# Chapter 5
# Ethics, Privacy, and Self-Restraint in Social Networking

**Bernhard Debatin**

## 5.1 Approaches to Privacy

Privacy is a basic human need. It is anthropologically and psychologically rooted in the sense of shame and the need for bodily integrity, personal space, and intimacy in interpersonal relationships. Especially in modern Western cultures, it is understood as a necessary condition for individual autonomy, identity, and integrity (Altman 1975; Westin 1967; see also Margulis, this volume, Chap. 2). The desire for privacy is historically variable and has increased noticeably throughout the process of modernization. As Jürgen Habermas (1962) has shown in his seminal study *The Transformation of the Public Sphere*, this process led to the emergence of the private sphere as a corollary to the public sphere: the private sphere offers the protection and freedom necessary for the undisturbed growth and self-fulfillment of the modern subject, who then, as a citizen, can participate in exchanging opinions and forming public discourse in the communicative space of the public sphere.

Privacy is to be distinguished from secrecy. While privacy can be understood in a broad way as the "right to be let alone" (Warren and Brandeis 1890) and the right not to reveal information about *oneself*, secrecy refers to blocking or hiding *any* type of information. A person's privacy is characterized by "a series of concentric circles of intimacy in which the degree of intimacy diminishes from the innermost circle outward" (Hodges 2009, p. 277f.). The more intimate something feels to a person, the more it is considered a private issue that will only be shared with someone who is close to them. While specific personal information, such as embarrassing facts, will sometimes be kept secret by an individual, secrecy has usually more to do with keeping certain places, persons, or information hidden from *any* unauthorized eye (e.g., arcane places, secret agents, state or business secrets).

B. Debatin (✉)
Ohio University, Athens, OH, USA
e-mail: debatin@ohio.edu

S. Trepte and L. Reinecke (eds.), *Privacy Online*,
DOI 10.1007/978-3-642-21521-6_5, 

There is no single definition of privacy because it is a complex and ambiguous notion, serving as an umbrella term for a variety of loosely related issues and problems (Solove 2008). However, it can be conceptualized in both positive and negative terms. Privacy is *positively* conceptualized as an individual's control over his or her circles of intimacy in four dimensions: personal space in the physical dimension, personal integrity in the psychological dimension, interaction with others in the social dimension, and personal data in the informational dimension (Leino-Kilpia et al. 2001). It can be defined *negatively* as the absence of invasion of privacy by the government, businesses, or other actors. The focus here is on different types of privacy violations and their disruptive or destructive effects on the integrity of certain human activities; consequently, much attention is given to attempts to protect privacy from intrusions. In his taxonomy of privacy, Solove (2008, pp. 101–170) identifies four types of *privacy problems*, most of which are related to informational privacy: firstly, information collection, encompassing surveillance and interrogation; secondly, information processing, with the subtypes of aggregation, identification, insecurity, secondary use, and exclusion; thirdly, information dissemination, including breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, and distortion; fourthly, invasion of one's private sphere, in the forms of intrusion or interference with personal decisions. Similarly, Nissenbaum (2010, pp. 21–64) identifies three types of technology-based privacy problems: tracking and monitoring, aggregation and analysis, and dissemination and publication. However, in order to avoid "conceptual sprawl," her notion of privacy focuses on "public/private" as a guiding normative distinction in the three dimensions of actors, realm/space, and information. Here, the right to privacy is not understood as mere access control but as the "right to appropriate flow of personal information" while maintaining the "contextual integrity" of the information (Nissenbaum 2010, p. 127).

## 5.2 Privacy Protection

Because of the rapid advances of information technology and its enormous processing and storing capacity, privacy protection has become particularly important in the informational dimension. Moreover, the ubiquity of information and communication technology also increasingly permeates the other three dimensions of privacy (For a systematic and detailed discussion of information technology-based invasions of privacy, see Nissenbaum 2010, pp. 21–64). For instance, personal space and territorial privacy are subject to invasive technologies, such as the increasing use of surveillance cameras at workplaces and in public or semi-public places (e.g., in shopping malls and airports) or the use of RFID tracking devices (Van den Hoven Aspen and Vermaas 2007). Personal communication can easily be intercepted and retained with wiretapping technology and the surveillance of e-mail and other Internet-based communication media, as warranted under the USA PATRIOT Act (Solove et al. 2006, pp. 107ff). Bodily privacy is infringed upon

by large-scale biometric checks at stadiums and other gathering places and also by the much debated body scanners in airports (Lombard 2010).

Privacy can be protected through three main mechanisms: *legal* regulation, *ethical* self-regulation, and privacy-enhancing *technology*. These three mechanisms will be discussed briefly in the following.

