12 Surveillance and sousveillance on Facebook: Between empowerment and disempowerment – Mateusz Bucholski

12.1 Introduction

It seems there is no end to the growth of social media. Facebook, in particular, enjoys its hegemonic position as the leading social networking site, with more than one and a half billion global monthly active users throughout 2015 (Facebook Newsroom, 2015). 71 per cent of all adult Internet users in the United States have used Facebook in 2014, which constitutes 58 per cent of the entire U.S. adult population (Duggan et al., 2015). The website has permeated many aspects of social, cultural, and economic life. It has equipped its users with new ways of online social interaction, governments with new means of communicating policies with the public opinion, and businesses and advertisers with a platform for reaching consumers faster and on a broader-than-ever scale. David Lyon (Bauman and Lyon, 2013), the leading scholar of international surveillance studies, observes: "Facebook has quickly become a basic means of communicating – of 'connecting', as Facebook itself rightly calls it – and is now a dimension of daily life for millions" (p. 35).

The effect of social networking and social media on mass popular culture of the modern world is undoubtedly immense. What is less clear, however, is the normative value and nature of Facebook. From its appearance on the Internet, the website has been an object of criticism pointing to the modern paradigm of individuals' lives being constantly exposed to the public gaze. The increasingly complex and decreasingly intelligible architecture of the globalising "technoscape" (Appadurai, 1990, p. 296) have created new means of surveillance. David Lyon (1994) has been at the forefront of this line of thinking, arguing together with Zygmunt

Bauman that modernity brought about the rise of a new Panoptic "surveillance society". Lyon sees Facebook as an exemplary modern surveillance system, designed for the purpose of collecting data about its users and turning it into commercial profits. The revelations about the global surveillance of Facebook users by the U.S. National Security Agency, exposed by Edward Snowden in 2013, seem to be a case in point. The international uproar that followed inspired many to reflect critically on the nature of social networking sites and to question their safety.

Contrastingly, technology and Internet enthusiasts are a lot more eager to promote social media. In their optimist narrative, Facebook (and the Internet in general) is "an arena for interactive democracy, critical expression, as well as a site of new identity formation" (Koskela, 2006, p. 165). The question remains how to see the role of surveillance in all this. Can surveillance have positive effects at all, and if so, what could they be? One answer is to turn the concept of surveillance on its head. Jean-Gabriel Ganascia (2010), for instance, talks about a "generalised *sousveillance*", which gives the user the opportunity to reverse the gaze and point it at their overseer. Ganascia proposes a reconceptualisation of the Panopticon into a "Catopticon" that "allows everybody to communicate with everybody and removes surveyors from the watchtower" (p. 489). Can this perspective of catoptic sousveillance be applied to Facebook?

This contribution aims to comparatively assess those two divergent perspectives in an attempt to answer the following central question: *To what extent is Facebook a system of panoptic surveillance or catoptic sousveillance?* The central question comprises two parts. I firstly reflect on whether Facebook can be seen as a system of surveillance and a Panopticon. Thereafter, I turn to the question of the Catopticon: Can Facebook be perceived as a system of sousveillance? Lastly, if Facebook can be theorised using both surveillance and sousveillance, what sort of synthesis can be

derived from these concepts? I analyse the contents of two documents underlying Facebook policy, the *Terms of Service* and the *Data Policy*. A Foucauldian toolbox is particularly useful here, since Foucault's reading of the Panopticon includes a reflection on the power dynamics within this mechanism. Surveillance is thus not only the condition of being watched, but also subjection to a certain power and discipline.

Following these lines, my focus does not shy away from a certain emphasis on power: surveillance and sousveillance both point to the concept of power and to (albeit divergent) power relations. I am interested not only in the content of the two analysed policy documents, but also in the implicit power relationships between Facebook and its users which may stem from their discourse. Power is defined by Foucault (1978) as a ubiquitous social relation: "Power is everywhere; not because it embraces everything, but because it comes from everywhere" (p. 93). It is not a "thing" which can be owned by individuals or the state, but rather a relation between people or groups in the social body (O'Farrell, 2005, p. 99). Thus, if surveillance is understood as a hierarchical dependency between the observer and the observed, then the gaze results in subjugating the latter and empowering the former. But the perspective of sousveillance reverses this power relation, and empowers the user of social media *vis-à-vis* Facebook. There no longer is a clear-cut dependency, but rather the idea that everyone can observe everyone in an egalitarian setting. This reversal of power relations is perhaps the clearest conceptual difference between surveillance and sousveillance. The answer to my central question, therefore, incorporates reflections on power within the concepts of surveillance and sousveillance.

