Fast Capitalism
Volume 10 • Issue 1 • 2013

ISSN 1930-014X
doi:10.32855/fcapital.201301.007

Critical Internet Privacy Studies

Thomas Allmer

1. Introduction

There is much public talk about privacy. The following collected news clips indicate this development:

- "Google Faces More Inquiries in Europe Over Privacy Policy. Instead of facing one European investigation into its privacy policy, Google now has to contend with at least six of them" (The New York Times, April 2, 2013).
- "I don't Likes — Facebook boss Zuckerberg's sister's anger over photo: Web nerd's sister is tripped up by the social network's complicated privacy settings" (The Sun, December 27, 2012).
- "Guidelines help China to take step forward in data privacy" (South China Morning Post, April 17, 2013).

These examples point out how important the topic of privacy has become for the media and for our daily lives. The media often alert that privacy seems to be under attack and vanishing especially caused by the emergence of new information and communication technologies such as the Internet. For instance, Web 2.0 activities such as creating profiles and sharing ideas on Facebook, announcing personal messages on Twitter, uploading or watching videos on YouTube, and writing personal entries on Blogger, enable the collection, analyses, and sale of personal data by commercial web platforms. Nevertheless, what is actually meant with the term Internet privacy? Although there is much public talk about privacy, it seems that there is no definite answer; rather, ambiguous concepts of what online privacy is and what indeed privacy in peril is.

The overall aim of this paper is to clarify how Internet privacy is defined in the academic literature, what the different concepts of privacy have in common, what distinguish them from one another, and what advantages and disadvantages such definitions have in order to clarify if there is a gap in the existing literature. For doing so, section two, three, and four contain a systematic discussion of the state of the art of online privacy studies by establishing a typology of existing privacy definitions and discussing commonalties and differences. For analysing the literature on a more abstract level and identifying advantages and disadvantages, it is essential to discuss commonalties and differences and to find certain typologies. Finally, section five gives a summary and makes some propositions for a critical contribution to Internet privacy studies.

Several privacy studies scholars have provided classifications of privacy definitions. Schoeman (1984: 2-3) for instance distinguishes between three groups of privacy approaches, namely privacy as a claim or entitlement, privacy as the measure of control an individual has over oneself, and privacy as a state or condition of limited access to a person. Solove (2002: 1099-1123) discerns six conceptions of privacy, that is privacy as (1) the right to be let alone, (2) limited access to the self, (Marx) secrecy, (4) control over personal information, (5) personhood (this includes individuality, dignity, autonomy, and antitotalitarianism), and (6) intimacy. Solove (2006: 489) additionally develops a taxonomy of privacy and lists four basic groups: information collection, information processing, information dissemination, and invasion. According to Tavani (2011: 137), there are three different views of privacy: accessibility privacy, decisional privacy, and informational privacy. Gormley (1992: 1337-1338) sees four different cluster definitions in the privacy literature, namely privacy as (1) an expression of one's personality or personhood, (2) autonomy, (Marx) ability to regulate information about oneself, and (4) multidimensional approach. These typologies of different privacy approaches are arbitrary and stated without a theoretical criterion for a certain typology. There are no theoretical

foundations given for the categories and the suggested definitions. A theoretical criterion is missing that is used for discerning different privacy approaches. A theoretically founded typology of defining privacy is important in order to undertake a theoretical analysis of privacy in modern society. Providing such an analysis is a meta-theoretical task.

"Privacy is a social relation" (Lyon 1994: 184) and therefore a social phenomenon. In order to establish a typology of privacy definitions, it makes sense to make use of social theory. Social theories can be classified according to how they deal with the relationship of social structures and social actors (Giddens 1981: 64; Bourdieu 1977: 4; Fuchs 2008: 40): Individualistic and subjectivistic theorists such as Weber, Mead, and Habermas argue that society is constituted by social actors. Structuralistic and functionalistic theorists such as Durkheim, Merton, Parsons, and Luhmann highlight the constraints of social structure (institutionalized relationships) on the individual. Subjective social theories underestimate the constraining effects of social structures and objective social theories do not consider agencies in an appropriate way (Giddens 1981: 15-17; Bourdieu 1977: 3-4). Therefore, it is crucial to elaborate an integrative approach in order to solve the foundational problem of sociology of how social structures and actors are related (Giddens 1981: 64). An integrative approach considers the relationship of society (object) and individual (subject) as mutual in order to bridge the gap between subjective and objective social theories. Integrative (object/subject) approaches " escape from the ritual either/or choice between objectivism and subjectivism in which the social sciences have so far allowed themselves to be trapped" (Bourdieu 1977: 4). Regardless whether someone agrees with this approach or not, this treatment indicates that social theories deal either with objects, or/and with subjects.