In modern societies, privacy enjoys specific *legal* protection, although the extent and range of the protection varies considerably. While most countries explicitly recognize basic privacy rights in their constitutions and have adopted comprehensive and general data protection laws, the United States Constitution does not mention a right to privacy. Yet, the protection of personal beliefs in the first Amendment, the search and seizure limits of the third and fourth Amendments, and the self-incrimination limit of the 5th Amendment protect at least certain aspects of personal privacy. In addition, a good dozen Supreme Court decisions have used the liberty clause of the 14th Amendment to establish a somewhat broader right of privacy. However, case law decisions and sectoral legislation, such as the Health Information Privacy Protection Act (HIPPA), the Family Educational Rights and Privacy Act (FERPA), and the Children's Online Privacy Protection Act (COPPA), only lead to "patchwork coverage" and fail to guarantee privacy as a basic right (Bennett and Raab 2006, p. 132).

Privacy as a basic human right is guaranteed in the UN Declaration of Human Rights (United Nations 1948, Art. 12), the European Convention on Human Rights (ECHR 1950, Art. 8), and many other international agreements and national statutory laws. Initially, legal regulations focused on preventing intrusion into personal privacy, home, family, and correspondence, but the rapid development of information technologies soon necessitated specific data protection laws. For instance, the OECD "Guidelines governing the protection of privacy and transborder flows of personal data" define basic fair information practices and principles (FIPP) regarding individual rights and accountability in the collection, use, purpose, and security of data (OECD 1980, Part 2). The Data Protection Directive of the European Union (European Parliament 1995) even defines *information privacy* explicitly as a basic human right. This stands in stark contrast to the situation in the US, where "the government is constitutionally prohibited under the First Amendment from interfering with the flow of information, except in the most compelling circumstances" (Cate 1999, pp. 179f.). Differences in national and international law, the lack of comprehensive privacy laws in some countries, and the rapid evolution of technology make legal regulation a cumbersome, inconsistent, and often outdated instrument of privacy regulation.

A different approach is voluntary *ethical self-regulation* of privacy. Although ethical regulation lacks the power of external sanctions (such as a legal penal system), it can be quite effective, particularly if based on the binding power of socially entrenched norms. Informal privacy norms are akin to rules of etiquette and personal morality. They govern reasonable expectations of privacy in interpersonal relationships, groups, and subcultures. More formal norms of privacy are embedded in professional norms, ethics codes, and express policies of organizations and institutions that typically deal with any kind of personal information. Such formal

policies often mix different types of privacy regulation, such as privacy commitments, privacy codes, privacy standards, and privacy seals (Bennett and Raab 2006, pp. 151–175). Professional discretion and confidentiality thus belong to the privacy standards that clients may reasonably expect in their interactions with agencies such as health care providers or educational institutions.

As Nissenbaum (2010, pp. 129ff.) has shown, all of these norms are entrenched in specific contexts, within which they regulate the flow of personal information, which is why they are referred to as informational norms. From this perspective, the right to privacy can be understood as a right to *context-appropriate flow* of personal information. In other words, privacy does not mean the indiscriminate control of personal information, but a highly differentiated practice of sharing and withholding information depending on its meaning and sensitivity in different contexts. Consequently, violations of privacy are seen as violations of contextual integrity or "breaches of context-relative informational norms" (Nissenbaum 2010, p. 140). This contextual approach to privacy not only allows a detailed descriptive analysis of privacy, it also provides a strong normative basis for an ethical critique of privacy invasion as an unjustified transgression of contextual integrity. The transgression would be deemed unjustified whenever (a) expectations of the established context-appropriate flow of information are breached, and (b) the novel flow is not morally superior to the existing contextual norms and practices (Nissenbaum 2010, p. 164). The task of the ethical evaluation is, then, "to compare entrenched and novel flows in terms of values, ends, and purposes of respective contexts" (Nissenbaum 2010, p. 227). The concept of contextual integrity thus provides both a rational explanation of the moral outrage individuals feel when their privacy is invaded and an ethical framework for assessing the legitimacy of their claims.

The technicization of privacy invasion, particularly in the realm of information technology, has led to an increased demand for the third approach to privacy protection, i.e., *privacy-enhancing technology*. This approach is broader than just protecting privacy with the help of specific information technology. For centuries, simple mechanical solutions have been used to protect people's privacy: screens, curtains, doors, fences, and sound insulation protect against the unwanted gaze and eavesdropping; sensitive paper documents are locked in filing cabinets and often shredded after their intended purpose expires. In digital information environments, technological privacy protection can be achieved through access control and privacy-sensitive data management. *Access* can be controlled with a variety of hard- and software tools, such as authentication tools, firewalls, spyware detectors, filters, secure connections, and privacy settings. In addition to this, privacy-sensitive digital *data management* employs techniques such as data encryption, anonymization tools, blocking of data aggregation, automatic data expiration, and secure data deletion tools (Bennett and Raab 2006, pp. 177–202).

