CONTENTS

1 What Is a Critical Introduction to Social Media? 1
   1.1 What Is Social about Social Media? 6
   1.2 What Is Critical Thinking and Why Does it Matter? 8
   1.3 What Is Critical Theory? 11
   1.4 Critical Theory Approaches 20

I FOUNDATIONS 31

2 What Are Social Media and Big Data? 33
   2.1 Web 2.0 and Social Media 34
   2.2 The Need of Social Theory for Understanding Social Media 37
   2.3 Explaining Social Media with Durkheim, Weber, Marx and Tönnies 44
   2.4 A Model of Social Media Communication 49
   2.5 Big Data 52
   2.6 Conclusion 61

3 Social Media as Participatory Culture 65
   3.1 The Notions of Participation and Participatory Culture 66
   3.2 Online Fan Culture and Politics 72
   3.3 Social Media and Participatory Culture 74
   3.4 Henry Jenkins and Digital Labour 76
   3.5 Jenkins’s Response to Criticisms 78
   3.6 Conclusion 81

4 Social Media and Communication Power 85
   4.1 Social Theory in the Information Age 86
   4.2 Communication Power in the Network Society 88
   4.3 Communication Power, Social Media and Mass Self-communication 90
   4.4 Communication Power in the Arab Spring and the Occupy Movement 98
   4.5 Conclusion 110
## II APPLICATIONS

### 5 The Power and Political Economy of Social Media

- 5.1 Social Media as Ideology: The Limits of the Participatory Social Media Hypothesis
- 5.2 The Cycle of Capital Accumulation
- 5.3 Capital Accumulation and Social Media
- 5.4 Free Labour and Slave Labour
- 5.5 Conclusion

### 6 Google: Good or Evil Search Engine?

- 6.1 Introduction
- 6.2 Google’s Political Economy
- 6.3 Googology: Google and Ideology
- 6.4 Work at Google
- 6.5 Google: God and Satan in One Company
- 6.6 Google and the State: Monopoly Power and Tax Avoidance
- 6.7 Conclusion

### 7 Facebook: Surveillance in the Age of Edward Snowden

- 7.1 Facebook’s Financial Power
- 7.2 The Notion of Privacy
- 7.3 Facebook and Ideology
- 7.4 Privacy and the Political Economy of Facebook
- 7.5 Edward Snowden and the Surveillance-Industrial Complex
- 7.6 Conclusion

### 8 Twitter and Democracy: A New Public Sphere?

- 8.1 Habermas’s Concept of the Public Sphere
- 8.2 Twitter, Social Media and the Public Sphere
- 8.3 Political Communication on Twitter
- 8.4 Uncivil Communication on Twitter
- 8.5 Twitter’s Political Economy
- 8.6 @JürgenHabermas #Twitter #Publicsphere
- 8.7 Conclusion

### 9 Weibo: Power, Ideology and Social Struggles in Chinese Capitalism

- 9.1 China’s Capitalism
- 9.2 Weibo’s Political Economy
- 9.3 Weibo and Social Media Ideologies
- 9.4 Chinese Social Struggles in the Age of Weibo
- 9.5 Conclusion
10 Airbnb and Uber: The Political Economy of Online Sharing Platforms 283
  10.1 Uber: The Pay per Service Sharing Model 284
  10.2 Airbnb: The Capitalist Sharing Economy’s Rent-on-Rent Model 292
  10.3 The Sharing Economy: A Capitalist Ideology 300
  10.4 An Alternative Sharing Economy Beyond Capitalism? 306
  10.5 Conclusion 313

11 Wikipedia: A New Democratic Form of Collaborative Work and Production? 317
  11.1 The Communist Idea 319
  11.2 Communication and Communism 323
  11.3 Wikipedia’s Political Economy 325
  11.4 Criticisms of Wikipedia 329
  11.5 Conclusion 335

III FUTURES 339

12 Conclusion: Social Media and its Alternatives – Towards a Truly Social Media 341
  12.1 Social Media Reality: Ideologies and Exploitation 341
  12.2 Social Media Alternatives 345
  12.3 Towards a Truly Social Media and a New Society 355

References 357
Index 377
KEY QUESTIONS

- How does Facebook’s political economy work?
- How has Facebook been criticized?
- What ideologies exist on and about Facebook? How does Facebook present itself to the world? What is the reality behind Facebook ideologies?
- What are the implications of Edward Snowden’s revelation of the existence of a surveillance-industrial complex in the age of social media?
- Are there alternatives to Facebook?

KEY CONCEPTS

<table>
<thead>
<tr>
<th>Digital labour</th>
<th>Targeted advertising</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy</td>
<td>Instant personalization</td>
</tr>
<tr>
<td>Social media and privacy</td>
<td>Commodification</td>
</tr>
<tr>
<td>Facebook ideologies</td>
<td>Private property</td>
</tr>
<tr>
<td>Privacy fetishism</td>
<td>Alternative social media</td>
</tr>
<tr>
<td>Privacy policy</td>
<td>Surveillance-industrial complex</td>
</tr>
<tr>
<td>Opt-out</td>
<td></td>
</tr>
</tbody>
</table>

OVERVIEW

Facebook is the most popular social networking site (SNS). SNSs are web-based platforms that integrate different media, information and communication technologies that allow at least the generation of profiles that display information describing the users, the display of connections (connection list), the establishment of connections between users displayed on their connection lists, and communication between users (Fuchs 2009b).
Mark Zuckerberg, Eduardo Saverin, Dustin Moskovitz and Chris Hughes, who were then Harvard students, founded Facebook in 2004. The movie *The Social Network* (Columbia Pictures, 2010) describes the history of Facebook as a bunch of talented Harvard students, who because of a good idea made it to be billionaires and realized the American Dream of becoming rich and famous. The movie frames the story in individualistic terms, neglecting to show that it, like most large Silicon Valley tech companies, received millions in venture capital, from Peter Thiel, Accel Partners, Jim Breyer and others, which allowed its expansion as a company. The movie advances the ideological view that in the American Dream a good idea such as Facebook can make anyone famous and popular. In reality, of course only a very small elite has the luck of becoming rich and famous precisely because others are not wealthy. In 2006, Facebook was turned from a college network into a general social network open to everyone. From then on the users of Facebook increased rapidly.

This chapter’s task is to discuss the power of Facebook, the role of surveillance and implications for privacy. First, I discuss Facebook’s economic development (section 7.1). Section 7.2 introduces the notion of privacy. Then, I criticize the dominant kind of analysis of Facebook privacy by characterizing it as a form of privacy fetishism (section 7.3). In section 7.4, I analyse Facebook’s political economy. Section 7.5 discusses Edward Snowden’s revelations. Finally, I draw some conclusions and outline strategies for alternative online privacy politics in section 7.6, and the alternative social networking site Diaspora* is introduced.
7.1 FACEBOOK’S FINANCIAL POWER

FACEBOOK’S PROFITS

Facebook became a public company on 1 February 2012. Facebook says that it generates “a substantial majority” of its “revenue from advertising”: 98.3 per cent in 2009, 94.6 per cent in 2010, 85 per cent in 2011, 84 per cent in 2012, 89 per cent in 2013, 92 per cent in 2014 and 95 per cent in 2015.1 It says: “We generate a substantial majority of our revenue from advertising. The loss of marketers, or reduction in spending by marketers with Facebook, could seriously harm our business.”2 Facebook’s self-assessment of this risk shows that it is coupled to the broader political economy of capitalism: an advertising-based capital accumulation model depends on a constant influx of advertisement investments and the belief of companies that specific forms of advertisement on specific media can increase their profits. A general economic crisis that results in decreasing profits can result in a decrease of advertisement investments.

Figure 7.1 shows the development of Facebook’s profits in the years 2007–2014. Since 2007, the company’s annual profits have increased from US$–138 million in 2007 to US$3.69 billion in 2015. There was a slump in 2008 (–$56 million), which was due to the big economic crisis that took effect in 2008 all over the world. Since 2009, Facebook’s profits have grown massively. At the same time, there was an increase of users: the number of monthly active users was 197 million in March 2009, 431 million in March 2010, 680 million in March 2011, 845 million in December 2011, 1.06 billion in December 2012, 1.23 billion in December 2013, 1.19 billion in December 2014 and 1.59 billion in December 2015.3 On 17 May 2012, Facebook became a public company. Its shares were offered at an initial price of $38 per piece.

FACEBOOK’S ACQUISITION OF OTHER COMPANIES

Facebook’s acquisition strategy is to buy other online technology providers that could either compete with Facebook directly or that allow the company to enhance its own platform and services in other technological realms. The most important acquisitions have been the mobile phone instant messaging app provider WhatsApp (2014, US$19 billion), the online video advertising company LiveRail (2014, US$500 million), Oculus Virtual Reality that produces head-mounted displays (2014, US$2 billion), the photo-sharing platform Instagram (2012, US$1 billion), the face recognition software company Face.com (2012, US$100 million), the advertising technology company Atlas (2013, US$100 million) and the mobile app developer Snaptu (2011, US$70 million).

WhatsApp and Instagram are examples of social media that competed with Facebook, which meant that Facebook became horizontally integrated in social media after acquiring the companies. The acquisitions of Atlas, Snaptu and Face.com are examples of vertical integration whereby Facebook extended its services into other realms, such as advertising, mobile phones and photo tagging. The acquisition Oculus is another example whereby

---

1 Facebook SEC filings, Form 10-K, financial years 2014+2015.
2 Ibid.
3 Ibid., 44.
Facebook extended its business into the virtual reality market. Taken together, these purchases constitute a case of conglomeration within the media technology sector.

The purchase of WhatsApp in 2014 gave Facebook a strong presence in the mobile online communication market. Instagram has become an increasingly popular social network that is focused on image sharing. Its acquisition allowed Facebook to strengthen its presence in the realm of content-sharing networks. Atlas strengthens Facebook’s provision and use of targeted advertising. Snaptu developed the Facebook app for use on all mobile phones, which increased Facebook’s presence on mobile phones. Face.com’s photo tagging applications are direct enhancements for Facebook that take into account the fact that people use their mobile phones as digital cameras and want to share the images they take with others. Facebook’s purchase of Oculus may have been driven by Google’s development of Google Glass, which may have raised Facebook’s fears about missing out on profits in the augmented reality market.