The next chapter inspects Facebook's *Terms of Service* and *Data Policy*. This analysis is followed by a more detailed discussion of the Panopticon in chapter three. Chapter four turns to the concept of sousveillance, in order to see if Facebook can also be used productively, e.g.

to create new subjectivities, as argued by Ganascia (2010). My conclusion then attempts to theoretically reconcile the perspectives of surveillance and sousveillance, and discusses power relations inherent to these concepts.

12.2 Facebook's Terms of Service *and* Data Policy*: Content Analysis*

Privacy policies are certainly not amongst the most frequently read documents. They do, nevertheless, to a large extent determine the power relations between the user and the website, in particular by specifying what happens to user data and who retains control over them. When Facebook's terms hit media headlines, it is typically with an aura of intransparency and surveillance (cf. Vedantam, 2012; Smith, 2013; Lapowsky, 2014; Smith, 2015). Concern often revolves around the issue of who owns and controls user data, and how it is used. These are also my guiding motifs here. I firstly look at the *Terms of Service* (Facebook, 2015a), which specifically deal with the topics of privacy, data-sharing and safety. I then inspect the *Data Policy* (Facebook, 2015b), a *de facto* privacy policy intended to supplement the *Terms of Service* with a more detailed discussion of privacy.

12.2.1 Terms of Service

The *Terms of Service* analysed here have been last revised on January 30, 2015, and were the most recent, original U.S. English version in force at the time of my writing (Facebook, 2015a). The document is divided into eighteen sections, of which the first four: (1) "Privacy", (2) "Sharing Your Content and Information", (3) "Safety", and (4) "Registration and Account Security", prove to be most illuminating for a discussion of surveillance on Facebook. The "Privacy" section opens with an assertion: "Your privacy is very important to us" (para. 1). The document, together with the *Data Policy*, as it is explained, was designed with the aim to disclose how

Facebook collects and uses user data. In theory, this should help users make informed decisions about privacy. But is this really the case? Do these policies explain what Facebook does with user data – and who owns this data – clearly and exhaustively? I argue this is far from being clear.

The first hindrance is at the level of language. The *Terms of Service* are written in a legalistic, elitist, vague, brief and abstract manner, without the use of any practical examples that would provide a more relatable level of understanding for the user. Evidence thereof is found in the opening paragraph of section two ("Sharing Your Content and Information") which states: "[Y]ou grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP [intellectual property] content that you post on or in connection with Facebook". The meaning of this passage is hardly accessible to the non-specialist. What does this accumulation of adjectives entail? Firstly, a non-exclusive license (undefined in the *Terms of Service*) "grants to the licensee the right to use the intellectual property, but means that the licensor remains free to exploit the same intellectual property and to allow any number of other licensees to also exploit the same intellectual property" (Taylor and Wessing, n.d., para. 3). Thus, when the user provides Facebook with data about themselves, they share this data not only with Facebook, but also with an unspecified number of third parties who are never explicitly listed by name in the *Terms of Service*. The user cannot know what companies have the right to use their data, and for what purpose. Secondly, "transferable" entails Facebook can sell or otherwise grant the rights to access user data to third parties. This is confirmed by the adjective "sub-licensable". Thirdly, the user provides their data without any monetary compensation, e.g. in the form of a royalty fee. Lastly, the content shared with Facebook can be used by the company worldwide.

The above passage establishes a one-directional power dependency between Facebook and the user, in which the latter is clearly in a disadvantaged position. The user does not own their data, since they cannot govern it with awareness and agency. It is not the user who can control what rights they grant to Facebook in terms of data usage and access, but Facebook itself who dictates how, when, and with whom it wishes to share information. In other words, users no longer control their data in any meaningful way. Data becomes a commodity; acquired, sold, and resold without any conscious involvement of its righteous owner. There is an additional passage that sheds light on who is in control, not only of data but of users' Facebook accounts in their entirety: "You will not transfer your account . . . to anyone without first getting our written permission" (section 4, para. 9). The rationale behind this requirement is left unexplained. The question which thus comes to mind is: Who owns our online personas, and who has the power to control them? It seems that the user has little power in this respect. Evidence in support of this is found in section two, paragraph two: "removed content may persist in backup copies for a reasonable [unspecified] period of time". The user has no way of deleting once-uploaded data effectively. Therefore, how can privacy be "very important" to Facebook, when the users not only cannot know with whom the website shares their data, but have no means of deleting their content with an immediate and conclusive effect?