Unfortunately, much as fences can be climbed and locks picked, digital access control and data management tools can be circumvented or hacked into. The reliability and trustworthiness of privacy technologies are thus rather questionable. They are a necessary but not sufficient condition for informational privacy. Sole reliance on such technologies often creates a false sense of security and may

actually lead to careless and imprudent behavior. As will be shown in Sect. 5.4, citizens must not only insist on their privacy rights but also acquire *privacy literacy,* which encompasses an informed concern for their privacy and effective strategies to protect it. First, though, ethical arguments that analyze the normative status of privacy and develop moral principles to justify its protection must be considered.

## 5.3 Ethical Justification of Privacy Protection

Similar to the conceptualization of privacy, the ethical justification of privacy and its protection can be founded on positive and negative arguments. The *positive* argument claims that the social-psychological need for privacy and the legal right to privacy imply that privacy possesses a specific moral value for individuals, relationships, and society, and therefore deserves special protection. Privacy is regarded both as an inherent value and as interrelated with a number of other essential human values, among them moral autonomy and freedom, equality and justice, dignity and self-fulfillment, and trust and variety in relationships. Privacy also draws moral value and legitimacy from its crucial role for the functioning of key social institutions and the well-being and freedom of citizens (Nissenbaum 2010, pp. 67–83; Solove 2008, pp. 77–100). The demand for privacy protection thus rests upon value-based moral claims and can be ethically justified by the moral value of privacy and its links to related basic values.

A central value and guiding principle of the positive ethical justification of privacy and its protection is the individual's right to *self-determination*, i.e., the right to freely determine what is necessary and desirable for a fulfilling and meaningful life and to freely pursue one's social, cultural, political, and economic development. Self-determination is thus part of an individual's autonomy and freedom. Self-determination and autonomy are, as Kant has shown, intrinsically connected: "Autonomy of the will is the property the will has of being a law unto itself" (Kant 1785/1964, p. 108). In short, self-determination of the free will is the basis for moral action and at the same time an inalienable natural right. Applied to privacy, self-determination is the underlying moral principle and right that enables individuals to control access to their private sphere and to regulate the flow and context of their information. Self-determination can thus be regarded as a basic positive moral and legal principle of privacy protection (Baker 2008, p. 10).

Given the ubiquity and influence of information technology in our society, *informational self-determination* has become a central positive concept in the privacy debate and also in privacy policy. As Hornung and Schnabel (2009, p. 85) have pointed out, privacy and informational self-determination guard the borders among different societal contexts, "as they prevent sensitive information from one context (e.g., the working world, medical treatment, family life, etc.) from proliferating into other ones." They also stress the fundamental role of informational self-determination for the development of autonomous individuals and for their unhampered participation in the political process. It is noteworthy that, in a

groundbreaking decision, the German Federal Constitutional Court in 1993 established the right to informational self-determination and data protection, linking them explicitly to "the fundamental values those rights are assumed to protect and which were identified by the German Constitutional Court as human dignity and self-development" (Rouvroy and Poullet 2009, p. 46). The right to informational self-determination is also expressed in the 1995 data protection directive of the European Union (European Parliament 1995). Even though some countries do not recognize the right to informational self-determination, the significance of this concept cannot be overemphasized.

The *negative* ethical argument for protecting privacy is based on the harm principle (Mill 1851/1991), which postulates the duty to avoid harming others for one's own benefit. As an ethical principle, harm avoidance is not just built upon a selfish interpretation of the Golden Rule, which simply advises us not to harm others so that we will not be harmed. Rather, it is based on a universal appreciation of a shared capacity for suffering, human connectedness, and compassion (Linklater 2006). It also does not exclude the causation of *any* harm (otherwise, for example, many medical procedures would be impossible). Instead, it specifically refers to harm that both violates a person's right and at the same time can actually be avoided without creating greater harm elsewhere. This necessitates applying a cost-benefit analysis that weighs the interest in invading a person's privacy against the individual's right to and need for privacy.

In media ethics, for instance, the cost-benefit analysis is typically based on two interdependent criteria: firstly, a privacy invasion is only acceptable if no other means are available for obtaining the needed information; secondly, any invasion of privacy requires the existence of an overriding public interest (Hodges 2009, p. 281). This approach, however, has been criticized insofar as it leaves open what exactly constitutes an overriding public interest, so that definitional power is inevitably vested in the privacy invaders, as they can always claim a higher interest in the name of the public. In the media, intrinsic journalistic news values and the frequently invoked audience's "right to know" quickly cancel out the individual's privacy claims (Christians 2010, p. 209). However, protection of privacy is a matter of general ethics and must not be subordinated to the imperatives of professional ethics or, worse, pragmatic purposes (Christians 2010).