Whereas Instagram uses a targeted advertising-based capital accumulation model just like Facebook, WhatsApp and Oculus have different strategies: the first charges subscription/access fees, the second sells hardware. Although Facebook uses predominantly targeted advertising (i.e. the commodification of user data, as capital accumulation model), it has also created a presence in the commodification of hardware and of the access to online services. But Facebook also engages in horizontal integration: LiveRail specializes in providing video advertising, an area where YouTube is the market leader. Facebook hopes to better compete with Google’s YouTube by specializing in video ads with LiveRail.

7.2 THE NOTION OF PRIVACY
DIFFERENT DEFINITIONS OF PRIVACY

Tavani (2008) distinguishes between the restricted access theory, the control theory, and the restricted access/limited control theory of privacy. The restricted access theory of informational privacy sees privacy as achieved if one is able to limit and restrict others from access to personal information. The classical form of this definition is Warren and Brandeis’s notion of privacy: “Now the right to life has come to mean the right to enjoy life – the right to be let alone” (Warren and Brandeis 1890, 193). They discussed this right especially in relation to newspapers and spoke of the “evil of invasion of privacy by the newspapers”. Although some scholars argue that Warren and Brandeis’s (1890) paper is the source of the restricted access theory (e.g. Bloustein 1964/1984; Rule 2007, 22; Schoeman 1984b; Solove 2008, 15–16), already John Stuart Mill had formulated the same concept 42 years before Warren and Brandeis in his 1848 book *Principles of Political Economy* (Mill 1965, 938). This circumstance shows the inherent connection of the modern privacy concept and liberal ideology. The control theory of privacy sees privacy as control and self-determination over information about oneself (Tavani 2008).

Westin (1967, 7) provided the most influential control definition of privacy: “Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” (Westin 1967, 7). In a control theory of privacy, there is privacy even if one chooses to disclose all personal information about oneself. In an absolute restricted access theory of privacy, there is only privacy if one lives in solitary confinement without contact with others.
The restricted access/limited control theory (RALC) of privacy tries to combine both concepts. It distinguishes “between the concept of privacy, which it defines in terms of restricted access, and the management of privacy, which is achieved via a system of limited controls for individuals” (Tavani 2008, 144; see also Moor 2000).

All three kinds of definitions of informational privacy have in common that they deal with the moral questions of how information about people should be processed, who shall have access to this data, and how this access shall be regulated. All have in common the normative value that some form of data protection is needed.

CRITICISMS OF PRIVACY

Etzioni (1999) stresses that it is a typical American liberal belief that strengthening privacy can cause no harm. He stresses that privacy can undermine common goods (public safety, public health). Countries like Switzerland, Liechtenstein, Monaco and Austria have a tradition of relative anonymity of bank accounts and transactions. One sees money and private property as aspects of privacy about which the public should have no information. In Switzerland, the Federal Banking Act (§47) defines the bank secret. The Swiss Bankers’ Association sees bank anonymity as a form of “financial privacy” that needs to be protected and speaks of “privacy in relation to financial income and assets”. Most countries treat information about income and the profits of companies (except for public companies) as a secret, a form of financial privacy. The privacy-as-secrecy conception is typically part of the limited access concept of privacy (Solove 2008, 22).

Control theories and limited access/control theories of privacy, in contrast, do not stress absolute secrecy of personal information as desirable, but rather highlight the importance of self-determination in keeping or sharing personal information and the different contexts in which keeping information to oneself or sharing it is considered important. In this vein, Helen Nissenbaum argues that the “right to privacy is neither a right to secrecy nor a right to control but a right to appropriate flow of personal information” (Nissenbaum 2010, 127). In all of these versions of privacy theories, secrecy of information plays a certain role, although the exact role and desirability of secrecy is differently assessed.

The problem of secret bank accounts/transactions and the intransparency of richness and company profits is not only that financial privacy can support tax evasion, black money and money laundering, but also that it hides wealth gaps. Financial privacy reflects the classical liberal account of privacy. So, for example, John Stuart Mill formulated a right of the propertied class to economic privacy as “the owner’s privacy against invasion” (Mill 1965, 232). Economic privacy (the right to keep information about income, profits or bank transactions secret) protects the rich, companies and the wealthy. The anonymity of wealth, high incomes and profits makes income and wealth gaps between the rich and the poor invisible and thereby ideologically helps legitimizing and upholding these gaps. It can therefore be considered an ideological mechanism that helps to reproduce and deepen inequality.

The Contradictions of Privacy in Capitalism: Facebook and Google

Social media corporations’ managers often express the view that privacy is outdated. Google’s Executive Chairman Eric Schmidt said for example: “If you have something that you do not want anyone to know, maybe you should not be doing it in the first place.” Schmidt and Zuckerberg argue for massive data sharing on social media. They do not, however, mention that this sharing is not primarily a sharing of data with friends and the public, but a sharing with Google and Facebook that are the largest data processors and data commodifiers in the world – which explains not just the recent rise of the term “big data”, but also their interest in hiding their commercial interests ideologically behind the ideas of sharing and openness. Their claims are double-edged if one considers, for example, that Mark Zuckerberg in 2013 bought four estates that surround his house in Palo Alto’s Crescent Park neighbourhood for US$30 million. He is concerned about his privacy. Zuckerberg’s logic is as simplistic as it is mistaken: “Privacy is good only if you can pay for it, it is not good if it makes Facebook or Google obtain less profits.”

Whereas social media corporations advocate openness, sharing of user data and an end of privacy in order to maximize profits, they claim closure, secrecy and financial privacy when it comes to their own global finance, profit and tax issues. Social media is facing an economic antagonism between users’ interest in data protection and corporate tax accountability on the one side and corporations’ interest in user data’s transparency/commodification and corporate secrecy on the other side.

Privacy: A Bourgeois Value?

It would be a mistake to dismiss privacy rights as bourgeois values. Liberal privacy discourse is highly individualistic. It always focuses on the individual and his/her freedoms. It separates the public and private sphere. Privacy in capitalism can best be characterized as an antagonistic value that is, on the one side, upheld as a universal value for protecting private property, but is at the same time permanently undermined by corporate surveillance into the lives of people for profit purposes and by political surveillance for administrative purposes, defence and law enforcement. Capitalism protects privacy for the rich and companies, but at the same time legitimates privacy violations of consumers and citizens. It thereby undermines its own positing of privacy as a universal value.

Privacy and Surveillance

In modern society, privacy is inherently linked to surveillance. Based on Foucault’s (1977, 1994) notions of surveillance as disciplinary power, one can define surveillance as a specific kind of information gathering, storage, processing, assessment and use that involves potential or actual harm, coercion, violence, asymmetric power relations, control, manipulation,

---

6 www.youtube.com/watch?v=A6e7wDHzew (accessed on 9 November 2015).
domination or disciplinary power (Fuchs 2011a, 2011c). Surveillance is instrumental and a means for trying to derive and accumulate benefits for certain groups or individuals at the expense of other groups or individuals. Surveillance is based on the logic of competition. It tries to bring about or prevent certain behaviours of groups or individuals by gathering, storing, processing, diffusing, assessing and using data about humans so that potential or actual physical, ideological or structural violence can be directed against humans in order to influence their behaviour. This influence is brought about by coercive means and brings benefits to certain groups at the expense of others. In modern societies, privacy is an ideal rooted in the Enlightenment.

Capitalism is grounded in the idea that the private sphere should be separated from the public sphere and should not be accessible by the public, and that therefore autonomy and anonymity of the individual are needed in the private sphere. The rise of the idea of privacy in modern society is connected to the rise of the central ideal of the freedom of private ownership. Private ownership is the idea that humans have the right to as much wealth as they want, as long as it is inherited or acquired through individual achievements. There is an antagonism between private ownership and social equity in modern society. Many contemporary societies treat how much and what exactly a person owns as an aspect of privacy. Keeping ownership structures secret is a precautionary measure against the public questioning of or the political and individual attack against private ownership.

Capitalism requires anonymity and privacy in order to function. But full privacy is also not possible in modern society because strangers enter social relations that require trust or enable exchange. Building trust requires knowing certain data about other persons, especially in capitalist market relations. It is therefore checked with the help of surveillance procedures whether or not a stranger can be trusted. This means that companies try to find out as much as possible about job applicants, workers, consumers and competitors and that various forms of monitoring and espionage are common means for doing so. Corporations have the aim of accumulating ever more capital. That is why they have an interest in knowing as much as possible about their workers (in order to control them) and the interests, tastes and behaviours of their customers. This results in the surveillance of workers/employees and consumers.

The ideals of modernity (such as the freedom of ownership) also produce phenomena such as income and wealth inequality, poverty, unemployment, precarious living and working conditions, crime and so on. The establishment of trust, socio-economic differences and corporate interests are three qualities of modernity that necessitate surveillance. Therefore, on the one hand modernity advances the ideal of a right to privacy, but on the other hand it must continuously advance surveillance that threatens to undermine privacy rights. An antagonism between privacy ideals and surveillance is therefore constitutive of capitalism.

**AN ALTERNATIVE NOTION OF PRIVACY**

When discussing privacy on Facebook, we should therefore go beyond a bourgeois notion of privacy. A socialist notion of privacy attempts to strengthen the protection of consumers and citizens from corporate surveillance. Economic privacy is posited as undesirable in those cases where it protects the rich and capital from public accountability, but as desirable where it tries to protect citizens from corporate surveillance. Public surveillance of the income of the rich, and of companies and public mechanisms that make their wealth transparent, is
desirable for making wealth and income gaps in capitalism visible, whereas privacy protection from corporate surveillance is also important. In a socialist privacy concept, the existing privacy values have to be reversed. Whereas today we mainly find surveillance of the poor and of citizens who are not owners of private property and surveillance for the protection of private property, a socialist privacy concept focuses on surveillance of capital and the rich in order to increase transparency and privacy protection of consumers and workers.

