognosed lack of vitality, privacy presently leads a remarkably lively existence in newspaper opinion columns and in public debate.

Contribution received in 2010.

A. Vedder (✉)
TILT – Tilburg Institute for Law, Technology and Society,
Tilburg University, Tilburg, The Netherlands
e-mail: anton.vedder@tilburguniversity.edu

S. van der Hof and M. M. Groothuis (eds.), Innovating Government,
Information Technology and Law Series 20, DOI: 10.1007/978-90-6704-731-9_2,
This public debate, however, deserves special attention because it suffers quite considerably from superficiality. Participants cling to a simplistic definition of privacy. At the same time they tend to label the normative impact of everything related to information and information technology, in terms of privacy. Because we are on the brink of a new informatization wave, this is the right moment to explore and, if need be, update the notion of privacy.

How does privacy exactly relate to new technical developments and changing social relationships? What are the human and social vulnerabilities, and the exact values to which privacy relates in light of these changes and developments? In order to keep the notion effective, it needs to undergo some maintenance and renovation work every now and then.

2.2 The Public Debate

In public, policymaking and politics, the recognition of privacy as a value seems to be losing quite a lot of ground (cf., Albrecht et al. 2003, p. 104; Vedder 2006). Policymakers and members of government tend to defend this trend referring to the alleged decline in the common citizen’s appreciation of privacy (Projectgroep Forensische Opsporing Raad van Hoofdcommissarissen 2004). Research into citizen privacy perception, however, provide no concrete confirmation of such a decline (Perri 6 1998; Koops and Vedder 2001; Schildmeijer et al. 2005; Verhue 2007; Koffijberg et al. 2009). Nevertheless, nearly all of these investigations do make it clear that the ‘ordinary’ citizen or consumer has an enormous lack of insight concerning the technical possibilities, regarding the retention and processing of data about them.

In the past few years, in many European countries, the public debate about privacy has particularly focused on the impact on privacy, by all kinds of measures to combat terrorism and major crime. In addition, the discussion was fueled now and then by the introduction of new services and techniques by companies, like Google (search machines that profile searchers, photography of home environments). All in all, this resulted in a lively debate with contributions from various authors.

Authors who cherish privacy are generally very good at pointing out threats founded on a certain security measure or on an electronic service, or new technique. For example, they make it clear in which situation certain personal data can be leaked and where there are loopholes in security systems. In their further interpretation of the notion they heavily rely on the European and national legal approaches to the protection of personal data (Directive 95/46/EC on the Protection of Personal Data). Central to this approach is the primordial status of the definition of personal data in terms of data that can be traced back to an individual unambiguously.

Protection of these data is aimed for in different ways, but all of these are centered on the ideal of the individual as the most important discretionary
authority with regard to ‘his’ personal data. In principle, the individual has the right to control who may have access to his personal data and what may be collected, processed or saved. This right is obtained in the form of permission or agreement requirements, inspection requirements, duties to specify the purposes of data collection and various rules for the transparency of the storage and processing of data. It must for example, be clear who is responsible for a collection of data, who the processor is, what the security conditions are, etc. Protecting privacy is thus protecting personal data by protecting (and re-establishing) the individual to whom the data refer to as the unique locus of control over their whereabouts and processing.

While in the current debate, people are very good in pointing out where a specific privacy problem might occur in a technical sense, they are less proficient in explaining why or in what way these risks exactly have to be taken seriously. It is as if the normative point of the notion, the gist of it, has been lost out of sight. Perhaps it is also for this reason that the debate does not provide much insight into the considerations that have to play a role when a balance must be struck between privacy and conflicting values and interests (see also Muller et al. 2007). It should not come as a surprise then that critics often complain that privacy in political discussions generally acts as a theoretical debate killer.

2.3 The Meaning of Privacy as a State of Affairs

There is a sharp contrast between this somewhat meagre view of privacy arising from the public debate and the views of privacy in the academic discussions between legal theorists and ethicists in scientific journals. During the latter part of the previous century, it was fashionable to start theoretical contributions on privacy with mentioning the ‘conceptual chaos’ surrounding the term. Judge Biggs found in 1956 that a haystack after a hurricane was in better shape than the conceptual structure of privacy (Prosser 1960; Johnson 1989a, p. 157; Parent 1983, p. 341). With all respect to the complainers in the past and present, it should be noted that debate and controversies are somehow natural to even the most ordinary normative notions (Gallie 1955–1956). It would indicate mental impoverishment if a society like ours did not regularly speak strongly about the conceptual constructions which are part of the foundations of our type of society.