Another concern arises from reading paragraph four of section two:

> When you publish content or information using the Public setting, it means that you are allowing everyone, including people off of Facebook [non-users], to access and use that information, and to associate it with you (i.e., your name and profile picture).

The Public setting is the default setting for all new user accounts, which needs to be changed with a conscious effort on the side of the user, should they wish to retain a higher level of privacy. This means that users uninformed about available privacy settings other than the Public setting automatically subject themselves to full transparency and potentially full surveillance, since there is no way of knowing who is viewing their data and with what intentions. Combined with paragraph one of section four ("You will not provide any false information on Facebook"), the data obtained *via* surveillance of Facebook users is readily-available to a broad audience and in principle factually valid. Connected with this is paragraph seven of the same section: "You will keep your contact information accurate and up-to-date", which begs to consider why. An answer, yet again, is nowhere to be found in the *Terms of Service*, but this theme returns in section six, paragraph two, which obliges the user to update their mobile phone number information within 48 hours after its change or deactivation.

The last issue with the *Terms of Service* is in the method used to inform Facebook users about policy revisions. Paragraph three of section thirteen states: "Your continued use of the Facebook Services, following notice of the changes to our terms, policies or guidelines, constitutes your acceptance of our amended terms, policies or guidelines". This method does not ensure the effective dissemination of information (and it does not specify how Facebook will inform users about its policy amendments), since it does not require the user to become familiarised with policy revisions and what they entail in practice. It is merely assumed that since the user has been notified in whatever way, their continued use of Facebook constitutes an agreement to all changes. This approach has backfired in the past, exposing Facebook to criticism for its inadequate communication of policy revisions and company plans, as well as for its outright ignorance of users' opinion (cf. Fiveash, 2012).

12.2.2 Data Policy

The *Data Policy* (Facebook, 2015b; last revised January 30, 2015) supplements the *Terms of Service* with an explanation of what data Facebook collects about its users. The document opens with a broad description of the types of information collected, but again it lacks specificity. Paragraph two ("Things you do and information you provide") states: "We collect the content and other information you provide . . . including when you sign up for an account, create or share, and message or communicate with others". It is not specified what sort of content and "other information" is meant. Disconcerting here is the inclusion of messaging under the surveillance umbrella: Facebook collects private messages exchanged between users. Given the vague meaning of the verb "collect" used throughout the text, it is impossible to assess how Facebook uses this data (e.g. are the contents of private messages being read or otherwise inspected, and is this done by a human or a machine). The paragraph then explains that the website also collects metadata, i.e. "data that provides information about other data" (Merriam-Webster, n.d.), such as the geographic location where a photo was taken, and the date a certain file was created. This list is certainly not exhaustive, since Facebook avoids completeness in its phrasing (e.g. by using open terms such as "This can include" in paragraph two). What is clearer is the ubiquity of surveillance: it is concerned not only with "what" (the content itself), but also "when" (file date-stamps), "where" (geotagging), and "how" (user interactions with Facebook). It is justified to say that nothing goes unnoticed. One's likes, political affiliations, beliefs, social connections, etc., are subject to constant oversight. Since data is collected at all times, the gaze is always present. Furthermore, what brings Facebook even closer to the model of the

Panopticon is the interest in behavioural patterns and means of controlling them.

Here, what is also being collected is the information about how users interact with Facebook, e.g. the types of content viewed or engaged with, or the frequency and duration of Facebook activities (Facebook, 2015b, para. 2). The company is interested in the behaviour of its users, which points to Foucault's (1995) disciplinary power and panopticism, with their emphasis on behaviour and means of controlling it. The more Facebook understands about the ways in which users interact with its services, the more potential it has to change and influence user behaviour. The aim is to maximise the amount of time spent on Facebook, since this increases user exposure to Facebook's advertising system. The purpose of surveillance is thus to discipline into a psychological state of social media dependency. For this to succeed, the user cannot realise just how much of their life they invest in the website. This is why such individual statistics, although evidently collected, are never disclosed.