A socialist privacy concept conceives privacy as the collective right of dominated and exploited groups that need to be protected from corporate domination that aims at gathering information about workers and consumers for accumulating capital, disciplining workers and consumers, and for increasing the productivity of capitalist production and advertising. The liberal conception and reality of privacy as an individual right within capitalism protects the rich and the accumulation of ever more wealth from public knowledge. A socialist privacy concept as the collective right of workers and consumers can protect humans from the misuse of their data by companies. The question therefore is, privacy for whom? Privacy for dominant groups in regard to the ability to keep wealth and power secret from the public can be problematic, whereas privacy at the bottom of the power pyramid for consumers and normal citizens can be a form of protection from dominant interests. Privacy rights should therefore be differentiated according to the position people and groups occupy in the power structure.

7.3 FACEBOOK AND IDEOLOGY

LIKE AS FACEBOOK IDEOLOGY: “I LIKE AUSCHWITZ”

Facebook advances an ideology of liking in the form of its “Like button”. For a long time, it was only possible to like pages and postings, but not to dislike them. Facebook wants to spread an affirmative atmosphere, in which people only agree and do not disagree or express discontent and disagreement. It was a common long-term criticism of Facebook that users complained about the one-dimensionality of the Like button. Zuckerberg said in 2010 that Facebook is “definitely thinking about” introducing a dislike button.8 In

---

8 Should Facebook add a dislike button? CNN Online, 22 July 2010.
September 2015, Zuckerberg argued that Facebook is testing ways of allowing users to express empathy.\(^9\) On 24 February 2016, Facebook introduced new reaction buttons that besides “Like” also include “Love”, “Haha”, “Wow”, “Sad” and “Angry”. It should be noted that there is a bias towards positive emotions in the design of these buttons: Four of the six buttons express positive emotions and only two negative ones (“Sad”, “Angry”). Furthermore, they are organized in the form of one button called “Like”: If one quickly clicks on this button, then the “Like” option is activated. Only if one puts the cursor on the “Like” button without clicking do all six buttons pop up and one can click on one of them. In this pop-up button dialogue, the “Like” symbol is closest to the cursor and the “Angry” symbol far away. This design makes “Likes” more likely than the expression of anger. Advertisers, brands and companies running campaigns on Facebook pages can therefore feel more assured that users are more likely to like than to dislike their products and postings.

Figure 7.2 shows an example of the problem of Facebook’s like-ideology. Many people liked a posting on the Facebook page of the Auschwitz Memorial page that says that on 1 November 1942, 659 Durch Jews were killed in the gas chambers in Auschwitz.\(^10\) One can assume that most of the users who pressed “like” are not neo-Nazis, but rather wanted to express their dismay about what had happened. Facebook’s “happy-go-like” ideology does not allow for expressing negative emotions. It turns Auschwitz mourners into Auschwitz likers. Likes sell, whereas dislikes contain the risk that companies obtain negative assessments. So it is more profitable for Facebook, by design, to make people like companies and also to make them “like” Auschwitz. “The page of the Auschwitz Memorial Museum on Facebook is a good example to sketch out how our social discourses are now subject to Facebook’s affirmation – if you want to be part of the new digital public, you need to be on Facebook” (Bunz 2013, 139).

Figure 7.3 shows an example of the re-designed reaction buttons from Coca-Cola’s Facebook page. Coca-Cola is one of the world’s largest corporations: In 2016 it was ranked number 83 in the Forbes list of the world’s largest transnational companies. Its 2015 profits amounted to US$ 7.3 billion.\(^11\) Given such profits, Coca-Cola can also invest a lot into its branding, marketing and advertising strategy. It is also one of the most powerful and most visible companies on Facebook: In late 2016, Coca-Cola’s Facebook page had around 100 million “Likes”. In the example posting, there are 97 emotional reactions to a posting that advertises the launch of Coca-Cola Zero Sugar: 91 “Likes”, 5 “Loves” and 1 “Haha”. There is no negative reaction. The design and structure of brand pages on Facebook invites positive and discourages negative reactions.

**THE LIBERAL FETISHISM OF PRIVACY**

Liberal privacy theories typically talk about the positive qualities that privacy entails for humans or speak of it as an anthropological constant in all societies, without discussing the particular role of privacy in capitalist society. Solove (2008, 98) summarizes the positive

---

9 ‘Dislike’ button coming to Facebook. BBC Online, 16 September 2015.
10 The “I like Auschwitz” Facebook example was introduced to academic discourse by Bunz (2013, 138).
values that have been associated with privacy in the existing literature: autonomy, counterculture, creativity, democracy, eccentricity, dignity, freedom, freedom of thought, friendship, human relationships, imagination, independence, individuality, intimacy, psychological well-being, reputation, self-development. The following values can be added to this list (see the contributions in Schoeman 1984a): emotional release, individual integrity, love, personality, pluralism, self-determination, respect, tolerance, self-evaluation, trust.

Analyses that associate privacy with universal positive values tend not to engage with actual and possible negative effects of privacy or the relationship of modern privacy to private property, capital accumulation and social inequality. They give unhistorical accounts of privacy by arguing that privacy is a universal human principle that brings about positive qualities for individuals and society. They abstract from issues relating to the political economy of capitalism, such as exploitation and income/wealth inequality. But if there are negative aspects of modern privacy, such as the shielding of income gaps and of corporate crimes, then such accounts are problematic because they neglect negative aspects and present modern values as characteristic for all societies.

Karl Marx characterized the appearance of the “definite social relation between men themselves” as “the fantastic form of a relation between things” (Marx 1867, 167) as fetishistic thinking. Fetishism mistakes phenomena that are created by humans and have social and historical character as being natural and existing always and forever in all societies. Phenomena such as the commodity are declared to be “everlasting truths” (Marx 1867, 175, fn. 34). Theories of privacy that do not consider privacy as historical, that do not take into...
account the relation of privacy and capitalism or only stress its positive role, can, based on Marx, be characterized as privacy fetishism. In contrast to privacy fetishism, Barrington Moore (1984) argues – based on anthropological and historical analyses of privacy – that it is not an anthropological need “like the need for air, sleep, or nourishment” (Moore 1984, 71), but “a socially created need” that varies historically (Moore 1984, 73). The desire for privacy, according to Moore, develops only in societies that have a public sphere that is characterized by complex social relationships, which are seen as “disagreeable or threatening obligation” (72). Moore argues that this situation is the result of stratified societies in which there are winners and losers. The alternative would be the “direct participation in decisions affecting daily lives” (79).

**PRIVACY FETISHISM IN RESEARCH ABOUT FACEBOOK**

A specific form of privacy fetishism can also be found in research about Facebook and social networking sites in general. The typical standard study of privacy on Facebook and other social networking sites focuses on the analysis of information disclosures by users (in many cases younger users). Bourgeois scholars argue that users’ privacy is under threat because they disclose too much information about themselves and thereby become targets of criminals and harassment. Such approaches see privacy as an individual phenomenon that can be protected if users behave in the correct way and do not disclose too much information. Such approaches ignore all issues relating to the political economy of Facebook, such as advertising, capital accumulation, the appropriation of user data for economic ends, and user exploitation. One can therefore characterize such analyses as Facebook privacy fetishism.

Marx has stressed that a critical theory of society does “not preach morality at all” (Marx and Engels 1846, 264) because human behaviour is an expression of the conditions individuals live in. Critical theorists “do not put to people the moral demand: love one another, do not be egoists, etc.; on the contrary, they are very well aware that egoism, just as much selflessness, is in definite circumstances a necessary form of the self-assertion of individuals” (264). The implication of uncritical analyses of social networking sites is moral condemnation and the simplistic conclusion that it is morally bad to make personal data public. Paraphrasing Marx, critical theorists, in contrast, do not put moral demands on users not to upload personal data to public Internet platforms, because they are very well aware that this behaviour is, under capitalist circumstances, a necessary form of the self-assertion of individuals. More than that, uploading and sharing information about oneself is also a form of communication, by which humans connect to others. The reason why many users do not find the idea of keeping their profiles invisible and closed infeasible is that they want to be seen and contacted by others.

One can also characterize Facebook privacy fetishism as victimization discourse. Such research concludes that social networking sites pose threats that make users potential victims of individual criminals, such as in the case of cyberstalking, sexual harassment, threats by mentally ill persons, data theft, data fraud and so on. Frequently, these studies also advance the opinion that the problem is a lack of individual responsibility and knowledge, and that as a consequence users put themselves at risk by putting too much private information online and not making use of privacy mechanisms, for example by making their profile visible for...
Facebook

all other users. One problem of the victimization discourse is that it implies young people are irresponsible, passive and ill informed, that older people are more responsible, that the young should take the values of older people as morally superior and as guidelines, and especially that there are technological fixes to societal problems. It advances the view that increasing privacy levels will technologically solve societal problems and ignores that this might create new problems because decreased visibility may result in less fun for the users, fewer contacts and therefore less satisfaction, as well as in the deepening of information inequality. Another problem is that such approaches implicitly or explicitly conclude that communication technologies as such have negative effects. These are pessimistic assessments of technology that imply that it carries are inherent risks.

The causality underlying these arguments is one-dimensional: it assumes that technology causes only one negative effect on society. But both technology and society are complex, dynamic systems (Fuchs 2008a). Such systems are to a certain extent unpredictable and their complexity makes it unlikely that they will have only one effect (2008a). It is much more likely that there will be multiple, at least two, contradictory effects (2008a). The techno-pessimistic victimization discourse is also individualistic and ideological. It focuses on the analysis of individual usage behaviour without seeing or analysing how this use is conditioned by the societal context of information technologies, such as surveillance, the global war against terror, corporate interests, neoliberalism and capitalist development.

In contrast to Facebook privacy fetishism, Critical Internet Studies’ task is to analyse Facebook privacy in the context of the political economy of capitalism.