These findings allow distinguishing objective, subjective, and integrative (objective/subjective) approaches of defining online privacy that can be used for constructing a typology of the existing Internet privacy literature:

Objective definitions of Internet privacy understand privacy as a specific social structure, a moral or legal right, which is used to enable someone's ability to limit or restrict others from access to persons or information (restricted access definition of privacy). Objective definitions of online privacy make one or more of the following assumptions:

- Privacy is a (moral and/or legal) right (rights-based conception of privacy).
- Privacy includes the freedom from unwarranted intrusion (non-intrusion).
- Privacy should be protected; for example, by law or certain "zones".
- Restrictions of privacy are violations.
- Privacy should be defined in a normative way.
- Full privacy can only be reached if there is no contact to other social actors.

To a certain extent, objective definitions of Internet privacy suggests that the more access to people or information is limited or restricted by a social structure such as the law, the more privacy people have.

In comparison, subjective approaches of defining online privacy focus on the individual and understand privacy as control over information about oneself (limited control definition of privacy). Subjective theories primarily understand privacy as self-determination and focuses on individual behaviour. Subjective definitions of Internet privacy make one or more of the following assumptions:

- Privacy is a personal interest (interest-based conception of privacy).
- Privacy includes the freedom from external interference in one's personal choices, decisions, and plans (non-interference).
- The degree of personal choice indicates how much privacy an individual has.
- Restrictions of privacy are losses.
- Privacy should be defined in a descriptive way.
- Full privacy is reached as long as the individual is able to choose which personalities should be disclosed.

Subjective definitions of Internet privacy suggest that the more the individual has control over his/her information, the more privacy s/he enjoys. Subjective theories primarily understand privacy as self-determination and focuses on individual behaviour.

Finally, integrative approaches of defining online privacy try to combine subjective and objective notions into one concept. Integrative definitions do not only understand privacy as a worth protecting right, they also treat individual control as an important aspect (restricted access/limited control definition of privacy).

Objective, subjective, and integrative (subjective/objective) approaches of Internet privacy will be outlined. The following three sections are therefore structured according to this distinction. The task of these sections is to give a representative, but still eclectic overview about different Internet privacy theories.

2. Objective Theories of Internet Privacy

Camp and Floridi have provided important objective approaches of privacy in the context of new technologies such as the Internet. Camp (1999) wants to know if Internet users are able to protect their privacy online and offers answers to these questions from the American legal tradition. The American legal tradition focuses on a right to privacy, rather than on an European claim for a need for data protection: "The American tradition of concern for privacy varies from the European approach. The European Community and Canada have principles of data protection, whereas the American tradition revolves around privacy. American considerations are based on common law tradition and a constitutional right, rather than on the more practical approach implied by data protection" (Camp 1999: 252).

For Floridi (1999: 53), "privacy is nothing less than the defence of the personal integrity of a packet of information" and informational privacy "a form of aggression towards one's personal identity" (Floridi 2005: 194). He considers the protection of personal identity as a "fundamental and inalienable right" (Floridi 2005: 195) and a right to informational privacy as "a right to personal immunity from unknown, undesired or unintentional changes in one's own identity as an informational entity" (Floridi 2005: 195). Camp's and Floridi's notion can be classified into objective approaches of defining privacy, because they have developed a rights-based conception of privacy.

Objective definitions of Internet privacy understand privacy as a specific social structure, a moral or legal right, which is used to enable someone's ability to limit or restrict others from access to persons or information (restricted access definition of privacy). Now, we move on to subjective approaches of studying online privacy.

3. Subjective Theories of Internet Privacy

Subjective approaches of defining Internet privacy focus on the individual and understand privacy as control over information about oneself. In the context of information privacy on the Internet, Clarke (1999: 60) states that " privacy is often thought of as a moral right or a legal right. But it's often more useful to perceive privacy as the interest that individuals have in sustaining a personal space, free from interference by other people and organizations". For Clarke (1998: 62), information technologies such as the Internet have dramatically increased the surveillance threats to personal data and personal identity. He furthermore claims that "the individual must be able to exercise a substantial degree of control over that data and its use" (Clarke 1998: 62). Agre (1997) studies privacy in the context of new information and communication technologies. He argues that the pervasive spread of computer networks has made it much easier to merge databases. Databases of personal information have thereby intensified and extensified on a global level (Agre 1997: 3). Following Clarke, for Agre (1997: 7), informational privacy can be understood as control over personal information and as "control over an aspect of the identity one projects to the world". This concept of defining privacy in the context of new technologies such as the Internet is considered as advantageously for several reasons: "It goes well beyond the static conception of privacy as a right to seclusion or secrecy, it explains why people wish to control personal information, and it promises detailed guidance about what kinds of control they might wish to have" (Agre 1997: 7-8). Because Clarke and Agre advance the idea that individuals require control over information about themselves, their notions can be classified as subjective definitions of Internet privacy.