Surveillance also targets non-users. Paragraph three of the *Data Policy* ("Things others do and information they provide") explains that Facebook collects data provided by other people using its services, including "information about you, such as when they share a photo of you, send a message to you, or upload, sync or import your contact information". Thus, one could be in Facebook databases without knowing and without consenting. Surveillance is no longer tied to the website itself, but permeates the offline reality. Facebook tracks the movements of users and non-users alike; specific geographic locations of devices used to access its services, data about one's phone operator or Internet service provider, and also about the movement of users across the Internet *via* the use of Facebook's social plugins (e.g. the ubiquitous "Like" button). Surveillance is a network where information is gathered not only through facebook.com, but

also *via* third parties and companies owned by Facebook (Facebook, 2015b, para. 7–10), e.g. the photo-sharing platform Instagram and the instant messaging service WhatsApp.

What is the purpose of this network of data-collection? How is this information used by Facebook? The answer is found in paragraph seventeen of the *Data Policy*:

> We use the information we have to improve our advertising and measurement systems so we can show you relevant ads on and off our Services and measure the effectiveness and reach of ads and services.

The aim is thus to rationalise with scientific precision the behaviours of Facebook users; to turn the user-body into a body of knowledge: studied, examined, tracked, surveilled, predictable, knowable. This process of "datafication" transforms the chaos of social action "into online quantified data, thus allowing for real-time tracking and predictive analysis" (van Dijck, 2014, p. 198). The obsessive fixation on measurement and effectiveness demands an endless stream of data. The user becomes objectified into a source of information about themselves and others; information which is extracted with the use of panoptic gaze and examination (Foucault, 1995). Because for advertising to be seductive and efficient, Facebook needs to establish the truth about the user. Examination, defined by Foucault (1995) in terms of a "normalizing gaze, a surveillance that makes it possible to qualify, to classify and to punish" (p. 184), together with surveillance (or "hierarchical observation" if one is to stick strictly with Foucault's terminology), make users into describable, analysable, knowable "cases": "object[s] for a branch of knowledge and . . . hold[s] for a branch of power" (p. 191).

Facebook's power is thus in the creation of a discipline; a body of knowledge about individuals. Just as hospitals employ registers on a micro-scale to identify and classify patients, Facebook is one immense register and database wherein observing users and their behaviours becomes an industry and is capitalised for financial gain: "[W]e use all of the information we have about you to show you relevant ads" (Facebook, 2015b, para. 30). At the surface, using Facebook demands no monetary payment from the user. It instead uses personal data as the "new currency" (cf. Taylor, 2014): users are expected to reveal their lives and give up privacy, since only then do they generate profit. Surveillance – or "*dataveillance*" (van Dijck, 2014) – is the business strategy of choice in the new "data economy" of Web 2.0 (Eggers et al., 2013, p. 20). The Facebook experience is commercialised, privacy commodified, and the user willy-nilly made into a consumer. Users are "simultaneously *promoters of commodities* and the *commodities they promote*. They are, at the same time, the merchandise and their marketing agents" (Bauman in Bauman and Lyon, 2013, p. 32, original emphasis). This is where Facebook's power is most explicit: in the ability to control user subjectivities, to persuade them to behave in a certain way, to make them share details of their lives that would not have been shared otherwise. This power is asymmetrical in its effects: the user is disprivileged and disciplined to obey the rules of the game (e.g. in that they will not upload certain content or use Facebook for commercial purposes), whereas the company enjoys almost unrestrained freedom to dictate those rules, while giving a negligible chance of appeal (cf. Facebook, 2015b, para. 40). Both the *Terms of Service* and the *Data Policy*, therefore, create a situation where the user is comparatively disempowered *vis-à-vis* the company.

Lastly, on the language employed in the *Terms of Service* and the *Data Policy*; it is informal, especially in the latter document. It aims to shorten the distance between Facebook and the user, e.g. by the frequent use of direct

"you". However, this easy-to-process linguistic simplicity does not go hand in hand with the complexity of technical solutions behind the website, which are hidden beneath discourse and remain invisible to the user. These policies do not explain how things really are. Instead, with the help of vague buzzwords such as "safety" and "security", they aim at reassurance. There is not much meaning or substance behind this user-friendly façade.

12.3 Surveillance: Facebook as Panopticon

What conclusions can be derived from the two analysed policies in terms of surveillance? Can Facebook be considered a modern-form Panopticon? This chapter presents arguments that can be put forward in support of such claims.