After further consideration, the supposed chaos surrounding privacy does not appear to be so bad. The majority of the differences in opinion concern state of affairs in reality to which the notion of privacy can refer on the one hand and the normative function or point of the notion on the other. A large part of these theoretical clashes concerning privacy again are more latent than manifest.

Generally, it is presumed that with regard to the state of affairs to which privacy can refer, it makes sense to distinguish a physical-spatial, relational, decisional, and informational dimension. The multidimensionality is often only mentioned to explain that privacy should not be understood as merely something spatial—as
something restricted to the body and the immediate home environment of an individual (see Nissenbaum 1998).

Over the years nearly all the aspects present in the meaning of the term when it was originally introduced by Warren and Brandeis (1890) have been retained. It was only at the end of the nineteenth century that the word ‘privacy’ came to be used explicitly as a moral and legal normative term. The normative roots of the modern privacy term appear to go back a lot further. J.S. Mill (1806–1873) argues for the protection of the domain of individual freedom against intrusions by governments, social institutions and other citizens. Mill describes this as the inner domain of consciousness, conviction, and feelings (Mill1974; cf., Schoeman 1992, pp. 24–36; Holmes 1995, pp. 17–18). Furthermore, the notions of freedom of will, moral independency, and self-determination that gradually crystallized during the Middle Ages and the Renaissance were important for the development of the modern idea of privacy. In addition, the famous article by Warren and Brandeis itself shows how old notions regarding ownership implicitly affected the term privacy. Finally, conventions and cultural traditions concerning dignity and a person’s status seem to play an important role.

Warren and Brandeis define privacy as a right of individuals to be protected against the unsolicited distribution of information concerning their private life, particularly via publications. According to them, private life concerns emotions, sensory experiences, feelings, thoughts, dealings, and includes personal relationships, relations, writings and statements (Warren and Brandeis 1890, p. 195). Both authors highlight the right to privacy in connection with a statement made two years earlier by Thomas McIntyre Cooley (1824–1898, judge of the Supreme Court of Michigan) concerning the citizen’s ‘right to be let alone by government, however, without identifying this with the right to privacy (Blok 2002).

There is a steady increase in both the social and theoretical debates about privacy during the second half of the previous century. A focus on what could be called the decisional dimension of privacy stabilizes for a while at the beginning of the 1960 and 1970s. In a number of rulings dating from this period, the Constitutional Court of the United States decided to interpret privacy as a kind of right to self-determination, a right for the individual to decide in a number of private matters.¹ This interpretation protects the right to privacy particularly against state regulatory pressure. Subsequently, the discussion focuses on the question as to how much freedom individuals should be allowed concerning their private life. In particular, this concerns decisions about an individual’s sexual preference, the use of contraceptives, abortion, etc. This discussion reminds us of a famous debate in the 1960s between the British

Philosophers Hart (1963) and Devlin (1965) with respect to the neutrality of the state in relation to a citizen’s views of the good life. The controversy is tenacious between proponents and opponents of ‘privacy protection’ in these questions. During the 1990s these questions flared up again in controversies between liberals and communitarians.

In the European and American literature of the late 1960 and 1970s, the concept of privacy is also often connected with the notion of intimacy of personal relationships (Aubel 1968; Gerstein 1978; Weinstein 1971). Many authors argue that family life must be immune from the judgement and interference by others. In these definitions, privacy is a sanctuary for intimate feelings. Feminist oriented legal professionals and ethicists questioned this argument (Allen 1988). During the 1990s, Inness defended the view that the intimacy of dealings, choices, and information should determine whether these should be considered to be worthy of protection. She provides an exhaustive, strongly normative elaboration of the term ‘intimacy’ (Inness 1992, pp. 10, 74–94).