In "Database Nation", Garfinkel (2000: 4) understands "privacy in the 21st century" in the context of self-possession, autonomy, and integrity. Privacy is "the right of people to control what details about their lives stay inside their own houses and what leaks to the outside. … It's about the woman who's afraid to use the Internet to organize her community against a proposed toxic dump – afraid because the dump's investors are sure to dig through her past if she becomes too much of a nuisance. … It's about good, upstanding citizens who are now refusing to enter public service because they don't want a bloodthirsty press rummaging through their old school reports, computerized medical records, and email" (Garfinkel 2000: 4). As mentioned above, subjective concepts of Internet privacy understand privacy as control over individual-specific information by the individual himself/herself. Therefore, when Garfinkel states that online privacy occurs on the initiative of its possessors (woman who's afraid to use the Internet, citizens who are refusing to enter public service), it becomes clear that his notion can be seen in the context of subjective approaches of Internet privacy.

Similar to Clarke, Agre, and Garfinkel, Solove focuses on individual behaviour and understands online privacy as

self-determination and control over information about oneself: "Privacy involves the ability to avoid the powerlessness of having others control information that can affect whether an individual gets a job, becomes licensed to practice in a profession, or obtains a critical loan. It involves the ability to avoid the collection and circulation of such powerful information in one's life without having any say in the process, without knowing who has what information, what purposes or motives those entities have, or what will be done with that information in the future. Privacy involves the power to refuse to be treated with bureaucratic indifference when one complains about errors or when one wants certain data expunged. It is not merely the collection of data that is the problem—it is our complete lack of control over the ways it is used or may be used in the future. … What people want when they demand privacy with regard to their personal information is the ability to ensure that the information about them will be used only for the purposes they desire." (Solove 2004: 43, 51)

To sum up: Subjective definitions of Internet privacy assume that privacy is a personal interest, or/and privacy includes the freedom from external interference in one's personal choices, decisions, and plans, or/and the degree of personal choice indicates how much privacy an individual has, or/and restrictions of privacy are losses, or/and privacy should be defined in a descriptive way, or/and full privacy is reached as long as the individual is able to choose which personalities should be disclosed. In the following section, integrative approaches of studying online privacy (a combination of subjective and objective approaches) will be treated.

4. Integrative (Objective/Subjective) Theories of Internet Privacy

Many authors have advanced an integrative approach of Internet privacy by combining rights-based ideas with individual control conceptions: For example, Ess (2009: 58) argues that "at least in those contexts and spaces where I can legitimately expect privacy, I should also be able to control the information about my behaviors in those spaces. That is, if I have a right to accessibility privacy – a sense that others cannot legitimately intrude upon me and perhaps others in certain contexts – then it would seem that I have a right to informational privacy as well". Lessig (2006) claims that with the rise of the Internet there are new challenges for privacy and that new privacy threats have emerged. He understands Internet privacy as a right and as individual control: "Individuals should be able to control information about themselves. We should be eager to help them protect that information by giving them the structures and the rights to do so" (Lessig 2006: 231). Miller and Weckert (2000: 256) assume that "the notion of privacy has both a descriptive and a normative dimension. On the one hand privacy consists of not being interfered with, or having some power to exclude, and on the other privacy is held to be a moral right, or at least an important good. … Naturally the normative and the descriptive dimensions interconnect".

Moor (1997: 31) combines objective and subjective notions in his "control/restricted access conception of privacy". For Moor (1997: 30-32), the term privacy should be used "to designate a situation in which people are protected from intrusion or observation by natural or physical circumstances" on the one hand and to "give individuals as much personal choice as possible" on the other hand. Moor (1997: 32) furthermore argues that it is important to study privacy in terms of a control/restricted access theory of privacy, "because this conception encourages informed consent as much as possible and fosters the development of practical, fine grained, and sensitive policies for protecting privacy when it is not". Tavani (2007; 2008) criticizes both objective and subjective notions of privacy. Based on Moor's concept of privacy, Tavani (2008: 144) mentions in his restricted access/limited control theory (RALC) "the importance of setting up zones that enable individuals to limit or restrict others from accessing their personal information" on the one hand and identifies "the important role that individual control plays in privacy theory" on the other hand. Tavani's notion does not only understand privacy as a legal right, which should be protected, it also treats individual control as an important aspect. In Tavani's (2007: 19) understanding, the restricted access/limited control theory, "in differentiating normative from descriptive aspects of privacy, enabled us to distinguish between the condition of privacy and a right to privacy and between a loss of privacy (in a descriptive sense) and a violation or invasion of privacy (in a normative sense)".