7.4 PRIVACY AND THE POLITICAL ECONOMY OF FACEBOOK

PRIVACY AND PRIVATE PROPERTY

Karl Marx positions privacy in relation to private property. The liberal concept of the private individual and privacy would see man as “an isolated monad, withdrawn into himself. […] The practical application of the right of liberty is the right of private property” (Marx 1843c, 235). Modern society’s constitution would be the “constitution of private property” (Marx 1843a, 166).

For Hannah Arendt, modern privacy is an expression of a sphere of deprivation, where humans are deprived of social relations and “the possibility of achieving something more permanent than life itself” (Arendt 1958, 58). “The privation of privacy lies in the absence of others” (58). Arendt says that the relation between private and public is “manifest in its most elementary level in the question of private property” (61).

Habermas (1989c) stresses that the modern concept of privacy is connected to the capitalist separation of the private and public realms. Habermas sees privacy as an illusionary ideology – “pseudo-privacy” (157) – that in reality functions as a community of consumers (156) and enables leisure and consumption as a means for the reproduction of labour power so that it remains vital, productive and exploitable (159).

The theories of Marx, Arendt and Habermas have quite different political implications, but all three authors stress the importance of addressing the notions of privacy, the private
sphere and the public by analysing their inherent connection to the political economy of capitalism. A critical analysis should not simply discuss privacy on Facebook as the revelation of personal data, but also inquire into the political economy and ownership structures of personal data on Facebook. Most contemporary analyses of privacy on web 2.0 and social networking sites neglect this dimension that Marx, Arendt and Habermas stressed. These three authors remind us that it is important to focus on the political economy of privacy when analysing Facebook.

Facebook is a capitalist company. Therefore its economic goal is to achieve financial profit. It does so with the help of targeted personalized advertising, which means that it tailors advertisements to the consumption interests of the users. Social networking sites are especially suited for targeted advertising because they store and communicate a vast amount of personal likes and dislikes of users that allow surveillance of these data for economic purposes and to identify and calculate which products the users are likely to buy. This explains why targeted advertising is the main source of income and the business model of most profit-oriented social networking sites.

Facebook uses mass surveillance because it stores, compares, assesses and sells the personal data and usage behaviour of several hundred million users. But this mass surveillance is personalized and individualized at the same time, because the detailed analysis of the interests and browsing behaviour of each user and the comparison to the online behaviour and interests of other users allow Facebook to sort the users into consumer interest groups and to provide each individual user with advertisements that, based on algorithmic selection and comparison mechanisms, are believed to reflect the users’ consumption interests. Facebook surveillance is mass self-surveillance (Fuchs 2011a). Mass self-surveillance (Fuchs 2011a) is the shadow side of mass self-communication (Castells 2009) under capitalist conditions. The users’ permanent input and activity is needed for this form of Internet surveillance to work. The specific characteristics of web 2.0, especially the upload of user-generated content and permanent communicative flows, enable this form of surveillance.

In order to understand the political economy of Facebook, one needs to analyse both its legal-political framework and its accumulation model.

**FACEBOOK’S PRIVACY POLICY**

The use of targeted advertising and economic surveillance is legally guaranteed by Facebook’s privacy policy. In this section of the chapter, I will conduct a qualitative analysis of those parts of the Facebook data policy that are focused on advertising.]

Facebook can largely regulate itself in what it wants to do with user data because it is a company that is legally registered in Palo Alto, California, USA. Facebook’s data policy is a typical expression of a self-regulatory privacy regime, in which businesses largely define themselves by how they process personal user data. The general perception in privacy and surveillance studies is that there is very little privacy protection in the United States and that the United States lags behind Europe in protecting privacy (Tavani 2010, 166; Wacks 2010, 124; Zureik and Harling Stalker 2010, 15). Also, US data protection laws only cover government databanks and, due to business considerations, leave commercial surveillance

---

12 Facebook Data Policy, version from 30 January 2015.
untouched in order to maximize profitability (Ess 2009, 56; Lyon 1994, 15; Rule 2007, 97; Zureik 2010, 351).

Facebook’s terms of use and its data policy are characteristic of the liberal US data protection policies that are strongly based on business self-regulation. They also stand for the problems associated with a business-friendly self-regulatory privacy regime – if privacy regulation is voluntary, the number of organizations engaging in it tends to be very small (Bennett and Raab 2006, 171): “Self-regulation will always suffer from the perception that it is more symbolic than real because those who are responsible for implementation are those who have a vested interest in the processing of personal data.” “In the United States, we call government interference domination, and we call marketplace governance freedom. We should recognize that the marketplace does not automatically ensure diversity, but that (as in the example of the United States) the marketplace can also act as a serious constraint to freedom” (Jhally 2006, 60).

Joseph Turow (2006, 83–84) argues that privacy policies of commercial Internet websites are often complex, written in turgid legalese, but formulated in a polite way. They would first assure the user that they care about his/her privacy and then spread over a long text advance elements that mean that personal data is given to (mostly unnamed) “affiliates”. The purpose would be to cover up the capturing and selling of marketing data. Turow’s analysis can be applied to Facebook. In another work, Turow (2011, 190) argues that targeted online advertisers create “reputation silos: flows of advertising, information, entertainment, and news designed to fit profiles about individuals and people who statistically seem similar”. Consumer culture would have resulted in a shift from society-making media to segment-making media:

Segment-making media are media that encourage small slices of society to talk to themselves, while society-making media are those that have the potential to get all those segments to talk to each other. […] [Segment-making media allow advertisers] to search out and exploit differences between consumers. (Turow 2011, 193)

**PRIVACY POLICY**

Facebook wants to assure users that it deals responsibly with their data and that users are in full control of privacy controls. Therefore as an introduction to the privacy issue, it wrote: “We give you the power to share as part of our mission to make the world more open and connected.” Facebook uses targeted advertising in which it sells user data to advertisers: “We want our advertising to be as relevant and interesting as the other information you find on our Services. With this in mind, we use all of the information we have about you to show you relevant ads.”

In its privacy policy Facebook avoids speaking of selling user-generated data, demographic data and user behaviour. It instead uses the phrase “sharing information” with third parties (“third parties we can share information with about you”), which is a euphemism for the commodification of user data. The words sharing/share appear 36 times in 13 www.facebook.com/privacy/explanation.php (accessed on 9 November 2015).
Facebook’s data policy from January 2015, the terms sell/selling/sale/commodity not a single time.

**UNAMBIGUOUS CONSENT?**

There are no privacy settings on Facebook that allow users to disable advertisers’ access to their data (there are only minor privacy settings relating to “social advertising” in Facebook friend communities). Facebook does not ask users whether they find targeted advertising necessary and agree to it.

Facebook in general uses targeted advertising. There is an opt-out in the advertising preferences option for Facebook’s use of data from across the web (e.g. which websites a user visits and which apps s/he uses on her/his mobile phone). Even if one opts out from this option, Facebook continues to target ads based on the user’s Facebook behaviour and profile data and continues to present the same amount of ads.

“If you turn off online interest-based adverts you’ll still see the same number of adverts, but they may be less relevant to you.” Facebook assumes that its targeting algorithm can calculate and predict interests and tastes. Its strategy excludes that some users may not at all want to have their data monitored, analysed and commodified.

Users must agree to the privacy terms in order to be able to use Facebook and thereby they agree to the use of their self-descriptions, uploaded data and transaction data to be sold to advertising clients. Given the fact that Facebook is the second most used web platform in the world, it is unlikely that many users refuse to use Facebook because doing so will make them miss the social opportunities to stay in touch with their friends and colleagues, to make important new contacts, and may result in being treated as outsiders in their communities. Facebook coerces users into agreeing to the use of their personal data and collected user behaviour data for economic purposes.

If you do not agree to the privacy terms that make targeted advertising possible, you are unable to use the platform. Users are not really asked if their data can be sold to advertisers, therefore one cannot speak of user consent. Facebook utilizes the notion of “user consent” in its privacy policy in order to mask the commodification of user data as consensual. It bases its assumption on a control theory of privacy and assumes that users want to sacrifice consumer privacy in order to be able to use Facebook.

**EXPLOITATION ON FACEBOOK**

Based on Dallas Smythe’s (1977, 1981/2006) notion of the audience commodity, the concept of the Internet prosumer commodity was introduced in section 5.3 of this book. Internet prosumer commodification in combination with economic surveillance that enables targeted advertising is at the heart of many commercial social media’s capital accumulation strategy.

**COMMODIFICATION AND DIGITAL LABOUR ON FACEBOOK**

Surveillance on Facebook is surveillance of prosumers, who dynamically and permanently create and share user-generated content, browse profiles and data, interact with others,

---

14 Facebook adverts settings (accessed on 9 November 2015).
join, create and build communities, and co-create information. The corporate web platform operators and their third-party advertising clients continuously monitor and record personal data and online activities; they store, merge and analyse collected data. This allows them to create detailed user profiles and to know about the personal interests and online behaviours of the users. Facebook sells its prosumers’ data as a commodity to advertising clients. Money is exchanged for the access to user data that allows economic surveillance of the users. The exchange value of the Facebook data commodity is the money value that the operators obtain from their clients. Its use value is the multitude of personal data and usage behaviour that is dominated by the commodity and exchange value form. Corporations’ surveillance of the prosumers’ permanently produced use values, that is personal data and interactions, allows targeted advertising that aims at luring the prosumers into consumption and at manipulating their desires and needs in the interest of corporations and the commodities they offer.

First, corporate platform operators commodify Facebook users’ data. The latter are sold as commodities to advertising clients. Second, this process results in the users’ intensified exposure to commodity logic. They are double objects of commodification: the products of their subjectivity are commodities and through this commodification their consciousness becomes, while online, permanently exposed to commodity logic in the form of advertisements. Most online time is advertising time. On Facebook, targeted advertising makes use of users’ personal data, interests, interactions, information behaviour, and also interactions with other websites. So while you are using Facebook, it is not just you interacting with others and browsing profiles – all of these activities are framed by advertisements presented to you. These advertisements come about by permanent surveillance of your online activities. Such advertisements do not necessarily represent consumers’ real needs and desires because the ads are based on calculated assumptions, whereas needs are much more complex and spontaneous. The ads mainly reflect marketing decisions and economic power relations: the ads do not simply provide suggestions to buy certain commodities, they provide suggestions by companies that have enough money for buying advertising for specific commodities, whereas other companies or non-profit organizations cannot purchase ads, which shows how selective and driven by financial power advertising actually is.