There are two approaches to remedy this problem: *Firstly*, a balance test, as proposed by Whitehouse (2010), demands that the benefit to the public must be considerably higher than the potential damage to the journalistic profession and the victim of privacy invasion. Here, too, the cost-benefit ratio remains somewhat speculative and arbitrary because it lacks clear and fair criteria for determining what constitutes "considerably higher" benefits. *Secondly*, the "informed consent" criterion is based on the maxim of informational self-determination and thus requires the unforced and well-informed consent of the individual whose privacy is at risk (Van den Hoven Aspen and Vermaas 2007, p. 285). For private citizens (as opposed to public figures), an overriding public interest could only be claimed if public safety is at stake and if no alternative, less invasive courses of action are available to reach the same goal.

While it makes sense that the public interest might override the individual's right to privacy in certain instances, the issue becomes much more complicated when special interests, such as businesses, are the driving force of privacy invasion. Nissenbaum (2010, p. 111) argues that such particular interests are often disguised as legitimate superior values, with the result that costs and benefits are unevenly distributed at the expense of the individual. An ethically justifiable approach, however, would require a fair distribution of costs and benefits. This could be achieved with the above described framework of contextual integrity, which would weigh the context-relative norms of the individual's flow of information against the new flow intended by the special interest actor. The invasion of privacy would only be justified if the new flow was demonstrably at least as beneficial to the individual as to the special interest.

However, the contextual integrity framework has two minor conceptual flaws: one is its preference for existing norms in present contexts, which may lead, as the author concedes, to conservatism and the "tyranny of the normal"– just because a social practice is well established does not mean it is a morally good practice. The suggested remedy, the principle of moral superiority, is somewhat weak because it relies on the optimistic assumption of a commonly accepted morality and is based on a circular assessment of "how effective each (competing practice) is in supporting, achieving, or promoting relevant contextual values" (Nissenbaum 2010, p. 166). Here, a *normative ethical* concept that provides a standard of moral quality would be needed, such as the question of whether a new technology or a new flow of information fosters autonomy, self-determination, and self-fulfillment for both individuals and society as a whole; in other words, a standard that foregrounds an emancipatory potential.

The second flaw is that the contextual integrity framework provides little room for the individual as an autonomous decision maker. The comparison of the context-relative norms of the existing flow of information to those of the new flow seems to operate like a court with the assumption of a generally accepted morality as the judge. However, based on the principle of individual self-determination and autonomy, one could argue that the *informed consent* criterion should govern the comparison, and not some external moral force. This would also imply that the default setting for privacy decisions must be positive consent: the *proactive opt-in* choice, rather than the retroactive opt-out (Bowie and Jamal 2006, p. 330).

Though preferred by online businesses, opt-out solutions are always problematic from an ethical point of view because they shift the burden to the individual: the opt-in approach disallows any privacy invasion unless the individual explicitly agrees to share his or her information. Contrary to this, the opt-out approach implicitly allows the invasion of privacy unless the user actually opts out. In addition, individuals often do not know about the opt-out possibility, and opt-out solutions often entail confusing piecemeal procedures or are hidden at the end of lengthy and complicated user agreements (Bowie and Jamal 2006, p. 330). Indeed, true self-determination and actual consumer choice can only be achieved through opt-in as the default standard (Gandy 1993; Bowie and Jamal 2006). The more consumer-friendly privacy laws in the European Union often include an opt-in

requirement while US law, favoring business interests, does not even require general opt-out procedures (Bowie and Jamal 2006, p. 331).

In conclusion, the above discussion on the ethical justification of privacy protection has shown that privacy and its protection are not negligible or secondary values. Rather, they belong to the inner core of basic human rights and needs. The discussion of privacy must be centered on the idea of contextual integrity and the individual's right to self-determination. This, then, provides the basis for an ethical approach to privacy that prioritizes the individual's privacy rights over others' interest in privacy invasion. It leads to three moral principles:

1. The positive right to self-determination and the negative duty to minimize harm require a fair distribution of costs and benefits, determined by the comparison of the existing and the intended flow of information.
2. Individuals must have access to informed and positive consent (opt-in) when their context-appropriate flow of personal information is in danger of being breached.
3. An overriding interest in privacy invasion is justified only under special circumstances, such as a threat to public security or the individual, and only when no other, less invasive procedures would reach the same goal.