In addition, Introna (1997: 264) underlines that "to claim privacy is to claim the right to limit access or control access to my personal or private domain" and "to claim privacy is to claim the right to a (personal) domain of immunity against the judgments of others". Spinello (2003: 143) argues that informational privacy "concerns the collection, use, and dissemination of information about individuals. The right to informational privacy is the right to control the disclosure of and access to one's personal information". Because Introna and Spinello connect restricted

access and limited control definitions of privacy, it can be argued that there approaches provide a combination of objective and subjective notions of privacy.

Nissenbaum (2010) links adequate privacy protection to norms of specific contexts. Her framework requires that the processes of controlling and accessing information are appropriate to a particular context (Nissenbaum 2010: 147). She understands privacy as contextual integrity. Contextual integrity is a decision heuristic that focuses on changes of information processes in certain contexts such as education, health care, and psychoanalysis (Nissenbaum 2010: 169-176). The idea of contextual integrity is neither solely a subjective nor exclusively an objective approach of defining privacy in the information age: " The framework of contextual integrity reveals why we do not need to choose between them; instead, it recognizes a place for each. The idea that privacy implies a limitation of access by others overlaps, generally, with the idea of an informational norm. … Control, too, remains important in the framework of contextual integrity" (Nissenbaum 2010: 147-148). Privacy control may change the degree of access in specific social contexts.

In summary, integrative definitions of Internet privacy try to combine subjective and objective notions into one concept. Integrative definitions consider both privacy as a right that should be protected and as form of individual control. The next section provides a discussion of the existing Internet privacy theories and argues for the need of a critical Internet privacy studies approach.

5. Critical Internet Privacy Studies

The overall aim of the previous sections was to clarify how online privacy is defined in the academic literature, what the different concepts of privacy have in common, and what distinguish them from one another. For doing so, section two, three, and four contained a systematic overview of the state of the art of how to define privacy by establishing a typology of the existing literature. The following table summarizes the results.

Table 1: Foundations of Internet Privacy Studies

Foundations of Internet Privacy Studies				
		Objective Theories of Internet Privacy	Subjective Theories of Internet Privacy	Integrative (Objective/ Subjective) Theories of Internet Privacy
Objective Theories of Internet Privacy	Objective approaches of defining Internet privacy understand privacy as a specific social structure, a moral or legal right, which is used to enable someone's ability to limit or restrict others from access to persons or information (restricted access definition of privacy).	Camp (1999), Floridi (1999)		
Subjective Theories of Internet Privacy	Subjective approaches of defining Internet privacy focus on the individual and understand privacy as control over information about oneself (limited control definition of privacy).		Clarke (1999: 60), Agre (1997), Garfinkel (2000), Solove (2004)	

Integrative (Objective/ Subjective) Theories of Internet Privacy		Integrative approaches of defining Internet privacy try to combine subjective and objective notions into one concept. Integrative approaches consider both privacy as a right that should be protected and as individual control of personal information (restricted access/limited control definition of privacy).		Ess (2009), Lessig (2006), Miller and Weckert (2000), Moor (1997) Tavani (2007; 2008), Introna (1997), Spinello (2003), Nissenbaum (2010)

Objective definitions of Internet privacy understand privacy as a specific social structure, a moral or legal right, which is used to enable someone's ability to limit or restrict others from access to persons or information; for instance, they are represented by Camp and Floridi. In contrast, subjective definitions of Internet privacy focus on the individual and understand privacy as control over information about oneself; for example, representatives are Clarke, Agre, Solove. Finally, integrative approaches of studying Internet privacy try to combine subjective and objective notions into one concept; for instance, they are represented by Ess, Tavani, Nissenbaum.

To a certain extent, objective definitions suggests that the more access to persons or information is limited or restricted by a social structure such as the law, the more privacy people have. In other words: These approaches state that the more an individual information can be kept secret, the more privacy is fulfilled. On the Internet, especially Web 2.0 activities such as creating profiles, sharing ideas, announcing personal messages, uploading or watching videos, and writing personal entries on social networking sites are based on information, sharing, and attention. Regardless whether individuals are able to decide which personal information is available on the Internet and regardless whether individuals are able to choose for whom these information is available, for representatives of an objective approach, these forms of information sharing are always restrictions of privacy and therefore should be avoided. For example, I want to upload some photos on my profile on a non-profit and non-commercial social networking platform such as Kaioo (owned by the non-profit organization OpenNetworX) in order to share them with my friends, have fun, and deepen our friendship. Furthermore in this example, I decide which photos should be shared, I choose with whom, and what my friends are able to do with these photos. In an objective understanding, this is still a restriction and violation of privacy, which should be questioned and struggled against, because the more my information is kept secret, the more privacy is attained. Therefore, these approaches tend to underestimate the individual role of control and choice, which is also required for enjoying privacy (Tavani 2007: 9; Tavani 2008: 142). These approaches do not take into account that individuals can limit or restrict their access, because individuals are able to control the flow of personal information to a certain extent (Moor 1997: 31; Fried 1968: 482). In addition, individuals should be able to control the flow of personal information by themselves, because "different people may be given different levels of access for different kinds of information at different times" (Moor 1997: 31).