Starting from the mid-1960s we also observe an approach to the concept in which privacy is almost completely defined in terms of the information about people (Westin 1967; Henkin 1974; Rule 1980; Parent 1983; Lyon 1994; Powers 1996; Etzioni 1999). The enormous flourish of mass media and the cautious emergence of new types of communication and techniques for data processing (the introduction of personal computers) undoubtedly gave rise to this. The idea of informational privacy is the basis of the previously mentioned European directive and national legislation regarding the protection of personal data. This approach to the idea particularly tends to be interpreted in terms of access to information about individuals. Even physical and spatial access is sometimes interpreted in terms of information (for example but not uniquely: Johnson 2001).

In all the more or less latent controversies about the priority of one of the dimensions, other points of view play a role as well. The role of social and cultural conventions and traditions regarding the meaning of privacy is sometimes highlighted (Stein and Shand 1974; Moore 1984; Johnson 1989a, b; Barth et al. 2006). This part of the discussion makes clear that the term privacy is not a rigid theoretical construction but also accommodates strong culturally dependent norms. I will come back to this point later on.

Another part of the discussion concerns the question whether privacy is a form of isolation as such or a form of controlled isolation. Unquestionably, from the beginning of the 1970s onward, privacy is being defined as spatial, relational or informational accessibility controlled by the individual (Westin 1967; Parent 1983). For example, Fried (1968, p. 209) defines privacy as, ‘the control we have over information about ourselves.’ Another author, Rachels (1975a, b, p. 326) talks of ‘the ability to control who has access to us.’ This line of discussion makes it very clear that contact with the outside world does not necessarily have to be uncomfortable with privacy when the individual remains in control of who has what kind of access to him.
2.4 The Meaning of Privacy as a Value

Does privacy present a value in itself, or is it of mere instrumental importance or a constituent, i.e., a representing part of another value? Which values are precisely at stake when infringements of privacy are observed?

There are hardly any scholars who are prepared to defend privacy as being intrinsically valuable. The only one who comes close to doing this is Benn (1988). His ideas about the relationship between privacy, autonomy, and dignity, can however be better defined in terms of constituent values: in his view, respect for personal privacy is derived from respect for the autonomy and the dignity of individuals (also cf., Bloustein 1964). The same is true for authors who—continuing along the lines of the discussions during the 1960 and 1970s concerning the decisional dimension—particularly connect privacy with individual freedom (Johnson 1989b; Gutwirth 1998; Rössler 2001). Others seem to see privacy more as being instrumentally valuable to material interests, like being able to get a job or insurance, having the right to emotional and physical tranquillity and to protection against defamation or loss of status (Rachels 1975a, b, pp. 323–333; Johnson 1994, pp. 81–102). In addition, social interests like facilitating relations and social links are often named as part of the normative view on privacy (Rachels 1975a, b; Schoeman 1984, 1992). Finally, some authors advocate the idea inspired by Mill (1974) and Foucault (1975) that privacy can be advantageous for the diversity of ideas and creativity in society. From this point of view, privacy provides a sanctuary against the disciplinary effect of mass opinion and the demands of a controlling government or the tyranny of big companies.

All the variations in focus and different views that I have briefly described above should not be understood as different or even consecutive stages in a linear historical process since the introduction of the term by Warren and Brandeis. When a new interpretation of the term is introduced, old definitions do not just disappear. Since the 1950s of the last century, there is a reasonably orderly situation. Hiding behind the refined theoretical controversies there is a useable broad privacy notion based on the relative inaccessibility to individuals by other parties. This inaccessibility can be spatial inaccessibility or refer to the relative absence of observation by instruments or of representation in data and information. It is surprising how much of Warren and Brandeis’ original notion has been kept alive. In the theoretical debate, monistic views about the value of privacy also seem to be put aside for notions about privacy as polyvalent: privacy as a servant to different values (cf., Thomson 1975a, b; Vedder 1996, 2000).