7.5 EDWARD SNOWDEN AND THE SURVEILLANCE-INDUSTRIAL COMPLEX

SURVEILLANCE

David Lyon (2015, 3) defines surveillance as “any systematic and routine attention to personal details, whether specific or aggregate, for defined purpose. That purpose, the intention of the surveillance practice, may be to protect, understand, care for, ensure entitlement, control, mange or influence individuals or groups”. There are several problems which such a general definition of surveillance (Fuchs 2011c, 2013a). When a Nazi henchman monitors Jews in Auschwitz who are sent to the gas chamber on the next day, then given this definition, this is a form of surveillance. But also operating a babyphone that monitors a sleeping baby, an electrocardiogram or an earthquake detection system are seen as forms of surveillance. Such a broad concept of surveillance is not suited for a critical theory of society. For countering this
tendency, we need a purely negative concept of surveillance, in which surveillance is a specific form of control that forms one dimension of domination, exploitation, class, capitalism, patriarchy, racism, and similar negative phenomena (Fuchs 2011c, 2013a). Just like Adorno (1973/2003) was calling for a negative dialectic, we need based on Foucault and Marx negative surveillance studies. A problem of the general understanding of surveillance is also that it makes surveillance categorically synonymous with information collection and processing so that no differentiation can be drawn between surveillance theory and information theory. Thomas Mathiesen (2013, 17–18, 23) therefore draws a distinction between information systems and surveillance systems. Surveillance stems etymologically from the French term “surveiller”, which means to oversee and watch over. Watching over implies that there is a social hierarchy between persons, in which one person exerts power over the other.

Michel Foucault did not give a clear definition of surveillance, but he characterized it as a negative and repressive form of power. For Foucault, surveillance is a form of disciplinary power. Disciplines are “general formulas of domination” (Foucault 1977, 137). Disciplinary power includes penal mechanisms (177), it encloses humans into institutions such as schools, orphanages, training centres, the military, towns, factories, prisons, reformatories, houses of correction, psychiatry, hospitals, asylums and so on in order to control their behaviour, to partition and rank them (141–149; see also 1994, 57–58, 75–76) and to normalize, punish, hierarchize, homogenize, differentiate and exclude (Foucault 1977, 183–184). Foucault argues that in order to secure domination, disciplines make use of certain methods such as the hierarchical observation, the normalizing judgement and the examination (170–194). Surveillance is based on “a principle of compulsory visibility” that is exercised through the invisibility of disciplinary power (187), it “must see without being seen” (171), is “capable of making all visible, as long as it could itself remain invisible” (214), it is a “system of permanent registration” (196) in which “all events are recorded” (197), a “machine for dissociating the see/being seen dyad” (202).

Surveillance is the systematic collection and use of information in order to dominate individuals and groups. It can operate as a mere threat and be overt in order to discipline behaviour. Or it can be covert so that it is unknown that it takes place. In any case it is a form of domination, that is a social relation, in which one group or individual derives power (money, control, influence, reputation) at the expense of others. Marx had the insight that accumulation is a key principle of modern society. Generalizing Marx’s analysis of capitalism, we can say that modern domination aims at the accumulation of money (economic power), decision-power (political power) and reputation/definition-power (cultural and ideological power). Combining Marx and Foucault, we can say that surveillance is a systematic collection and use of information for the accumulation of power (see also Fuchs 2013a).

CORPORATE AND STATE SURVEILLANCE

The dominant forms of surveillance in modern society are a) corporate surveillance of workers, consumers, applicants and competitors, and b) state surveillance of citizens as well as of perceived internal and external enemies of the state. Corporate and state surveillance are also interlinked: the state may collaborate with private security technology and service providers. It can obtain access to data gathered by corporations. Corporations’ economic surveillance activities are to certain degrees enabled and constrained by state laws. The regulation of surveillance refers, for example, to questions like: Are employers allowed to use CCTV camera surveillance at workplaces for monitoring employees? Should the surveillance of consumer
behaviour for advertising purposes be legal or illegal? What is the penalty for industrial espionage? Should it be legal that employers search for data about job applicants and base their employment decisions on these data?

Economic surveillance has a relation to the state’s role in internal and external defence. Internal defence involves activities like policing, the prison system and intelligence activities directed towards a state’s citizens. Policing relates to property questions by guaranteeing the protection of private property. Property crime is one specific type of crime. Surveillance of citizens is used for locating people who have committed property crimes and increasingly also for pre-emptive purposes, which raises questions about the legal principle of the presumption of innocence: all citizens are considered to be potential criminals until proven not guilty by pre-emptive surveillance methods. The prison system makes use of surveillance of criminals in order to hinder them escaping. Internal intelligence makes use of surveillance technologies for monitoring the activities of citizens and political groups that are under suspicion of actually or potentially questioning the foundations of the state system. The history of the working-class movement has also been accompanied by a history of surveillance of this movement. Examples are the surveillance and control of trade unionists, communists and social democrats in the McCarthy era, and the systematic surveillance of socialist and civil rights organizations in the US COINTELPRO (Counter Intelligence Programme). Surveillance of socialist movements and for the defence of property rights has a relatively direct link to the capital accumulation cycle, although it is part of the political system. It protects from disruption of the capital accumulation cycle by protests or the disappearance of resources.

External defence and intelligence is related to the opposition of the state to external threats by military means. Surveillance here is the surveillance of other nation states, institutions and political groups in other countries. It serves predominantly the defence of the existence of the nation state. Any war or external threat is always a threat to the whole societal system. It is also a threat to the capitalist economy. So surveillance for reasons of external defence in capitalist societies is also a defence of the capitalist economy, just as it is a defence of the state, the educational system, the health care system, the welfare system and so on. It indirectly serves capitalist purposes.

It is important to stress that the state is not always a “class state” that serves capitalist interests by conducting and enabling surveillance. Given the right kind of government, states can also pass legislation that protects consumers’ and employees’ privacy from surveillance that serves corporate interests. The state, for example, has the power to potentially ban or considerably limit all workplace surveillance and consumer surveillance, and to thereby strengthen privacy rights. This requires, however, consumer- and worker-oriented politics.

THE SURVEILLANCE STATE

The security industry has especially been growing since 9/11 (Lyon 2003, 2007), which resulted in an increased interest in the application of surveillance technologies that is guided by the technological-deterministic belief that crime and terrorism can best be stopped by creating a surveillance society. David Lyon (2007, 184) suggests that the welfare state is being superseded by “the safety state”. There is an increased focus on law and order politics. 9/11 has resulted legally in the definition of “states of exception”,
“most notably for preemptive war, domestic surveillance, and the torture of terrorist suspects; and practically” in “the establishment of elaborate surveillance rituals for citizens (for example, airport screening) and the outsourcing of lucrative security contracts to private industries” (Monahan 2010, 6). “Capturing terrorists before they strike became an obsessive goal of many governments after 9/11” (Lyon 2003, 52). Since 9/11, also European security politics have “been mainly oriented towards the right for governments to strengthen coercive and surveillance security measures” (Bigo 2010, 265–266).

Stuart Hall et al. (1978) describe how a moral panic about street robbery (“mugging”) developed in the UK in the 1970s. They argue that this panic must be seen in the context of the crisis of the mid-1970s. Hall et al. (1978) stress that the moral panics of the 1970s were used for creating and enforcing law and order politics that not only tackled criminals, but especially the working class, the black working class and social movements. The result was the rise of what Hall calls a “law & order society”. In the political constellation characterizing the first decade of the twenty-first century, something comparable happened: 9/11 was indicative of a crisis of the hegemony of Western thought that was questioned by people and groups in Arab countries that put religious ideology against Western liberal and capitalist ideology.

The “war against terror”, the security discourse and the intensification of surveillance resulted in a political crisis, in which war and terrorism tend to reinforce each other mutually, which results in a vicious cycle that intensifies hatred and conflict. Financialization and neoliberalism made capitalism more unjust (which constitutes a social crisis) and also crisis-prone, which resulted in a new world economic crisis that started in 2008. Western societies have faced a multidimensional crisis in the first two decades of the twenty-first century. One of the ideological responses was to erect a surveillance society that is based on law and order politics and omnipresent surveillance. This new surveillance not only tackles criminals and terrorists, but erects a visibility of everyone and everything that also allows (actually or potentially) the control of political protests (that are on the rise in situations of crisis), which not only undercuts the liberal values of freedom of speech and assembly and thereby shows how modern society contradicts and limits its own values on which it is built.

Thomas Mathiesen (2013, 61) argues that three “new enemy images replaced the enemy image of communism when this vanished or lost its impetus towards the end of the 1980s”: “the struggle against terrorism, the struggle against organized crime, and the effective control of the EU’s common external borders”. The exaggerated public presentation of these enemy images would have resulted in a constant extension and intensification of surveillance. Key terrorist events would have resulted in law and order politics and more surveillance as responses, which, however, would only have prevented further terrorism in single cases. Mathiesen argues for strengthening human security in the form of democracy and social security as the best antidotes to violence. Writing several months before Edward Snowden made his revelations in June 2013, Mathiesen (2013, 155) argued that the “development of mass surveillance systems covering ‘everyone’ may be viewed as a final surveillance stage”.

SNOWDEN’S REVELATIONS AND THE SURVEILLANCE SOCIETY

Surveillance is not just a necessary feature of capitalism, but also an inherent feature of modern society and modern politics: it involves activities of state institutions such as secret services and the police that monitor criminals, political activists, enemies of the state, as well as
companies that track workers, customers and competitors. The purpose is not only to collect
data, but to use this data to exert social control. The rise of consumer culture and computing
have in the twentieth century brought about some qualitative changes of surveillance such
that it has become more networked, ubiquitous, focused on everyday life and consumption,
and organized in real time.