## 5.4 Privacy Protection in Online Social Networks

Privacy protection in online social media seems to be an oxymoron. After all, the main purpose of participating in social networks is the exchange of information, most of it highly personal, and the maintenance and expansion of one's social relationships. The informal character of online social networking and the possibility to communicate casually with few words through wall posts and status updates enables users to manage a large number of rather superficial contacts with relatively little effort – a phenomenon discussed in network sociology as "weak ties in the flow of information" (Gross and Acquisti 2005, pp. 2f.). The pervasiveness and user-friendliness of social networking sites provide additional motivation for users to post frequently. Thus, they voluntarily disclose large amounts of personal information and contribute continually to the creation and maintenance of extensive dynamic user profiles.

However, social networking sites pose many privacy risks for their users, ranging from unauthorized use of their information by government agencies and businesses to attacks by hackers, phishers, and data miners (Lynch 2010; Clark and Roberts 2010; WebSense 2010). Risks can also result from harmful activities by other users, such as cyberstalking, harassment, and reputation damage (boyd and Ellison 2008; Hoy and Milne 2010; Mishna et al. 2009). The potential risks can actually be plotted on two dimensions: a horizontal axis, which is visible to the user, and an invisible vertical one. The horizontal axis represents social interactions among the users, where people present themselves though their profiles and engage

in communicative exchanges. The vertical axis is the systematic collection, aggregation, and use of data by the networking company. The horizontal interactions occur in the visible tip of the iceberg, while the data generated by the users trickle down into the submerged part of the iceberg. For the average user, the vertical invasion of privacy and its potential commercial or criminal exploitation by third parties therefore tend to remain invisible (Debatin et al. 2009, p. 88; Nissenbaum 2010, pp. 221 ff.).

The situation is aggravated by insufficient, sloppy, and misleading privacy practices in online social networks, which have been criticized early on (Jones and Soltren 2005; Privacy International 2007). The world's largest online social network Facebook, which had over half a billion users at the end of 2010, is known for its cumbersome and confusing privacy features and its invasive and deceptive practices (EPIC 2010). The default setting for its privacy features is usually at the lowest, most open level and opt-out procedures are burdensome and convoluted, which means that users have to be very proactive if they want to protect their privacy effectively. All in all, social online networks perform poorly with respect to privacy protection and data security. A 2010 study by the German consumer organization "Stiftung Warentest" found data protection in online social networks to be rather weak. In the overall evaluation, only two of the ten networks tested showed "minor flaws," while four displayed "clear flaws" and four "severe flaws"–among the latter were the mega-networks Facebook, LinkedIn, and MySpace (Test 2010).

Studies on online privacy behavior have shown that social network users tend to be rather careless with their personal data. Most users have a general awareness of possible risks but do not act accordingly: they often know little about privacy policies and use privacy settings inconsistently or not at all (Debatin et al. 2009). The most common privacy risk management strategy is *building fences*, i.e., managing spatial boundaries by using the "friends only" setting to restrict the visibility of one's information, while users are "less aware of, concerned about, or willing to act on possible "temporal" boundary intrusions posed by future audiences because of the persistence of data" (Tufekci 2008, p. 33). And even the "friends-only" strategy is only used by a third to a half of the users (Ellison et al. 2007; Debatin et al. 2009). Moreover, the term "friend" is ambiguous in the online world, designating soulmates, acquaintances, and strangers alike. Most Facebook users have hundreds of friends, and statistically, about one third of users will accept complete strangers as friends (Jones and Soltren 2005; Jump 2005).

Even if a user profile is restricted to "friends only," the restriction can easily be bypassed through tagging, so that at least the friends of the friend who tagged something can view this information. Worse yet, the "friends only" restriction obviously affects only the horizontal dimension of interactions among users, but has no impact on the vertical dimension of data harvesting by the networking company and its partners. Therefore, it is highly questionable if one can call the "friends only" strategy a real "privacy-enhancing behavior," as Stutzman and Kramer-Duffield (2010) suggest. Might this particular strategy – like privacy technologies in general–simply create a false sense of security among its users?

This would be consistent with the finding that users tend to be satisfied with the mere idea of privacy control without much real control: while they may use privacy restrictions, "they do not quite understand that their level of privacy protection is relative to the number of friends, their criteria for accepting friends, and the amount and quality of personal data provided in their profiles, which they tend to divulge quite generously" (Debatin et al. 2009, p. 102).