Subjective definitions suggest that the more the individual has control over her/his information, the more privacy he/she enjoys. This includes that if a person is not able to control his/her information anymore, but some other people or organisation may do so, privacy is restricted. While social media allow people to make new friends, share information, videos, music, or images, discuss with others, and stay in touch with friends, relatives, and other contacts, they also provide a vast amount of personal(ly) (identifiable) information. If I want to share information on commercial social networking sites, I do not have control over my information anymore, because web platforms are allowed to use my information as well in order to generate profit. From a subjective point of view of Internet privacy, the most effective way of controlling information about oneself is not to share it in the first place. Therefore, in a subjective understanding, the only opportunity to keep control over his/her information and to enjoy privacy, is not using such web platforms. This view ignores that it might cause new problems, because it could result in less fun, less social contacts, less satisfaction, a deepening of information inequality, and social exclusion (Fuchs 2009: 13). My point of view is that one opportunity for users having control over their personal information on such platforms is to foster international data protection regulations in order to hinder the collection, analyses, and sale of personal

data by commercial web platforms. Subjective privacy definitions tend to underestimate the constraining effects of social structures, which restrict the individual control over information (Tavani 2007: 9; Tavani 2008: 143). These approaches do not take into account that having full control over personal information cannot be reached in modern society (Moor 1997: 31) and that enclosing information might create new problems.

On the one hand, integrative concepts recognize the constraining effects of social structures, which restrict the individual control over information. On the other hand, they also consider the individual role of control and choice, which is also required for having privacy. Integrative notions take into account that having full control over personal information cannot be reached, but that individuals can limit or restrict their access because they are able to control the flow of personal information to a certain extent. In short, integrative approaches of studying privacy try to avoid objective and subjective pitfalls. Nevertheless, many authors have advanced critique of the concept of privacy in general (Gouldner 1976: 103; Lyon 1994: 179-198; Lyon 2001: 20-23; Lyon 2007: 174-176; Gilliom 2001: 121-125; Etzioni 1999: 183-215; Bennett and Raab 2006: 14-17; Ogura 2006: 277-280; Fuchs 2010: 174-175; Neocleous 2002: 85-110). Privacy is a modern concept of liberal democracy and is used in order to justify liberty from public intervention (Lyon 1994: 185). In the liberal understanding of privacy, the sovereign individual should have freedom to seek his/her own interests without interference and those interests are primarily interpreted as property interests and private ownership rights (Fuchs 2010: 174; Lyon 1994: 186-188). Therefore, the concept of privacy fits neatly into the concept of private property (Fuchs 2010: 174; Lyon 1994: 186; Ogura 2006: 278). The debate of privacy advances the idea of possessive and self-protective individualism (Gouldner 1976: 103; Lyon 2001: 21). Possessive individualism means that the individual is proprietor of his/her own person, capabilities, potentialities, and capacities (Macpherson 1990: 3). In the understanding of possessive individualism, the nature of human is that everyone is the owner of himself/herself and that the individual is not part of a larger social whole. The human essence is considered as being the proprietorship of himself/herself and the overall aim of society in liberal democracy is considered as being the protection of this property (Macpherson 1990: 3). In addition, individuals are seen as being related as proprietors and therefore society is considered as consisting of relations of proprietors. The actual outcome of such an understanding in reality is a competitive and possessive market society (Macpherson 1990: 271). The idea of possessive individualism can be summarized with the following propositions:

> (i) What makes a man human is freedom from dependence on the wills of others.
>
> (ii) Freedom from dependence on others means freedom from any relations with others except those relations which the individual enters voluntarily with a view to his own interest.
>
> (iii) The individual is essentially the proprietor of his own person and capacities, for which he owes nothing to society. ...
>
> (iv) Although the individual cannot alienate the whole of his property in his own person, he may alienate his capacity to labour.
>
> (v) Human society consists of a series of market relations. ...
>
> (vi) Since freedom from the wills of others is what makes a man human, each individual's freedom can rightfully be limited only by such obligations and rules as are necessary to secure the same freedom for others.
>
> (vii) Political society is a human contrivance for the protection of the individual's property in his person and goods, and (therefore) for the maintenance of orderly relations of exchange between individuals regarded as proprietors of themselves." (Macpherson 1990: 263-264)

Privacy concepts advance the idea of possessive individualism in order to define the private individual embedded in a system of a competitive market society (Gouldner 1976: 103; Lyon 2007: 174). In a market society, primarily economic and political actors are a threat to privacy, undertake surveillance and, exercise violence in order to control certain behaviours of people (Castells 2001: 173-174; Turow 2006: 118; Andrejevic 2007: 242-243). Corporations control the economic behaviour of people and coerce individuals in order to make them produce or buy specific commodities for accumulating profit and for guaranteeing the production of surplus value.