The Panopticon was designed by the English founder of utilitarianism Jeremy Bentham in 1791 (Lyon, 1994, p. 63). This new type of penitentiary – an "all-seeing place" – was to have a semi-circular layout with cells grouped around a central "inspection lodge" from where the guards could see every prisoner. The prisoners themselves, however, could never see the guards who remained outside their gaze, hidden behind a clever system of louvres (O'Farrell, 2005). The defining features of Bentham's Panopticon were hence the permanency, inevitability and uncertainty of surveillance. By permanency is meant that the Panopticon subjected the prisoner to a ceaseless gaze; there were no periods in time when the inmate was not being potentially watched. Surveillance was inevitable, since there was no escape from the gaze. The cell was an enclosed space which was at all times exposed. In this setting, privacy is a utopia, since no action can be performed in secrecy.

Furthermore, what is perhaps the crucial characteristic of the Panopticon is the uncertainty whether one is being watched at any given moment. Since the prisoner had no way of seeing the guard, they could

never know for certain if the gaze was being directed at them. Nevertheless, the potential of being watched was in itself sufficient to change the prisoners' behaviours. The Panopticon is therefore a place where individuals are governed by the "art of distributions" (Foucault, 1995, p. 141) which comprises four processes: (1) enclosure (the prison as a distinct enclosed place, separated from the outside world); (2) partitioning (each person having their own delegated space within this enclosed place); (3) elimination of confusion *via* the use of functional sites (space rationalised, everything serving its purpose, elimination of waste); and (4) ranking (classification of people's performance, their division into homogenised groups such as classes or units) (pp. 141–146).

Thus, for Facebook to be a Panopticon, its design would have to reflect these principles. Is this the case? Firstly, the website is an enclosed place in the Internet *ex definitione*. Facebook is a domain separated from all other sites in the World Wide Web. Access to Facebook is restricted and subscription-based, since an account is needed to view and share content. Signing up for an account constitutes the first layer of surveillance: a real first name and surname, email address or mobile phone number, and date of birth are required. This information, as outlined in the *Terms of Service* to which the user agrees upon registration, must be truthful (whether the user has really read the *Terms of Service* and the *Data Policy* is never verified upon registration). Facebook is, like the Panopticon, "a place heterogeneous to all others and enclosed in upon itself" (Foucault, 1995, p. 141). Secondly, every user interacts with Facebook *via* their own account and personalised Timeline and News Feed. User experience is highly individualised, since the content displayed under each account will vary depending on the user's personal likes, affiliations, friend network, activity level, etc. But what is obvious is that indeed "[e]ach individual has his own place" there (p. 143).

If Facebook is a Panopticon, then each account is a cell designed to contain all the information about the user.

Thirdly, the space of Facebook is rationalised; divided into "functional sites" for the purpose of quick and easy navigation and control. Having logged in, the user is presented with a list of Favourites. Atop is the link to their News Feed, which allows the user to decide how to sort posts ("stories"): chronologically or by highest popularity (popularity is measured, e.g., by the number of "likes" and comments a post has received). This is followed by three other constants: Messages, Events, and Photos. The remainder of the Favourites list consists of Groups (small-scale discussion forums, public or restricted) the user has joined. Facebook is hence a structured, well-ordered and coherently organised place. Each element of the News Feed and the user interface serves a purpose and is everything but incidental. The complex, proprietary logic by which the News Feed is populated with content ensures each element catches the user's eye. There is no room for redundancy if users are to spend increasingly more time on Facebook each year.

Fourthly, one can also see the last feature of the Panopticon mirrored in Facebook's design. Ranking works to divide users into groups differentiated by hobby, profession, residence, nationality, education, etc. This process is double-layered. On the one hand, users purposefully become members in communities they choose. On the other hand, Facebook itself ranks individuals into broad categories: "[we] provide non-personally identifying demographic information (such as 25 year old female, in Madrid, who likes software engineering) to . . . partners [i.e. advertisers] to help them *understand* their audience or customers" (Facebook, 2015b, para. 30, own emphasis). Thus, ranking aims to make users intelligible, their behaviours predictable. Additionally, Facebook friendships often become a benchmark for personal popularity. The quantification of social relations into

calculable figures rewards those who favour quantity over quality of connections.