In June 2013, Edward Snowden revealed with the help of the Guardian the existence
of large-scale Internet and communications surveillance systems such as Prism, XKeyscore
and Tempora. According to the leaked documents, the National Security Agency (NSA),
a US secret service, in the PRISM programme obtained direct access to user data from
seven online/ICT companies: AOL, Apple, Facebook, Google, Microsoft, PalTalk, Skype
and Yahoo! The Powerpoint slides that Edward Snowden leaked refer to data collection
“directly from the servers of these U.S. Service Providers”. Snowden also revealed the
existence of a surveillance system called XKeyScore that the NSA can use for reading
emails, tracking web browsing and users’ browsing histories, monitoring social media activ-
ity, online searches, online chat, phone calls and online contact networks, and following
the screens of individual computers. According to the leaked documents, XKeyScore can
search both meta-data and content data. The documents that Snowden leaked also showed
that the Government Communications Headquarters (GCHQ), a British intelligence agency,
monitored and collected phone and Internet communications data from fibre optic cables and
shared such data with the NSA. According to the leak, the GCHQ, for example, stores phone
calls, emails, Facebook postings and the history users’ website access for up to 30 days and
analyses these data. Further documents indicated that, in co-ordination with the GCHQ,
also intelligence services in Germany (Bundesnachrichtendienst, BND), France (Direction
Générale de la Sécurité Extérieure, DGSE), Spain (Centro Nacional de Inteligencia, CNI) and
Sweden (Försvarets radioanstalt, FRA) developed similar capacities.

David Lyon (2015, 18–20) gives a comprehensive overview of the surveillance practices
that Snowden uncovered by distinguishing three levels of surveillance: the surveillance of
a) data from physical cables that transport communications data, b) user data stored by com-
munications companies such as AOL, Apple, Facebook, Google, Microsoft, PalTalk, Skype
or Yahoo!, c) data on individual computers with the help of spyware. Computer-mediated
communication requires the transmission of data from one computer to at least one other via
a network. So individual computers are involved that connect via networks.

15 NSA Prism program taps in to user data of Apple, Google and others. Guardian online. 7 June 2013.
16 Ibid.
17 XKeyscore: NSA tool collects ‘nearly everything a user does on the internet’. Guardian online. 31
July 2013. www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data (accessed
26 September 2016).
18 GCHQ taps fibre-optic cables for secret access to world’s communications. Guardian online.
21 June 2013. www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-
19 Ibid.
20 GCHQ and European spy agencies worked together on mass surveillance. Guardian online. 1
November 2013. www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-
surveillance-snowden (accessed 26 September 2016).
applications that run on the Internet and/or individual computers enable online communication. Part of the data also tends to be stored online on servers (“in the cloud”). The surveillance-industrial Internet complex that Snowden uncovered is capable of conducting surveillance at all levels of computer-mediated communication: individual computers, communications companies’ servers and network cables. The conducted surveillance is, according to Lyon (2015, 80–89), automated, anticipatory (the use of predictive analytics for predicting who could be or become a terrorist, which puts innocent people at risk of being suspected of terrorism, undermines the liberal principle of the presumption of innocence and relies on algorithms that are error-prone) and adaptive (data and meta-data generated in certain contexts are put together, repurposed and decontextualized).

Various scholars have worked on the critical analysis of Internet and social media surveillance (Andrejevic 2007, 2013; Fuchs and Trottier 2015; Fuchs et al. 2012; Mathiesen 2013; Trottier 2012, 2014; Trottier and Fuchs 2015). Given the intensification and extension of surveillance and law and order politics and surveillance ideology since 9/11 (Ball and Webster 2003; Chomsky 2011; Lyon 2003; Mathiesen 2013; Rockmore 2011), Snowden’s revelations did not come as a surprise. The Internet surveillance that the NSA and other secret services conduct are forms of Deep Packet Inspection surveillance that have been analysed before Snowden (Fuchs 2013b). What came as a surprise for many, however, was the extent and dimensions Internet surveillance has taken on. We can therefore without a doubt assert that the twenty-first century information society is not just a capitalist society, but also a mass surveillance society.

THE SURVEILLANCE-INDUSTRIAL COMPLEX AND THE POWER ELITE

Edward Snowden’s revelations about the existence of surveillance systems such as Prism, XKeyScore and Tempora have shed new light on the extension and intensity of state institutions’ Internet and social media surveillance. The concept of the military-industrial complex stresses the existence of collaborations between private corporations and the state’s institutions of internal and external defence in the security realm. C. Wright Mills argued in 1956 that there is a power elite that connects economic, political and military power:

There is no longer, on the one hand, an economy, and, on the other hand, a political order containing a military establishment unimportant to politics and to money-making. There is a political economy linked, in a thousand ways, with military institutions and decisions. […] there is an ever-increasing interlocking of economic, military, and political structures. (Mills 1956, 7–8)

Edward Snowden has confirmed that the military-industrial complex contains a surveillance-industrial complex (Hayes 2012), in which social media are entangled: Facebook and Google each have more than 1 billion users and have likely amassed the largest collection of personal data in the world. They and other private social media companies are first and foremost advertising companies that appropriate and commodify data on users’ interests, communications, locations, online behaviour and social networks. They make profit out of data that users’ online activities generate. They continuously monitor usage behaviour for this economic purpose. Vincent Mosco (2014) speaks of a military information complex (7)
in which surveillance capitalism and the surveillance state interact (10): both capitalism and
the state engage in mass surveillance of communications so that big data is “big surveillance” (146). David Lyon (2015, 13) argues that Snowden’s revelations show that “surveillance is
carried out by government and commercial agencies acting together. […] Big government
and big business dominate these processes”.

Since 9/11 there has been a massive intensification and extension of surveillance that is
based on the naïve technological-deterministic surveillance ideology that monitoring technol-
ologies, big data analysis and predictive algorithms can prevent terrorism. The reality of the
murder of a soldier that took place in the South-East London district of Woolwich in May 2013
shows that terrorists can use low-tech tools such as machetes for targeted killings. High-tech
surveillance will never be able to stop terrorism because most terrorists are smart enough not to
announce their intentions on the Internet. It is precisely this surveillance ideology that has cre-
ated intelligence agencies’ interest in the big data held by social media corporations. Evidence
has shown that social media surveillance not just targets terrorists, but has also been directed
at protestors and civil society activists.21 State institutions and private corporations have long
collaborated in intelligence, but the access to social media has taken the surveillance-industrial
complex to a new dimension: it is now possible to obtain detailed access to a multitude of citi-
zens’ activities in converging social roles conducted in converging social spaces.

Yet the profits made by social media corporations are not the only economic dimen-
sion of the contemporary surveillance-industrial complex: the NSA has subcontracted and
outsourced surveillance tasks to approximately 2000 private security companies22 that
make profits by spying on citizens. Booz Allen Hamilton, the private security company
that Edward Snowden worked for until recently, is just one of these firms that follow
the strategy of accumulation-by-surveillance. According to financial data,23 it had 22,500
employees in 2015 and its profits increased from US$25 million in 2010 to US$84 million
US$233 million in 2015. Surveillance is big business, both for online companies and those
conducting the online spying for intelligence agencies.

Users create data on the Internet that is private, semi-public and public. In the social
media surveillance-industrial complex, companies commodify and privatize user data as pri-
vate property, and secret services such as the NSA driven by a techno-determinist ideology
obtain access to the same data for trying to catch terrorists that may never use these technolo-
gies for planning attacks. For organizing surveillance, the state makes use of private security
companies that derive profits from organizing the monitoring process.

User data is in the surveillance-industrial complex first externalized and made public or
semi-public on the Internet in order to enable users’ communication processes, then privat-
ized as private property by Internet platforms in order to accumulate capital, and finally par-
ticularized by secret services who bring massive amounts of data under their control that are
made accessible and analysed worldwide with the help of profit-making security companies.

on-occupy-activists (accessed on 27 September 2016).
post.com/top-secret-america/articles/a-hidden-world-growing-beyond-control (accessed on 27
September 2016).
23 Booz Allen Hamilton. SEC filings, form 10-K for various years.
With the rise of digital media and networked communication technologies, it has become easier for everyday people to conduct surveillance. Everyone can easily turn a mobile phone into a tool for audio-visual surveillance. It is, however, a mistake to assume that surveillance thereby has become “democratic” or “participatory”. The Snowden case shows that big corporations and big state institutions dominate surveillance. They have more powerful surveillance technologies than others and legal rights that enable them access to data that others have no access to. So although information technologies have become more decentralized and networked, big government and big corporations understand how to use them for big surveillance and big data surveillance.

Thomas Mathiesen therefore argues that the polyoptical communication of social media and networked media, in which there are multiple sources of information, have not abolished panoptic surveillance: “But the panoptical form has not disappeared. Power is still around. The blossoming of the several/many ways profile, the Polyoptical profile, has not supplanted the one-way phase, but has merged with – and you might say improved on – the one-way phase” (Mathiesen 2013, 44). In the surveillance-industrial complex, the world’s most powerful state institutions have collaborated with the world’s most powerful communications companies to implement totalitarian surveillance systems. It is a system that centralizes control by monitoring decentralized technologies with multiple technologies and networking the obtained data. The result is centralized surveillance that as whole is a sum that is larger than its parts.

DEEP PACKET INSPECTION SURVEILLANCE TECHNOLOGIES

The Internet surveillance technologies, whose existence Snowden uncovered, are so-called deep packet inspection surveillance technologies. Data transmission on the Internet is based on the TCP/IP Protocol (Transmission Control Protocol/Internet Protocol). TCP/IP is an application of the so-called Open-Systems Interconnection (OSI) Model of network data transmission to the realm of the Internet. Whereas the OSI Model consists of seven dimensions of transmission, TCP/IP maps these seven dimensions to five (Comer 2004; Stallings 1995).