Though ignorance and a false sense of security play an important role, it remains perplexing why social networking users tolerate deep invasions of their privacy. An important explanation lies in the expected benefits of social networking. The most important gratification is arguably the social capital from creating and maintaining contacts and friendships (see Ellison et al., this volume, chap. 3). In addition, social media are now deeply rooted in everyday habits and routines. Routinized social networking allows users to maintain relationships while keeping people at a ritualized distance, thus enabling large scale weak ties management (Debatin et al. 2009, p. 101). However, whether social network users follow a rational choice model in weighing the benefits and risks, such as Petronio's communication privacy management model (Xu et al. 2008), is still questionable. Similarly unconvincing is the hypothesis that they are just willing to take more risks than other people (Fogel and Nehmad 2009; Ibrahim 2008). More likely, disclosure of private information in online social networks happens through a kind of bargaining process in which the perceived concrete benefits of networking outweigh the abstract interest in guarding one's privacy. The potential impact of the disclosure is a hypothetical event in the future, while the benefits of social networking are tangible and immediate. Moreover, in analogy to a third-person effect, possible risks are typically projected into the environment and thus seen as happening to others, not to oneself (Debatin et al. 2009).

It is noteworthy, though, that users react with outrage to concrete and visible violations of their privacy. When Facebook launched the "News Feed" in September 2006, a feature that tracks users' activities and displays them on the pages of their friends, users protested massively against this intrusive feature. They formed anti-News Feed groups on Facebook, including the 700,000 member group "Students Against Facebook News Feed." Facebook reacted to this by introducing specific privacy controls for the News Feed (boyd 2008). Similarly, the Facebook advertising platform Beacon, which broadcasted online shopping activities to the users' friends, met great resistance when it was introduced in November 2007. Facebook responded by first offering various opt-out features and then, after continuing protests, changing to an opt-in policy for Beacon (Nissenbaum 2010, p. 223).

These privacy invasions visibly breached users' reasonable expectations of the context-appropriate flow of their personal information. Applying the three moral principles introduced earlier, the following conclusions can be drawn: Firstly, the comparison of the existing and novel flow shows in both cases that costs and benefits were unfairly distributed, thus violating *principle 1*. Secondly, massive protest led to a repair of the disrupted flow of information (appropriate privacy control tools in one case, and opt-in in the other). This reinstated *principle 1* and

followed the requirements of *principle 2*. Thirdly, there was obviously no overriding interest and no lack of alternative options that might have justified the continuation of the invasive practices, as stated in *principle 3*. Finally, these examples also show that moral outrage, public discourse, and political pressure are necessary to effect change in privacy policies and practices. Only then can businesses and governmental agencies be held accountable and compelled to adhere to fair privacy standards.

## 5.5 Conclusion: Toward an Ethics of Self-Restraint

In order to have a vital public discourse about privacy invasions, they must be brought to light and no longer be carried out under cover of invisibility or obscured by "technological constraints." Unfortunately, the widespread focus on technological solutions to privacy problems not only results in a false sense of security, it also encourages unthinking self-subordination to ostensible technological constraints. This is part of the broader problem that technology creates a universe of immanence with its own putatively inherent necessities and constraints, leading people to believe that there are no alternatives to technological solutions and that they have no agency and responsibility (Jonas 1984a).

The first step toward regaining agency and responsibility is the development of an enlightened understanding of technology and its unintended consequences. In the case of privacy in social media, it means that users develop *privacy literacy* that enables them to see through the technological veil and to make educated choices. In other words, users of social media need to develop an *informed concern* about their privacy, avoiding both moral panic and ignorant or naive indifference toward information technology. This implies that users must inform themselves proactively about the potential negative impact of social media on their privacy and that they must acquire the skills necessary to mitigate or entirely prevent negative consequences.

A privacy-literate user would thus not simply make use of technical privacy settings, because they are merely *spatial* access barriers that can always be bypassed somehow. Additionally, this user would employ *temporal* privacy protection, i.e., limit the availability of free floating private information from the outset so that it cannot be abused in the future. As long as there are no effective mechanisms for user-driven data annulment, any personal information that is put out on the Internet must be considered *as if* it were public, because information in digital networks is persistent and can arbitrarily be copied, distributed, and repurposed without the original owner's knowledge and consent. Reducing the flow of information is therefore a reasonable and effective strategy for maintaining the integrity of personal information. Admittedly, this would require users to readjust their expectations and behavior in social networking environments. It would require a user-centered *ethics of self-restraint* as the guiding principle of operation (Jonas 1984b). In a Kantian test of universalization, users who follow the principle

of self-restraint should always ask themselves, when posting information, *if they can at the same time will that this information become known not only to their friends but to the whole world.*

This should not be misread as carte blanche for social network owners and others to harvest user data. Rather, the user's informed concern and the subsequent ethics of self-constraint are corollaries to the three principles set forth above. Thus, the onus is on all parties involved:

- Network owners and third parties are expected to follow principles of fair information practices, i.e., to respect the user's right to self-determination, to foster a fair distribution of costs and benefits, and to employ positive consent (opt-in) as a default. The ethics of self-restraint can be applied to them too, as they should put themselves in the shoes of their users and ask *if they, in the position of the user, could at the same time will that their information become known not only to their friends but to the whole world.*
- Users have a responsibility to be sufficiently educated about their choices and actions in social media. After all, truly informed consent presupposes the user's informed concern for his or her privacy.
- And finally, ethicists, educators, system developers, and service providers are also responsible for creating an environment that fosters *privacy literacy* among the users of social media and in society as a whole.