Moreover, the "Year in Review" feature, available from late 2014, which produced a collage of the most popular status updates, events and photographs posted on a person's Timeline during the passing year, can also be seen as the process of ranking at work. One's "Year in Review" could be shared with others. The longer, more cheerful, colourful and significant the collage, the better one's 2014 must have been in comparison with others. "It's been a great year!" read the automatically inserted headline, as if forcing enjoyment. Whose year was the greatest, whose collage the most startling, whose life the most enviable? Submitting oneself to the gaze is undoubtedly enticing – surveillance produces a seductive state of complete visibility:

> The condition of being watched and seen has thereby been reclassified from a menace into a temptation. The promise of enhanced visibility, the prospect of 'being in the open' for everybody to see and everybody to notice, chimes well with the most avidly sought proof of social recognition, and therefore of valued – 'meaningful' – existence. (Bauman in Bauman and Lyon, 2013, p. 26)

Naturally, Facebook is not a prison where users are physically held locked in cells. The cell is rather purely figurative and psychological: deleting the traces of one's online presence is possible but no longer permissible: "[L]iving social life electronically is no longer a choice but a 'take it or leave it' necessity" (Bauman in Bauman and Lyon, 2013, p. 30). The price for non-compliance with the "show-and-tell culture" of today is social death (pp. 30–31). But the willingness with which Facebook users disclose the details of their lives, regardless if they are being physically disciplined into doing so, is consistent with the Panopticon's logic. For panopticism, Foucault (1995)

argues, with time replaces the need for external disciplining with internal self-discipline: "[T]he inmates should be caught up in a power situation of which they themselves are the bearers" (p. 201). Although the possibility of deleting's one account exists, exercising it seems almost unthinkable.

It appears that the prerequisite to living a life is to live it publicly. Bauman (Bauman and Lyon, 2013) observes that this confessional tendency is perhaps not new: "The eagerness to disclose the details of one's life is not a generational characteristic of today's youth, but a proof of an underlying commonality of all people and all ages – of an inherently confessional society" (p. 31). Confession is in itself an act which breeds on surveillance: without the possibility of one's secrets being discovered uncontrollably, there would be no need to share them in a controlled manner. Confession gives the illusion of having power over one's self-narrative. This is what makes social networking sites so universally appealing. Facebook capitalises on the confessional society by providing a platform where secrets can be revealed, and are indeed expected to be revealed. This can also explain the online "privacy paradox" – the fact "that while Internet users are concerned about privacy, their behaviors do not mirror those concerns" (Taddicken, 2014, p. 248). Taddicken (2014) discovered that people's privacy concerns have little impact on their online self-disclosure. Indeed, Facebook normalised surveillance. Submitting oneself to its gaze is an oft-rewarding experience which affords a sense of being heard and understood; of significance and belonging.

Is Facebook a system of panoptic surveillance? The permanency and totality of surveillance on Facebook suggests that it indeed is. The *Data Policy* showed how the gaze works continuously to gather all the available data about the user: their status updates, comments, private messages, "likes", political affiliations, hobbies, personal connections, photographs, videos, geographic locations, events attended, places visited, and many

more. This totality of collected data allows to create a comprehensive behavioural profile of an individual, and to track its changes over time.

Who is then the surveillant in this setting? Bruno (2012) makes two arguments: (1) personal data is subject to corporate and police inspection, but also to a "lateral surveillance" by family members and friends (p. 344); (2) the user is not only a subject of surveillance, but can also surveil others in a system of "collaborative surveillance" (p. 344). Thus, the users are at the same time subjects to and sources of surveillance. They are being surveilled, but can themselves watch others. This is a major difference between Facebook and the original Panopticon. The modern gaze works in more than one direction, which invites to consider the alternative perspective of sousveillance: Can users reverse the direction of surveillance and point it at Facebook, so as to make the once-inspector seen?

12.4 Sousveillance and the Catopticon

Whereas the previous chapter argued for a view of Facebook as a modern informational Panopticon, this one explores the alternative perspective of sousveillance and the Catopticon it is argued to create.

The notion of sousveillance, introduced by Mann (Mann et al., 2003) and further developed by Ganascia (2010) who applies it to the modern "Infosphere" of the Internet, is a reversed or inverted form of surveillance. If surveillance signified watching from above (the French prefix *sur* translates to "over"), sousveillance is an act of watching from below (*sous*) (p. 493). It is a situation where "anybody may take photos or videos of any person or event, and then diffuse the information freely all over the world" (Ganascia, 2010, p. 489). Sousveillance is a recent theoretical development in

contemporary technological societies; one which is argued to describe their reality better than the traditional conceptualisation of surveillance.