For illustration, the example of Google and DoubleClick can be outlined: According to the top sites of the web by Alexa Internet (2011), Google has the second most visits on the Internet. Google uses a wide range of methods in order to collect data on its users, namely click tracking (to log clicks of users), log files (to store server requests), JavaScript and web bugs (to check users visits), as well as cookies (to record individual actions) (Stalder and Mayer

2009: 102). DoubleClick is one of the main projects of Google (Google 2008). It is a global leader in ad serving and has developed sophisticated methods in order to collect, analyse, and assess huge amounts of users' data on the Internet (Campbell and Carlson 2002: 596-597). Google acquired DoubleClick in 2008 for US$ 3.1 billion (Google 2007; Google 2008). DoubleClick is headquartered in New York City. It was found in 1996 and works for leading digital publishers, marketers, and agencies around the world such as About, Durex, Ford, Friendster, Optimedia, Scripps, and MTV (DoubleClick). Ad serving companies such as DoubleClick use methods by placing advertisements on websites and analysing their efficiency. DoubleClick develops and provides Internet ad serving services that are sold primarily to advertisers and publishers. DoubleClick collects personal data on many websites, sells this data, and supports targeted advertising. DoubleClick's main product is known as DART (Dynamic Advertising, Reporting, and Targeting). DART is an ad serving programme working with a complex algorithm and is primarily developed for publishers and advertisers and is sold as product, which ensures that "you get the right message, to the right person, at the right time, on the right device" (DoubleClick). This example can be seen as a threat to online users' privacy, because Google and DoubleClick collect invisible personal information of online users and undertake analyses of individual behaviour on the Internet. The collection of personal information and the analyses of individual behaviour includes; for instance, which websites users visit immediately before and after the analysed site, how long and how often users are on this site, where users are located, as well as what users do on this site.

Corporations and state institutions are the most powerful actors in society and are able to undertake mass-surveillance extensively and intensively, because available resources decide surveillance dimensions. In the modern production process, primarily electronic surveillance is used to document and control workers' behaviour and communication for guaranteeing the production of surplus value. The commodification of privacy is important for enabling targeted advertising that is used for accumulating profit. State institutions have intensified and extended state surveillance of citizens in order to combat the threat of terrorism (Gandy 2003: 26-41; Lyon 2003). Therefore, one can assume that corporations and state institutions are the main actors in modern surveillance societies and surveillance is a crucial element for modern societies.

In conclusion, integrative definitions claim that privacy is an important value for modern society. These privacy concepts advance the idea of possessive individualism in order to define the private individual embedded in a system of a competitive market society. In a market society, the commodification of privacy is important in order to enable targeted advertising that is used for accumulating profit. Hence, economic actors undertake surveillance in order to threaten privacy. In modern society, there is a contradiction between privacy on the one hand and surveillance on the other hand (Fuchs 2010: 175). Therefore, the privacy ideal of integrative definitions comes into conflict with surveillance actions. These privacy concepts claim privacy as a crucial value within a society that is not able to fulfil this value.

To sum up, objective definitions of privacy tend to underestimate the individual role of control and choice. In contrast, subjective approaches of defining privacy tend to underestimate the constraining effects of social structures. Although integrative approaches of studying privacy try to avoid objective and subjective pitfalls, these concepts do not recognize the contradiction between privacy and surveillance in modern society and do not give answers to this foundational problem. The existing approaches of privacy seem to be not fruitful for studying privacy on the Internet. Therefore, the following treatment makes some propositions for a critical contribution to Internet privacy studies that ought to be outlined more in detail in further research:

- Similar to integrative approaches, a critical (Horkheimer 1937: 245-294; Horkheimer and Marcuse 1937: 625-647) contribution to Internet privacy studies is interested in combining individualistic and structuralistic notions, but does not want to advance the ideas of liberal democracy, private ownership, and possessive individualism.
- A critical notion of Internet privacy strives for the development of theoretical and empirical research methods in order to focus on online privacy in the context of domination, asymmetrical power relations, resource control, social struggles, and exploitation.
- It asks who can obtain privacy in cyberspace and who benefits from the contradiction between privacy and surveillance in modern society. It critically analyses (a) the threats of privacy as important aspects for guaranteeing the production of surplus value and for accumulating profit on the one hand and (b) privacy protection of income inequality, property interests, as well as power and ownership structures on the other hand.
- A critical notion of Internet privacy wants to overcome (a) privacy threats as well as (b) entrepreneurial privacy protection and privacy protection for other powerful actors in society in order to establish political processes and social transformations towards a participatory society.