Each device (like a computer or a printer) in a network connected to the Internet has a specific IP address. In the Internet protocol version 4 (IPv4), each IP address is a unique 32-bit long identifier (such as 170.12.252.3). For enlarging the available IP address space, the identifier length has been increased to 128 bit in version 6 of the Internet protocol (IPv6). In order for data to be transmitted over the Internet, a source and destination IP address are needed. If a user, for example, searches for data on Google, he enters a search keyword into the Google search box. This is at the application level.

At the TCP level, the Transmission Control Protocol (TCP) takes the data, adds a communication port number (an address, by which the application is addressed) and breaks the data into packets. TCP identifies ports, the sequence number of a packet and a checksum and provides a reliable transport service (Comer 2004, 386). At the IP level, the IP address of the destination is determined as well as the routing over the Internet are determined. The Internet Protocol (IP) “specifies addressing: IP divides each Internet address into a two-level hierarchy: the prefix of an address identifies the network to which the computer attaches, and the suffix identifies a specific computer on the network” (Comer 2004, 301). At the lower levels, the data is transmitted. The data is routed over the various routers of the Internet until it finally arrives in our example in Google’s network, where it is treated in the opposite sequence (from...
the lowest level to the highest layer) so that data that correlates with the search query is generated and is then in the same way sent back to the user who requested the information.

A TCP/IP packet is a “small, self-contained parcel of data sent across a computer network. Each packet contains a header that identifies the sender and recipient, and a payload area that contains the data being sent” (Comer 2004, 666). The payload is “the data being carried in a packet” (667), the header contains data like the network address of source and destination. In the TCP/IP protocol that the Internet uses, the packet is called an IP datagram. It consists of “a header that identifies both the sender and receiver and a payload area that contains the data being carried” (658).

Deep packet inspection (DPI) surveillance technologies are communications surveillance tools that are able to monitor the traffic of network data that is sent over the Internet at all seven layers of the OSI Reference Model of Internet communication, which corresponds to the five layers of the TCP/IP Protocol. This means that DPI surveillance includes the surveillance of Internet content data. Important features of DPI are the recognition of objects on the network that may trigger notification and manipulation (Mueller et al. 2012).

THE SURVEILLANCE-INDUSTRIAL COMPLEX

The events of 9/11 have resulted in “the misguided and socially disruptive attempts to identify terrorists and then predict their attacks” (Gandy 2009, 5).

In this generalized control society, governed by the managerial model, the ability to anticipate individual behaviour, identify the probability of a specific behaviour and construct categories based on statistical frequency is the common thread among the “styles” of marketing specialists, the ‘scores’ of financiers and the ‘profiles’ of the police. (Mattelart 2010, 184)

Policing looks for security by algorithms in a world of high insecurity. It advances a fetishism of technology – the belief that crime and terrorism can be controlled by technology. Technology promises an easy fix to complex societal problems. This explains the results that the security industry tends to justify the selling of surveillance technologies, such as DPI, with reference to the ideological assumption that more surveillance is needed for fighting crime and terror.

The post-9/11 situation has resulted not only in the intensification of surveillance (Lyon 2003), but at the same time in the growth of the security industry. DPI Internet surveillance as well as communication surveillance must be placed in the context of the post 9/11 moral panic about terrorism, the rise of a security-industrial complex, the new imperialistic vicious cycle of war and terrorism, and the neoliberal politics of privatization and commodification of everything.

The interconnection of state surveillance and corporate surveillance that is expressed in examples such as DPI surveillance must be seen in the context of the rise of neoliberal governmentality that has generalized the principles of markets, competition, the enterprise, commodification, individual responsibility and the ideology of the homo economicus to large realms of society. The capitalist economy has thereby become an important principle that governs the life and conduct of populations and interacts with other apparatuses of government such as the state. Surveillance in the climate of neoliberalism has taken on commercial forms and become a central principle of consumer culture. After 9/11, Western states tried to erect panoptic surveillance mechanisms in order to control and gain insights...
into the world population’s communication based on the naïve belief that technological methods of surveillance can prevent the societal problem of terrorism. The context of these surveillance state endeavours is the situation of neoliberal governmentality, which requires that states gain access to privately gathered data in order to build a panopticon that makes citizens’ communicative activities visible for the state. The visibility erected by companies is coupled to state activities. The results have been policies like the EU’s Data Retention Directive that requires EU Internet service providers and telecommunications companies to store identification and connection data of all users of phones and the Internet so that the police can gain access to data about suspected terrorist or criminal activities. Surveillance after 9/11 has acquired its own specific form of political economy that connects economic surveillance and state surveillance.

“The surveillance state […] now uses the dispersed systems and devices of surveillance society” (Lyon 2003, 37). Foucault uses the notion of governmentality for non-state forms of governing. In policing, governing the population has taken on a new governmentality regime that is based on the access of the state to surveillance data gathered by private actors and the state use of surveillance technologies produced by the capitalist security industry. The state–capital nexus is a central feature of the contemporary political economy of surveillance.

Ben Hayes (2009, 2010) speaks in this context of the emergence of the security-industrial complex. He argues that there is a “close bond between corporate and political elites in the homeland-security sector” and that on an ideological level one finds “the inherently neoconservative appeal to the defence of the homeland” (Hayes 2010, 148).

Neocon ideology is centred upon the “right to limitless profit-making”, which is at the very heart of the EU’s desire to create a lucrative Homeland Security industry. The EU’s security policies are premised on the neocon philosophy of global policing and intervention in failed states to both pre-empt “threats” to security and further the spread of the free market and western-style democracy around the world. (Hayes 2009, 7)

The security-industrial complex on the one hand wants to make a business out of developing military and surveillance technologies, and on the other hand advances the large-scale application of surveillance technologies and the belief in managing crime, terrorism and crises by technological means. DPI Internet surveillance is part of this political-economic complex that combines profit interests, a culture of fear and security concerns, and surveillance technologies.

7.6 CONCLUSION

We can summarize the main results of this chapter as follows:

- The modern concept of privacy is a highly individualistic ideology that legitimates private property relations and social inequality. It is a universal Enlightenment ideal that finds its own limit and its critique in capitalism’s immanent tendencies for the surveillance of employees and consumers in the economy and the surveillance of citizens by the state that enable the accumulation of money capital and power.
Facebook

- Facebook’s privacy policy is the legal mechanism that enables prosumer exploitation. It is complex, an expression of the self-regulatory US privacy regime and sugar-coats the surveillance of users’ personal data.
- Facebook’s capital accumulation model commodifies the digital labour of users.
- Edward Snowden has revealed that Facebook and other communications corporations are entangled in a surveillance-industrial complex that is driven by the combination of the corporate commodification and state surveillance of big data.

Ello: A Self-Proclaimed “Alternative” to Facebook

In 2014, the social network Ello presented itself as alternative to Facebook and to targeted advertising (“simple, beautiful & ad-free”), which attracted users and made it the 6,112th most accessed website in the world on 4 October 2014. On 10 February 2016, it had lost some popularity and was ranked at position 19,608. In February 2015, the news platform Vice asked: “Who the hell is still using Ello?” Ello’s capital accumulation model was to sell special features. Venture capital firm Fresh Tracks invested around US$435,000 into Ello in 2014. Ello in the same year also attracted venture capital of US$5.5 million from Bullet Time Ventures, the Foundry Group and FreshTracks Capital. It became a so-called B corporation (public benefit corporation). These are for-profit companies that “must create value for society, not just shareholders”. The B corporation concept is an ideology: every for-profit company is necessarily driven by the need to accumulate capital and to exploit labour. When it exploits labour it is definitely not doing good to society, but benefits a class of owner at the expense of workers. Ello has committed to not using advertising as Facebook does:

> Every post you share, every friend you make and every link you follow is tracked, recorded and converted into data. Advertisers buy your data so they can show you more ads. You are the product that’s bought and sold. We believe there is a better way. We believe in audacity. We believe in beauty, simplicity and transparency. We believe that the people who make things and the people who use them should be in partnership. We believe a social network can be a tool for empowerment. Not a tool to deceive, coerce and manipulate—but a place to connect, create and celebrate life. You are not a product.

Ello’s current privacy policy rules out advertising: “Ello does not make money from selling advertising on the site, serving ads to you, or selling information about our users to third parties, including advertisers, data brokers, search engines, or anyone else.” Ello published a charter that says:

---

26 Who the hell is still using Ello? Vice Online, 11 February 2015.
1) Ello shall never make money from selling ads; 2) Ello shall never make money from selling user data; and 3) In the event that Ello is ever sold, the new owners will have to comply by these terms. In other words, Ello exists for your benefit, and will never show ads or sell user data.\(^{30}\)

Once venture capital enters a company, there is pressure to sooner or later accumulate capital. So Ello needs to sell something as commodity. It can, for example, sell premium services, premium memberships, or wait until it has a large user base and then charge for access. In any case, it does not transcend the logic of labour-exploitation. In any of these cases, it exploits the employees or freelancers who produce these services for a wage and create not just the platform as use-value, but also the company’s (potential) profits. If such commodification strategies do not work, it may even be the case that Ello has to introduce advertising and to renounce its own manifesto promises. Even if Ello does not exploit users, it has to exploit some form of labour in order to make profits and to be profitable, which is also an imperative for a B company. Thus far the low level of success of Ello shows that it is difficult to compete with a monopoly capitalist such as Facebook. Given that there is little interest, no business model may work at all. Ello cannot be profoundly different from Facebook because it also follows a capitalist logic and can therefore only make profits by exploiting some form of labour. It can commit to not exploit users, but it cannot commit to not use exploitation as long as it is a for-profit company.

Ello is not fundamentally different from Facebook because both are capitalist social media. Being ad-free is not enough – the point is that you have to be non-capitalist in order to be an alternative to Facebook.