The sousveillance perspective hence challenges Lyon and Bauman's view of modern surveillance society. Postmodernity, it argues, has replaced the surveillance-governed state with a new, more fluid and flexible form of social organisation; with a new "sousveillance state" (Ganascia, 2010, p. 491), and a "sousveillance society" which is "equally distributed, strictly egalitarian and delocalized over the entire planet" (p. 496). This is not to say that surveillance has dissolved completely. Rather, surveillance and sousveillance coexist, although the latter now dominates. Sousveillance has led to the blurring of boundaries between public and private, and to the emergence of the Catopticon:

> [W]hile the architecture of the Panopticon was designed to facilitate surveillance by prohibiting communication and by installing surveyors in a watchtower, the architecture of the 'Catopticon' allows everybody to communicate with everybody and removes surveyors from the watchtower. (p. 489)

Unlike the original Panopticon, the Catopticon makes everyone seen while allowing everyone to see. There is no longer need for the watchtower, regardless if occupied or abandoned. Sousveillance generalises supervision equally onto everyone. The prisoner becomes the guard; not only to himself, but also to his once-inmates.

Ganascia (2010) gives an example of sousveillance at work. In 1996, twenty-year-old Jennifer Ringley began recording her life with a webcam and streaming the image online (an activity termed "lifecasting"). For seven years Ringley shared the images of her private life with an unknown audience, what gave her an Internet celebrity status and three million daily

visits to her website (p. 492). Today, Facebook and its ilk allow anyone to become Jennifer Ringley. This sort of online exhibitionism has become a customary habit for Generation Y. But can it be said that Facebook is a system of catoptic sousveillance? Several points for consideration arise.

Firstly, let us briefly return to Facebook's News Feed. The previous chapter described the left-hand side portion of the website. In the right corner of the user interface lurks an even more intriguing feature – the friends' activity feed widget known as the "Ticker". The Ticker shows the activity of our Facebook friends in real time: their new posts, comments, "likes", social connections, attended events, etc. (Facebook, 2014). Thus, the Ticker affords surveillance of the online actions of others as they unfold. It shows

> who had friended whom, who changed profile pictures, who had written on other people's Walls and what they wrote, and who had posted new photographs, joined or left a new group, started dating, broken up, written a public note, or altered their lists of favorite books or movies. (Westlake, 2008, pp. 21–22)

It is a powerful tool, perhaps more revealing of a person's life than Jennifer Ringley's visual "lifecasting" project could have ever aspired to be. The News Feed itself gives an insight into the lives of others, but whereas content posted to the News Feed is nearly always decided on by the user, the Ticker tracks user's actions without any prior consent. Altogether, the elements of the News Feed work to create a system of mutual observation – of sousveillance. Catoptic sousveillance is based on three principles: (1) totality of transparency; (2) its equality; and (3) unrestricted communication (Ganascia, 2010, p. 497). All of those are reflected in the logic of the News Feed: transparency is a universal principle applied to every user equally by

default (there is no escape from one's actions being mentioned in their friends' Ticker); everybody is hence able to watch everybody else. Communication flows between Facebook users are also unrestricted, meaning that they remain outside the control of any particular state authority.

Moreover, the last feature, dubbed by Ganascia (2010) as "total communication" (p. 497), played an important role during the Arab Spring of 2010–2011. Social networking sites like Facebook and Twitter allowed protesters to bypass the state-controlled media channels in an effort to create their own, independent and autonomous narratives. Sousveillance thus ensures a system of checks and balances between the people and the governments. It helps "to denounce abuse or to check the conformity of public goods" (p. 493). Facebook can be a tool for an independent dissemination of truths about events, companies, states and individuals, which challenges the traditional power structures of the localised nation-state. Moreover, Facebook's global outreach allows these truths to circumvent national propagandas and to cross-check with information across multiple sources. The outside world knew what was happening inside Egypt, Tunisia or Libya from Facebook and Twitter users on the spot who posted about events as they were unfolding. This sort of honest, first-hand insight was made possible by these social networking platforms, since Facebook allows its users to broadcast information on a larger scale. Ganascia (2010) observes:

> In the past, only powerful institutions like states or rich companies had the ability to broadcast information on any scale. Since those new techniques enable everybody to be a potential source of information, they appear to promote individual autonomy. Anyone who has something to say to the world can do so freely on the Web. (p. 495)

This shows that the Catopticon can have positive effects as a safeguard against tyranny. When everyone is equally empowered to see what everyone else is doing, it is less likely that crime and abuse will go unnoticed. Facebook has performed this function during the Arab Spring, and will likely continue to be a platform for politically-subversive advocacy.