A turn toward respectful, fair, and open information practices, based on informed consent and the ethics of self-restraint, may sometimes mean short-term losses with regard to the data harvesting business. However, long-term benefits will not only be enjoyed by users who interact in a safer and more trustworthy environment, they will also extend to social network owners and third parties because they can be trusted and will thus gain and sustain a positive reputation among their customers.

## References

Altman I (1975) The environment and social behavior: privacy, personal space, territory, crowding. Cole Publishing Company, Monterey, CA

Baker DJ (2008) Constitutionalizing the harm principle. Criminal Justice Ethics 27:3–28, Summer/Fall 2008

Bennett CJ, Raab CD (2006) The Governance of Privacy: Policy Instruments in Global Perspective, Cambridge, MA, London: MIT Press, 2 ed.

Bowie NE, Jamal K (2006) Privacy rights on the internet: self-regulation or government regulation? Bus Ethics Q 16(3):323–342

boyd d (2008) Facebook's privacy trainwreck: exposure, invasion, and social convergence. Convergence: The International Journal of Research into Media Technologies 14(1):13–20

boyd d, Ellison NB (2008) Social network sites: definition, history, and scholarship. JComput-Mediat Commun 13:210–230.http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html. Accessed 12 Jan 2011

Cate FH (1999) The changing face of privacy protection in the European Union and the United States. Ind L Rev 33:173–233

Christians CG (2010) The ethics of privacy. In: Meyers C (ed) Journalism ethics: a philosophical approach. Oxford University Press, Oxford, pp 203–214

Clark LA, Roberts SJ (2010) Employer's use of social networking sites: a socially irresponsible practice. J Bus Ethics 95:507–525

Debatin B, Lovejoy J, Hughes B, Horn A (2009) Facebook and online privacy: attitudes, behaviors, and unintended consequences. J Comput-Mediat Commun 15(1):83–108. http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2009.01494.x/pdf Accessed 11 Jan 2011

ECHR (1950) European convention on human rights. Registry of the European Court of Human Rights 2010., http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/ENG_CONV.pdf Accessed 15 Dec 2010

Ellison N, Steinfield C, Lampe C (2007) The benefits of Facebook "friends": exploring the relationship between college students' use of online social networks and social capital. JComput-Mediat Commun 12, 4. http://jcmc.indiana.edu/vol12/issue4/ellison.html Accessed 5 Dec 2010

EPIC (2010). Social Networking Privacy. Epic.Org Electronic Privacy Information Center. http://epic.org/privacy/socialnet/ Accessed 10 Dec 2010

European Parliament (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281, 23/11/1995 P. 0031 – 0050. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML Accessed 15 Dec 2010

Fogel J, Nehmad E (2009) Internet social network communities: risk taking, trust, and privacy concerns. Comput Hum Behav 25:153–160

Gandy OH Jr (1993) The panoptic sort: a political economy of personal information. Westview Press, Boulder, CO

Gross R, Acquisti A (2005) Information revelation and privacy in online social networks. Workshop on Privacy in the Electronic Society (WPES). http://privacy.cs.cmu.edu/dataprivacy/projects/facebook/facebook1.pdf Accessed 22 Dec 2010

Habermas J (1962) Strukturwandel der Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft. Darmstadt: Luchterhand Verlag. English Edition: Habermas J (1989) The Structural Transformation of the Public Sphere: An Inquiry into a category of Bourgeois Society (trans. Burger, T.). Cambridge, MA: MIT Press.

Hodges L (2009) Privacy and the press. In: Wilkins L, Christians CG (eds) The handbook of media ethics. Routledge, New York, pp 276–287

Hornung G, Schnabel C (2009) Data protection in Germany I: the population census decision and the right to informational self-determination. Comput Law Security Review 25:84–88

Hoy MG, Milne G (2010) Gender differences in privacy-related measures for young adult facebook users. J Interactive Advertising 10(2):28–45

Ibrahim Y (2008) The new risk communities: social networking sites and risk. Int J Media Cult Polit 4(2):245–253

Jonas H (1984a) The imperative of responsibility: in search of ethics for the technological age. University of Chicago Press, Chicago

Jonas H (1984b) Warum wir heute eine Ethik der Selbstbeschränkung brauchen. In: Ströker E (ed) Ethik der Wissenschaften? Philosophische Fragen. Wilhelm Fink Verlag, München, Paderborn, Wien, Zürich, pp 75–86