**DIASPORA*: AN ALTERNATIVE TO FACEBOOK?**

One strategy of socialist Internet politics is to establish and support non-commercial, non-profit Internet platforms. It is not impossible to create successful non-profit Internet platforms, as the example of Wikipedia – which is advertising-free, provides free access and is financed by donations – shows. The best-known alternative social networking site project is Diaspora*, which tries to develop an open source alternative to Facebook. Other examples are BuddyPress, Crabgrass, Cryptocat, Elgg, Friendica, kaioo, Lorea, N-1 and Occupii (see Allmer 2015; Cabello et al. 2013; Sevignani 2012, 2013, 2016). Diaspora* is a project created by four New York University students – Dan Grippi, Maxwell Salzberg, Raphael Sofaer and Ilya Zhitomirskiy. Diaspora* defines itself as a “privacy-aware, personally controlled, do-it-all, open source social network”.\(^{31}\) It is not funded by advertising, but by donations. The three design principles of Diaspora* are choice, self-ownership of data and simplicity.\(^{32}\)

The Diaspora* team is critical of the control of personal data by corporations. It describes Facebook as “spying for free”.\(^{33}\) The basic idea of Diaspora* is to circumvent

---

\(^{30}\) [https://ello.co/wtf/about/pbc/](https://ello.co/wtf/about/pbc/) (accessed on 10 November 2015).

\(^{31}\) [www.joindiaspora.com](http://www.joindiaspora.com) (accessed on 11 November 2010).


\(^{33}\) [Four nerds and a cry to arms against Facebook. *The New York Times* online, 10 March 2013 (accessed on 27 September 2016)].
the corporate mediation of sharing and communication by using decentralized nodes that store data that is shared with friends. Each user has his/her own data node that s/he fully controls. As Ilya Zhitomirskiy states: “On Diaspora, users are no longer dependent on corporate networks, who want to tell you that sharing and privacy are mutually exclusive.”

So Diaspora* aims to enable users to share data with others and at the same time to protect them from corporate domination and from having to sacrifice their data for corporate purposes in order to communicate and share. Diaspora* can therefore be considered as a socialist Internet project that practically tries to realize a socialist privacy concept. The Diaspora* team is inspired by the ideas of Eben Moglen, author of the *dotCommunist Manifesto* (2003). He says that an important political goal and possibility today is the “liberation of information from the control of ownership” with the help of networks that are “based on association among peers without hierarchical control, which replaces the coercive system” of capitalist ownership of knowledge and data (Moglen 2003). “In overthrowing the system of private property in ideas, we bring into existence a truly just society, in which the free development of each is the condition for the free development of all” (2003).

Diaspora* is explicitly a non-profit project. It is based on donations. On 10 February 2016 it was the world’s 355,396th most frequently visited website, whereas Facebook was the second most accessed site. This circumstance shows that there is an asymmetry between Facebook’s monopoly power and alternative social networks. Facebook’s users are socially “locked in” because they have invested a large labour of love, emotion and connection into their profiles. If they leave it, they may lose important contacts, content and advantages they have built up. They also only have limited time available to use multiple social networking sites. This puts alternative sites such as Diaspora* at a disadvantage. Diaspora* is also financially more volatile because it does not sell data, but rather depends on donations, which is a logic that transcends the commodity form, but is organized within a society ruled by instrumental reason.

Some Facebook users have diffuse feelings of discontent with Facebook’s privacy practices that have manifested themselves into groups against the introduction of Facebook Beacon, news feed, mini-feed and so on, the emergence of the web 2.0 suicide machine (http://suicidemachine.org/), or the organization of a Quit Facebook Day (www.quitfacebookday.com/). These activities are mainly based on liberal and Luddite ideologies, but if they were connected to ongoing class struggles against neoliberalism (like the ones that have taken place throughout the world in the aftermath of the new global capitalist crisis) and the commodification of the commons, they could grow in importance.

On Facebook, the “audience” is an exploited worker-consumer. How can socialist privacy protection strategies be structured? The overall goal is to drive back the commodification of user data and the exploitation of prosumers by advancing the decommodification of the Internet and society.

RECOMMENDED READINGS AND EXERCISES

For understanding Facebook, it makes sense to engage with its statement of rights and responsibilities, data use policy, financial statements as well as criticisms of the platform.

Read Facebook’s latest Statement of Rights and Responsibilities and discuss the following questions in groups. Ask yourself:

- What rights does Facebook have in relation to the content that you create on its services?
- If you feel you have been treated in an illegal manner by Facebook, how can you hold it legally reliable? Which court is responsible?
- Try to find more information on how national regulations (e.g. the ones in your home country) work for a global system like the Internet?

Read Facebook’s latest Data Use Policy and ask yourself the following questions:

- Make a systematic and ordered list of data that Facebook collects about users.
- Discuss which data Facebook uses for targeted advertising. Find out how this form of advertising works. Which data does Facebook use about you for targeted advertising?
- Are there mechanisms for limiting targeted advertising on Facebook? Do you think they are sufficient? Why? Why not?
- How do you politically assess targeted advertising?
- Are there alternative organization models for social media that do not use targeted advertising? Which ones? How do you think social media should best be organized?

Read Facebook’s latest Proxy Statement and its Annual Financial Report. You will find both on its website under SEC filings. Ask yourself:

- How does Facebook present itself in these documents?
- Try to make sense of and interpret the financial data presented in the reports. What do Google’s ownership structure and its financial operations look like?
- According to these reports, what role does advertising play in Facebook’s operations?

Work in groups and present the results of the following exercises to the class.

Facebook has faced a lot of criticism. These exercises focus on engagement with this criticism.

- Search for videos, documents, press releases, blog posts, etc. in which Facebook presents itself. What kind of image does Facebook construct of itself? What are the major themes in its discourse?
- Search for documents, interviews, news articles, reports by critical scholars, critical journalists, civil society representatives, privacy and data protection advocates, consumer protection advocates and organizations as well as watchdog organizations that criticize the topics that (Continued)
FACEBOOK

(Continued)

Facebook presented in a positive light in the material you found earlier. Summarize the basic points of criticism. Compare them to how Facebook presents itself. Discuss which assessments you find more convincing and provide reasons for your assessments.

- The initiative Europe vs. Facebook filed a complaint about Facebook to the Irish Data Protection Commissioner. First, read the basic complaint documents and the Irish Data Protection Commissioner’s audit. Conduct a search about how Facebook, Europe vs. Facebook and other data protection commissioners (e.g. Thilo Weichert in Germany and others) have reacted to the audit report. Document the discussion and its basic arguments. Position yourself on the involved political issues. Present your results.


These readings deal with the notion of surveillance in the context of computing. Read the texts and ask yourself:

- How should surveillance best be defined?
- What is the relevance of Michel Foucault’s works for studying surveillance?
- What is the panoptic sort? What is the synopticon?
- Do the panoptic sort and the synopticon matter for understanding social media? Try to find examples that you can analyse with the help of these concepts.
- What are aspects of the political economy of surveillance on social media? Try to give some examples.


212
Ask yourself:

- What are Arendt and Habermas’s basic criticisms of privacy? In which respect do these criticisms matter for understanding Facebook and other social media critically?
- In light of the criticisms of privacy, do you think there is anything that is politically valuable about this concept? If so, why and what? If not, why not?
- Discuss what the advantages and disadvantages of the privacy concept are and how they relate to Facebook and other social media.


Ask yourself:

- Make a systematic and ordered typology of characteristics of social media surveillance. Give a name to each dimension and take care that the dimensions are not overlapping. Constructing such a typology presupposes that you understand and can define the terms “social media” and “surveillance”.
- Have a look at your characteristics of social media surveillance. Give two examples that relate to specific platforms for each dimension.


Social networking sites like Diaspora* and N-1 are alternative social networking sites. Read first the given articles. Then make a list of ten alternative social networking sites. This presupposes that you have an understanding of what an alternative medium is. Ask yourself:

- What is an alternative medium? Discuss different meanings of the term and devise a working definition.

*(Continued)*
FACEBOOK

(Continued)

- In which respect can the social networking sites that you selected be considered as being alternatives to Facebook? What does the term “alternatives” mean here? In what respect are the platforms different from Facebook?
- Compare the terms of use and privacy policy of these platforms to the ones of Facebook. What are the differences and commonalities?


Ask yourself:

- What are the basic points of criticism of Facebook formulated by Douglas Rushkoff, Trebor Scholz and Richard Buchanan?
- Which strategies of resistance are mentioned? What commonalities and differences are there? What other strategies are there? What do you think about such strategies?
- One strategy is to demand a wage from Facebook for platform usage. This demand is based on the assumption that Facebook usage is labour that creates value. Another strategy is to build, use and support alternative non-commercial platforms such as Diaspora*. What are the differences between these strategies? What do you think about them? What are their ultimate goals?

Edward Snowden’s revelations about the existence of a surveillance-industrial Internet complex have given a new dimension to social media surveillance. Work in groups:

- Search for interviews with and talks by Edward Snowden and read, listen to and watch them. Ask yourself: Why did Snowden make these revelations? What does he see as the dangers of communications surveillance? What personal risks did he take? In which cases would you take personal risks for political reasons? Can you give examples?
- Do you think Edward Snowden is a hero who should be commended for letting the public know that our governments are running electronic surveillance programmes that threaten people’s privacy, or a villain who threatens the West’s national security by revealing secret services’ covert surveillance actions? Give reasons for your answers.

Read the following chapter in Thomas Mathiesen’s book Towards a Surveillant Society. Mathiesen is a Norwegian sociologist whose works have been very influential in the critical study of surveillance and in critical criminology. In this chapter, he describes the aftermath of Anders Breivik’s fascist terrorist attacks in Norway on 22 July 2011. Breivik first detonated a bomb in a government building in Oslo that killed eight people, and then shot dead 69 young social democrats on Utøya Island. Discuss in groups.

- What are possible responses to terrorism and organized crime? What are the most common responses?
- What are differences between right-wing and left-wing responses? How does Mathiesen position himself in this respect?
- How did Norway respond to the July 2011 terrorist attacks? If you compare it to the USA’s response to 9/11, what differences can be found? How do you assess the two different responses? Which one is more appropriate? Why?