The differences in focus and the appearance of various definitions can be in good part explained by the need to protect individuals against the risks that come along with people’s vulnerabilities that are transforming as a result of technical and technological developments, changes in the socio–economic relations, disappearing lines of demarcation between the private and the public sector, and altering conventions and traditions (Vedder 1996). Previously, I briefly suggested that the rise of mass media and the introduction of the personal computer have influenced
the understanding of privacy in terms of access to data and information concerning individuals. Something similar seems to occur regarding conventions and traditions. These factors can cause a certain vulnerability to which privacy norms can provide a protection barrier (Vedder 2000). Conventions and taboos concerning the (naked) body, the practice of certain biological functions (e.g., sex), talking with and about intimate relations etc., make people vulnerable in terms of loss of status and reputation if they are seen, observed or tape recorded. Privacy norms provide protection against these risks of loss of status and reputation by having these activities generally conducted in seclusion and by ensuring that this seclusion is respected. At the same time, where the purpose of these conventions is no longer clear or experienced, the question is what is really more effective: applying privacy norms or changing the taboo? (Sometimes the conventions or taboos seem to disappear by themselves. The rise of the mobile telephone seems in any case to have gone hand in hand with a reduction of the restrictive conventions and taboos about speaking with and about intimate relations. The call for protection through privacy norms does not seem to be so strongly needed any longer.)

2.5 Normative Impact of Ambient Intelligence and Converging Technologies

The social debate on privacy would benefit from input from the theoretical controversies. The popular and superficial notion of privacy in the public debate is, for instance, unsuccessful in uncovering the relevant risks for citizens involved in all kinds of technology-related measures against crime and terrorism. The consequences of group profiling, for example, cannot be well articulated with the help of this privacy concept because of the inherent restriction to personal data in the strict sense. There is also a need to pay attention to other normative principles like those of equality and fairness (Vedder 1997, 1998, 2006).

In two recent critical studies (Winter et al. 2008; Brouwer et al. 2009) concerning the Dutch Personal Data Protection Act (‘Wet bescherming Persoonsgevens’) and its enforcement, far reaching changes were called for. Unfortunately little attention was given to the radical consequences of some imminent technical developments for the basic principles of the act.

Two developments in technology will drastically change our world in the coming 10–15 years: ambient intelligence and converging technologies. Ambient intelligence refers to the gradual integration of technical devices and technology in the environment and leads to more and better communication between devices and their users. This is possible because of three movements:

- Advanced miniaturization of computers, sensors and actuators (small instruments that start these processes or adjust them);
- Increase in storage, transmission, and processing capacity of data; and
- Omnipresence of networks and wireless communication possibilities.
Devices will be less dependent on manual operation through buttons, menus or keyboards and screens. They will be able to determine what we expect from them and, consequently, react or anticipate this. They will also be able to communicate more and better with each other, which means that the functionality of the used techniques and applications will increase enormously.

Converging technologies refer to the cross-pollination between nano technologies, biotechnologies, information and communication technologies, and cognitive science. The fusion of some or all of these technologies create new possibilities to externally intervene in people’s behavior and can serve as a substitution for the present ways of influencing people, such as upbringing, education, pills, fences, walls and, written and unwritten rules/laws (Teeuw and Vedder 2008; Vedder 2008a, b).

What impact will these technologies have on our normative standards? To start with they will make it necessary to earnestly adapt the laws and rules concerning privacy and data protection. With the event of ambient intelligence and converging technologies, more information must be generated, processed, and combined than we can presently imagine. In order for these technologies to work, all kinds of information about individuals will continuously be collected and analyzed, concerning their physical condition, location, and context (for example, family and social background). These developments make the conceptualization of privacy as we know it from the social debate and the European and national legislation largely obsolete. Firstly, the assumption that individuals should be in a position to control what happens to the data and information about them cannot be maintained in this future scenario. The system of information flows will simply become too complex and incomprehensible. Secondly, the present notion is restricted to personal data which are very rigidly defined as data that can be traced to individuals. The great amount of data and information generated in the future will not be about personal data but about profiles of groups, that can often not be traced back to individual persons in the way that currently personal data is defined.