For instance, a critical contribution to Internet privacy studies makes an effort to the individual role of control

and choice as well as to the constraining effects of social structures on Web 2.0 platforms and social networking sites such as Facebook, Twitter, Myspace, YouTube, and Blogger. (a) It furthermore investigates the principle of web 2.0 platforms, that is the massive provision and storage of personal(ly) (identifiable) data that are systematically evaluated, marketed, and used for targeted advertising. Web 2.0 applications and social software sites collect personal behaviour, preferences, and interests with the help of systematic and automated computer processes and sell these data to advertising agencies in order to guarantee the production of surplus value and to accumulate profit. A critical approach of privacy studies wants to deepen the knowledge of such privacy threats by its user. (b) In addition, to whom personal information are sold by commercial web platforms and how much these corporations such as Twitter earn with targeted advertising and the sale of data is not known to the public, because such transactions are treated as an aspect of corporation's privacy. One can assume that Twitter's business model is very successful and the company earns a lot of money with the sale of users data, because Twitter is expected to make 1 billion USD in revenue in 2013 (The New York Times 2012). A critical contribution to Internet privacy studies strives to analyse such cases and wants to make them more public in order to deepen the knowledge of social inequality and property interests. A critical notion of Internet privacy wants to put (a) privacy threats and (b) ownership structures of such commercial platforms into the larger context of societal problems in public discourse in order to establish political processes and social transformations towards a participatory society.

References

Agre, Philip. 1997. "Introduction." Pp. 1-28 in Technology and Privacy: The New Landscape, edited by P. Agre and M. Rotenberg. Cambridge: MIT Press.

Alexa, Internet. 2011. "Top Sites." http://www.alexa.com. Accessed May 14, 2013.

Andrejevic, Mark. 2007. "Surveillance in the Digital Enclosure." The Communication Review 10:295-317.

Bennett, Colin and Charles Raab. 2006. The Governance of Privacy: Policy Instruments in Global Perspective. Cambridge: MIT Press.

Bourdieu, Pierre. 1977. Outline of a Theory of Practice. Cambridge: Cambridge University Press.

Camp, Jean. 1999. "Web Security and Privacy: An American Perspective." The Information Society 15:249-256.

Campbell, John and Matt Carlson. 2002. "Panopticon.Com: Online Surveillance and the Commodification of Privacy." Journal of Broadcasting & Electronic Media 46:586-606.

Castells, Manuel. 2001. The Internet Galaxy: Reflections on the Internet, Business, and Society. Oxford: Oxford University Press.

Clarke, Roger. 1998. "Cyberspace Invades Personal Space: Information Privacy on the Internet." Telecommunication Journal of Australia 48:61-67.

—. 1999. "Internet Privacy Concerns Confirm the Case for Intervention." Communications of the ACM 42:60-67.

DoubleClick. http://www.doubleclick.com. Accessed June 14, 2013.

Ess, Charles. 2009. Digital Media Ethics. Cambridge: Polity Press.

Etzioni, Amitai. 1999. The Limits of Privacy. New York: Basic Books.

Floridi, Luciano. 1999. "Information Ethics: On the Philosophical Foundations of Computer Ethics." Ethics and Information Technology 1:37-56.

—. 2005. "The Ontological Interpretation of Informational Privacy." Ethics and Information Technology 7:185-200.

Fried, Charles. 1968. "Privacy." The Yale Law Journal 77:475-493.

Fuchs, Christian. 2008. Internet and Society: Social Theory in the Information Age. New York: Routledge.

—. 2009. Social Networking Sites and the Surveillance Society: A Critical Case Study of the Usage of studiVZ, Facebook, and Myspace by Students in Salzburg in the Context of Electronic Surveillance. Salzburg: Research Group Unified Theory of Information.

—. 2010. "studiVZ: Social Networking in the Surveillance Society." Ethics and Information Technology 12:171-185.

Gandy, Oscar. 2003. "Data Mining and Surveillance in the Post-9/11 Environment." Pp. 26-41 in The Intensification of Surveillance. Crime, Terrorism and Warfare in the Information Era, edited by K. Ball and F. Webster. London: Pluto Press.

Garfinkel, Simson. 2000. Database Nation: The Death of Privacy in the 21st Century. Beijing: O'Reilly.