It seems that the use for Facebook, and what one makes of it, is an individualised enterprise. Social networking can become a Panopticon but it can also serve to empower the user, to provide them with tools to subvert existing power structures within modern societies. Facebook as Catopticon enables a truly independent and unrestricted expression of opinion. Such freedom is certainly liberating, but at the same time also overwhelming. With the increasing abundance of information shared online, making sense of the world demands more initiative and responsibility on the side of the user than ever before. The power of Facebook, whether it lies in the hands of the company or its users, can be at once destructive and productive.

12.5 Conclusion

Returning to my central question whether Facebook constitutes a system of panoptic surveillance or catoptic sousveillance, I argued in favour of both perspectives. Firstly, I discussed the perspective of surveillance, pointing to similarities between the logic and architecture of Facebook, and the structure of Bentham's Panopticon, supplemented with Foucault's concept of panopticism. My content analysis of Facebook's *Terms of Service* and *Data Policy* pointed to the immense scope of online surveillance: all sorts of data shared by the user are being subject to the company's close scrutiny, serving to create a holistic behavioural profile for the purpose of targeted, personalised advertising. Facebook hence becomes a site for the working of a specific power-knowledge, concerned with making the user-body

discernible, analysable, calculable, and predictable. This was reflected in Foucault's "art of distributions" which comprised of enclosure, partitioning, elimination of confusion, and ranking. I argued that these four principles are mirrored in the functioning of Facebook.

Secondly, the perspective of sousveillance was then considered, defined by Mann (2003) and Ganascia (2010) as an inversed form of surveillance where it is the user who becomes the observer. Indeed, this pattern of the gaze's working can also be observed in the case of Facebook. Not only does the website render its users visible to itself, but it also equips users with tools to surveil others in a lateral direction. The Ticker was one discussed example thereof. Sousveillance thus turns complete personal transparency into the norm. It also empowers users with new means of self-narration, and provides a platform for autonomous narratives of the world. This makes Facebook particularly helpful as a tool for politically subversive, anti-systemic advocacy, e.g. during the Arab Spring of 2010–2011.

But if Facebook is a site where surveillance and sousveillance blend, what does this tell us about the nature of those two phenomena? What is the relationship between surveillance and sousveillance, and are they necessarily mutually exclusive? Surveillance argued for a downward gaze, pointed by Facebook from above at the user placed below. In this scenario, the gaze subjects users to a ceaseless observation and disallows them to see its source. Sousveillance, contrastingly, reversed the gaze's direction upwards and sideways. The user is now the one who subjects their surroundings to oversight.

Yet, is this not ultimately a situation of surveillance, inverted or not? If surveillance is understood as watching someone without their knowledge or consent, then it can be said that Facebook surveils its users but the users similarly surveil Facebook. The only difference between surveillance and

sousveillance is the direction at which the gaze is pointed. What is common to both is their infringement of the individual freedom to not be seen or gazed upon. Surveillance and sousveillance should hence be seen as two sides of the same coin. It makes less sense to speak of subjective empowerment or disempowerment here, since power becomes an overarching fluidity. Power, perceived as the ability to create knowledge – a Foucauldian "power-knowledge" – is not exercised by Facebook or the users alone. There is not a single subject of power here but multiple entities bound by mutual dependencies: Facebook needs users for its economic survival, and users need Facebook as the platform for social connectedness and online self-narration:

> Social media depend for their existence on monitoring users and selling the data to others. The possibilities for social media resistance are attractive and in some ways fruitful, but they are also limited, both due to the lack of resources for binding relationships in a liquefying world and to the fact that surveillance power *within* social media is endemic and consequential. (Lyon in Bauman and Lyon, 2013, p. 12, original emphasis)

Doubtless, sousveillance gives leeway for social media resistance, but these possibilities are not unlimited. Furthermore, it would seem that in the modern globalising world of increased pace and interconnectedness, services such as Facebook become essential for sustaining social relationships over geographic distance. The ultimate responsibility for how Facebook is employed, and what purposes it serves, is with the users themselves:

> [I]t is the uses that we – Facebook's 'active users', all half-billion of us – make of those offers that render them, and their impact on our lives, good or bad, beneficial or harmful. It all depends on what we are after; technical gadgets just make our longings more or less realistic and our search faster

or slower, more or less effective. (Bauman in Bauman and Lyon, 2013, pp. 27–28)

This is why awareness and consciousness are crucial in the online realm. I hope to have equipped readers – users of social media – with basic insights needed to make informed choices about our online presences, and the risks involved therein.