Jones H, Soltren JH (2005) Facebook: threats to privacy (white paper, December 14, 2005). http://www-swiss.ai.mit.edu/6805/student-papers/fall05-papers/facebook.pdf. Accessed 12 Jan 2011

Jump K (2005) A new kind of fame: MU student garners a record 75,000 Facebook friends. Columbia Missourian, 1.9.2005. http://www.columbiamissourian.com/stories/2005/09/01/a-new-kind-of-fame/. Accessed 5 Jan 2011

Kant I (1964) Groundwork of the metaphysic of morals (trans. H.J. Paton). Harper & Row, New York (Original work published 1785 in German)

Leino-Kilpia H, Välimäki M, Dassen T, Gasull M, Lemonidou C, Scott A, Arndt M (2001) Privacy: a review of the literature. Int J Nurs Stud 38:663–671

Linklater A (2006) The harm principle and global ethics. Global Soc J Interdisciplinary Int Relat 20(3):329–343

Lombard E (2010) Bombing out: using full-body imaging to conduct airport searches in the United States and Europe amidst privacy concerns. Tul J Int Comp Law 19(1):337–367

Lynch J (2010). New FOIA documents reveal DHS social media monitoring during Obama inauguration. Electronic Frontier Foundation, 13.10.2010. http://www.eff.org/deeplinks/2010/10/new-foia-documents-reveal-dhs-social-mediaAccessed 11 Jan 2011

Mill JS (1991) On liberty and other writings. Oxford University Press, Oxford (Original work published 1841)

Mishna F, McLuckie A, Saini M (2009) Real-world dangers in an online reality: a qualitative study examining online relationships and cyber abuse. Soc Work Res 33(2):107–118

Nissenbaum H (2010) Privacy in context. technology, policy, and the integrity of social life. Stanford University Press, Stanford

OECD (1980). Guidelines on the protection of privacy and transborder flows of personal data. Organisation for Economic Co-operation and Development, Washington, DC. http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html. Accessed 15 Dec 2010

Privacy International (2007) A race to the bottom: privacy ranking of internet service companies–A consultation report. Privacy International, June 9, 2007.http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-553961. Accessed 22 Dec 2010

Rouvroy A, Poullet Y (2009) The right to informational self-determination and the value of self-development: reassessing the importance of privacy for democracy. In: Gutwirth S, Poullet Y, De Hert P, de Terwangne D, Nouwt S (eds) Reinventing data protection? Springer, New York, pp 45–76

Solove DJ (2008) Understanding privacy. Harvard University Press, Cambridge, MA

Solove DJ, Rothenberg M, Schwartz PM (2006) Privacy, information, and technology. Aspen, New York

Stutzman F, Kramer-Duffield J (2010). Friends only: examining a privacy-enhancing behavior in facebook. In: CHI '10 Proceedings of the 28th international conference on Human factors in computing systems, ACM Digital Library. http://portal.acm.org/citation.cfm?id=1753559. Accessed 26 Dec 2010

Test (2010) Soziale Netzwerke: Datenschutz oft mangelhaft. Stiftung Warentest – test.de, 25. 03. 2010. http://www.test.de/themen/computer-telefon/test/Soziale-Netzwerke-Datenschutz-oft-mangelhaft-1854798-1855785/. Accessed 3 Dec 2010

Tufekci Z (2008) Can you see me now? Audience and disclosure regulation in online social network sites. B Sci Technol Soc 28(1):20–36

United Nations (1948) The universal declaration of rights. United Nations. http://www.un.org/en/documents/udhr/index.shtml. Accessed 15 Dec 2010

Van den Hoven Aspen J, Vermaas PE (2007) Nano-technology and privacy: on continuous surveillance outside the panopticon. J Med Philos 32:283–297

Warren S, Brandeis L (1890) The right to privacy. Harv Law Rev IV(5):193–220

WebSense (2010) Facebook used for phishing attacks and open redirects. In: WebSense Security Labs Blog, 29. 11. 2010. http://community.websense.com/blogs/securitylabs/archive/2010/11/29/facebook-used-for-phishing-attacks-and-open-redirects.aspx. Accessed 12 Jan 2011

Westin AF (1967) Privacy and freedom. Atheneum, New York

Whitehouse G (2010) Newsgathering and privacy: expanding ethics codes to reflect change in the digital media age. J Mass Media Ethics 25(4):310–327

Xu H, Dinev T, Smith HJ, Hart P (2008) Examining the formation of individual's privacy concerns: toward an integrative view. In: International conference on information systems (ICIS) ICIS 2008 proceedings, Paris. http://faculty.ist.psu.edu/xu/papers/conference/icis08a.pdf. Accessed 22 Dec 2010