Giddens, Anthony. 1981. A Contemporary Critique of Historical Materialism: Power, Property and the State. London: Macmillan.

Gilliom, John. 2001. Overseers of the Poor: Surveillance, Resistance, and the Limits of Privacy. Chicago: University of Chicago Press.

Google. 2007. "Press Center: Google to Acquire Doubleclick: Combination Will Significantly Expand Opportunities for Advertisers, Agencies and Publishers and Improve Users' Online Experience." http://www.google.com/intl/en/press/pressrel/doubleclick.html. Accessed June 14, 2013.

—. 2008. "Press Center: Google Closes Acquisition of Doubleclick." http://www.google.com/intl/en/press/pressrel/20080311_doubleclick.html. Accessed June 14, 2013.

Gormley, Ken. 1992. "100 Years of Privacy." Wisconsin Law Review:1335-1441.

Gouldner, Alvin. 1976. The Dialectic of Ideology and Technology: The Origins, Grammar, and Future of Ideology. New York: Seabury Press.

Horkheimer, Max. 1937. "Traditionelle und Kritische Theorie." Zeitschrift für Sozialforschung 6:245-294.

Horkheimer, Max and Herbert Marcuse. 1937. "Philosophie und Kritische Theorie." Zeitschrift für Sozialforschung 6:625-647.

Introna, Lucas. 1997. "Privacy and the Computer: Why We Need Privacy in the Information Society." Metaphilosophy 28:259-275.

Lessig, Lawrence. 2006. Code: Version 2.0. New York: Basic Books.

Lyon, David. 1994. The Electronic Eye: The Rise of Surveillance Society. Minneapolis: University of Minnesota Press.

—. 2001. Surveillance Society: Monitoring Everyday Life: Issues in Society. Maidenhead: Open University Press.

—. 2003. Surveillance after September 11. Cambridge: Polity Press.

—. 2007. Surveillance Studies: An Overview. Cambridge: Polity.

Macpherson, Crawford. 1990. The Political Theory of Possessive Individualism: Hobbes to Locke. Oxford: Oxford University Press.

Marx, Karl (MEW 23). 2005. Das Kapital: Kritik Der Politischen Ökonomie: Erster Band: Der Produktionsprozeß Des Kapitals. Berlin: Dietz.

Miller, Seumas and John Weckert. 2000. "Privacy, the Workplace and the Internet." Journal of Business Ethics 28:255-265.

Moor, James. 1997. "Towards a Theory of Privacy in the Information Age." Computers and Society 27:27-32.

Neocleous, Mark. 2002. "Privacy, Secrecy, Idiocy." Social Research 69:85-110.

The New York Times. 2012. Disruptions: Instagram Testimony Doesn't Add Up. Accessed July 10, 2013. http://bits.blogs.nytimes.com/2012/12/16/disruptions- instagram-testimony-doesnt-add-up-2.

Nissenbaum, Helen. 2010. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford: Stanford Law Books.

Ogura, Toshimaru. 2006. "Electronic Government and Surveillance-Oriented Society." Pp. 270-295 in Theorizing Surveillance: The Panopticon and Behind, edited by D. Lyon. Portland: Willan Publishing.

Schoeman, Ferdinand. 1984. Philosophical Dimensions of Privacy: An Anthology. Cambridge: Cambridge University Press.

Solove, Daniel. 2002. "Conceptualizing Privacy." California Law Review 90:1087-1155.

—. 2004. The Digital Person: Technology and Privacy in the Information Age. New York: New York University Press.

—. 2006. "A Taxonomy of Privacy." University of Pennsylvania Law Review 154:477-564.

Spinello, Richard. 2003. Cyberethics: Morality and Law in Cyberspace. Sudbury: Jones and Bartlett Publishers.

Stalder, Felix and Christine Mayer. 2009. "The Second Index: Search Engines, Personalization and Surveillance." Pp. 98-116 in Deep Search: The Politics of Search Beyond Google, edited by K. Becker and F. Stalder. Innsbruck: Studienverlag.

Tavani, Herman. 2007. "Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy." Metaphilosophy 38:1-22.

—. 2008. "Informational Privacy: Concepts, Theories, and Controversies." Pp. 131-164 in The Handbook of Information and Computer Ethics, edited by K. Himma and H. Tavani. Hoboken: Wiley.

—. 2011. Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing. Hoboken: John Wiley & Sons.

Turow, Joseph. 2006. "Cracking the Consumer Code: Advertising, Anxiety and Surveillance in the Digital Age." Pp. 279-307 in The New Politics of Surveillance and Visibility, edited by K. Hagerty and R. Ericson. Toronto: University of Toronto Press.