Finally, there will be important consequences for which the present privacy-approach does not provide us with any tools for direction. The use of converging technologies will lead to an increase in data about people’s physical and clinical status. In fact this will result in an enormous expansion of the domain of medical data. Medical data will no longer merely be relevant in traditional health care and insurance domains, but expand to the domains of security and education. As ambient intelligence and converging technologies will play a bigger role in areas like security and education, they will lead to unprecedented medicalization. Physical and biological data about persons will be needed to make these applications work. These data may however indirectly reveal important information about the medical condition of the persons involved, in the same way as iris scans used for border crossing procedures may reveal information about illnesses of the passengers whose irises are scanned already now. This new medicalization and, more in general, the further expansion of information flows in our society will require radical reconsideration of the current privacy approach.
Again, reconceptualization of privacy is in itself not sufficient to come to terms with the normative impact of ambient intelligence and converging technologies. We should also be aware of other consequences. In 10–15 years’ time, for reasons of efficiency and effectivity, the state will allow traditional regulatory enforcement to be carried out by automated means. This is already happening on a small scale by means of relatively simple technologies, like roundabouts and speed bumps used in traffic control. In the future, people’s behavior can be influenced in a much more sophisticated way by instruments that either directly affect them or make changes to their environment which in turn will change their behavior. Private parties will be contracted for the production, management, and maintenance of these techniques. As a result of large scale availability and ultimately lower investments, the use of ambient intelligence applications and converging technologies for ‘private regulation’ will also increase in the coming ten years. Both the delegation of traditional state regulation and enforcement to private parties as well as private regulation arrangements create new demarcations of the public and the private, and call for reflection on the controllability and legitimacy of these new regulation and enforcement schemes.

There is another point of concern. Given, that it is highly attractive to incorporate regulation for reasons of efficiency and effectivity in technical devices, the temptation to merge the rules of technique with those of enforcement will increase. In traditional forms of regulation, such as law and social morality, it is possible to make a distinction between knowing a norm and deciding whether to act accordingly. When making this decision, there is a certain freedom because you can choose not to abide by the rule in spite of the risk of sanctions. When the norm and enforcement are merged through technical devices, people will automatically be forced to follow the rule: they will stop for a red light not because they want to but because they have no other choice. Technology will make them stop. This is interesting for two reasons. Firstly, it must be ensured that the right rules are incorporated in the technical devices and that they are applied fairly and reasonably. Justified civil disobedience is difficult or impossible. Secondly, knowledge of norms and moral motivation to follow norms (e.g., because you consider the norms good or because you want to be a good person) become needless. However, in many ideologies and philosophical-ethical streams, autonomous moral motivation is considered very important, in itself and because without the autonomous moral motivation individuals become morally lazy; the sensitivity and principal willingness to act according to norms may become redundant which could have a severe impact if these technical devices would fail to work at a certain moment.

2.6 Conclusion

In view of present and future technological developments, a more in-depth social debate about privacy enriched with elements from the ethical and legal theoretical debate, is important. Privacy is not a simple and elegant term as the present social
debate might insinuate. Privacy is a complex term and must be substantiated with the help of insights from the theoretical debate. The analytical potential of the popular notion of privacy is limited. To do justice to the real problems and risks of new technologies, privacy should be viewed as a notion that plays an instrumental role in protecting individuals, not merely in light of their naturally human vulnerabilities, but also from the viewpoint of constantly changing circumstances in the socio–economic relationships, the boundaries between the private and the public sector, and conventions and traditions. The underlying values at stake are autonomy, welfare, equality, justice, dignity, status, and tranquillity. By pinpointing the values at stake and explaining precisely when there is a breach of privacy, we clarify the importance and the meaning of the breach.

Naturally, it will not always suffice to give a fully well reasoned assessment in the event a normative conflict with other values or interests arises. The precise meaning of a breach of privacy is often not easy to illustrate in terms of concrete detrimental effects for, for example, the welfare or the freedom of the individual in question. This applies even more to the ideals of diversity and creativity in a society inspired by Mill and Foucault. The disciplining or normalizing effects of observation and surveillance systems (adaptation of own behavior, not to be conspicuous for fear of being observed) can, in principle, be seen as a threat for diversity and creativity. Nevertheless, it is difficult to determine when observation would instigate behavior adaptation or how these possible adaptations should be qualified exactly. If observation or surveillance systems do lead to changed behavior and lifestyle, a good reason should be given to accept this disciplining effect.

Finally, privacy is important but not all-important. On the one hand, sometimes the benefits and advantageous opportunities offered by new technological applications simply outweigh the privacy risks. On the other, technological applications may have other important drawbacks, which are easily overlooked when privacy is considered to be primordial.

References

Thomson JJ (1975a) The right to privacy. philosophy and public affairs, pp 295–315
Innovating Government
Normative, Policy and Technological Dimensions of Modern Government
van der Hof, S.; Groothuis, M.M. (Eds.)
2011, XVIII, 466 p., Hardcover
A product of T.M.C. Asser Press