Information Polity 27 (2022) 275–289
DOI 10.3233/IP-211536
IOS Press

Power in the modern ‘surveillance society’: From theory to methodology[1]

Catharina Rudschies
Department of Informatics, Universität Hamburg, Vogt-Kölln-Strasse 30, 22527 Hamburg, Germany
Tel.: +49 40 42883 2034; E-mail: catharina.rudschies@uni-hamburg.de

Abstract. The rapid expansion of new Information and Communication Technologies has improved the possibilities for surveillance, rendering modern society a ‘surveillance society’ (Lyon, 2006). Surveillance practices today comprise a myriad of actors. However, relations between different groups of “observers” and “observed” and their respective impact on the form of surveillance are not yet sufficiently considered. Furthermore, methodologies are missing “to look beyond abstract theory” (Galič et al., 2017, p. 34). This paper proposes theoretical considerations as well as a methodological framework by taking a meso-level perspective and by incorporating the examination of power relations in surveillance systems. It is argued that contemporary surveillance structures encompass hierarchies, albeit not in a traditional unidirectional manner. Furthermore, a first attempt is made to provide a methodological framework that helps to analyse the power relationships between diverse actors that emerge due to differences in capabilities to observe and hide. Based on a number of specified indicators, the framework aims to assist in understanding how power is distributed and in how far actors and their position within the hierarchy determine the form of surveillance and the impact it can take.

Keywords: Surveillance, surveillance theory, methodology, power, power relations

Key points for practitioners:

- In modern surveillance practices power relations are determining the scope surveillance can take.
- Power relations between diverse actors need to be examined.
- This paper proposes theoretical reflections and a methodological framework that help to understand
  1. how power is distributed and
  2. in how far the position of actors within a hierarchy determine the extent of surveillance and the impact it can have.

1. Introduction

Over the last decades, the rapid expansion of new Information and Communication Technologies (ICTs) has increased the interconnectedness worldwide. Although this process bears many benefits for our lives, as the new technologies facilitate the way we work, consume, and communicate for instance, it also improves the possibilities for surveillance. David Lyon defined surveillance as the “focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction” (2007, p. 14). Clarke described it as “the systematic investigation or monitoring of the actions or communications of one or more persons” (1988, p. 499). Accordingly, its main goal is to collect information about people, their activities, or their associates (ibid).

[1] This article received a correction notice (Erratum) post publication with DOI 10.3233/IP-229012, available at http://doi.org/10.3233/IP-229012.

Modern surveillance practices comprise a myriad of actors – private, corporate, and governmental. Therefore, surveillance can take multiple forms: *inter alia* corporations collecting consumers' data in order to enhance marketing strategies and product developments; citizens engaging in the observation of the powerful; self-surveillance via fitness trackers; surveillance of children in parenting activities; CCTV (Closed Circuit Television) and facial recognition systems to surveil, prevent, and punish crimes. Additional surveillance activities are constantly emerging due to the development and expansion of new technologies. Consequently, surveillance has become a norm in our daily life, rendering modern society a 'surveillance society' (Lyon, 2006, p. 7).

Many scholars have tried to theorise surveillance in order to understand where it originates, how it works, and what effects it has. Among them are notably Foucault's concept of the 'Panopticon' (1979), Mathiesen's theory of the 'Synopticon' (1997), Lyon's concept of 'social sorting' (2003), Deleuze's notion of a 'rhizomic' surveillance structure (1987), and Zuboff's account of 'surveillance capitalism' (2015; 2019). While these theories certainly have their merits, many focus on the macro – therefore, the systemic – level. While a macro-level approach focuses on the surveillance society as a whole, it offers little to describe how surveillance differs when looking at varying actors involved in surveillance measures. Thus, what is missing in surveillance studies is a theoretical approach that focuses on the meso-level. Relations between different groups of "observers" and "observed" and their respective impact on the scope of surveillance are not yet sufficiently considered. Furthermore, methodologies are missing "to look beyond abstract theory" (Galič et al., 2017, p. 34).

This paper argues that, contrary to some network theorists, contemporary surveillance structures encompass hierarchies, albeit not in a traditional unidirectional manner. New forms of hierarchies have developed and are important determinants for surveillance structures. Therefore, this paper suggests that the surveillance system is structured in an undefined multidimensional sphere, in which actors are all potentially linked in a network with 'multidirectional hierarchies'. Moreover, surveillance entities decreasingly act in isolation, but often cooperate in an attempt to increase their surveillance potentialities or benefit from the sharing of resources.

In a second step, this study provides a methodological framework to analyse the power relationships between diverse actors that emerge due to differences in capabilities to observe and hide. Based on a number of specified indicators or hypotheses, the framework aims to assist in understanding how power is distributed and in how far actors and their position within the hierarchy determine the form of surveillance and the impact it can have. Unbalanced power relations are always problematic, since they bear threats such as domination, manipulation, or abuse. Therefore, it is of utter importance to identify the strong and weak powers within the surveillance system and to provide solutions for their regulation or protection.

2. Reviewing influential surveillance theories

One of the most influential notions in surveillance studies is the 'Panopticon' by Michel Foucault (1977). Originally developed by Jeremy Bentham, it described an architectural figure of a prison that was characterised with a circular arrangement of cells visible to a ward who was located in a tower in the middle of the ring.[2] While the ward was able to observe each inmate at any given time, he himself was invisible to the prisoners making it uncertain when observation actually took place. Foucault used the

[2] Besides the prison-Panopticon Bentham actually described a number of different Panopticons with varying characteristics in his writing, see e.g., Galič et al., 2017.

architecture to explain surveillance structures of any sort. He argued that a panoptic structure with its hierarchical observation produced a consciousness of permanent visibility in the prisoners, which exerted disciplinary power and resulted in their own self-discipline to behave according to a pre-established norm. (Foucault, 1979, p. 200; Gill, 1995, pp. 11–12) With his concept of power/knowledge he argued that institutions create knowledge in order to regulate and 'normalise' individuals. This knowledge, as Foucault explains, authorises or legitimises power, hence, is power (Danaher et al., 2000, p. 26).

The Panopticon soon became one of the most applied concepts in surveillance studies. Scholars have utilised it to describe the workings of various modern institutions and technologies such as consumer technology, advertising agencies, mass media, data retention, and closed-circuit television (Simon, 2005; Clarke, 1993; Rogers, 2008; Koskela, 2004, Hackley, 2002). Whereas many scholars have affirmed the mechanisms of the Panopticon, there has also been some criticism to its validity. Critics argued that the mechanisms of modern technologies would go beyond the Panopticon. While the Panopticon and its focus on a unilateral power vested in the observer describes a dystopia of totalising power over helpless and passive victims, surveillance operations today no longer have one single authority conducting surveillance over all others. Instead, various groups have acquired the ability to observe others. Thus, surveillance mechanisms of modern technologies would also entail that the many watch the few or the many watch the many. Researchers have, thus, introduced the notions of the 'Synopticon' (Mathiesen, 1997), 'Polyopticon' (Allen, 1994), 'Superpanopticon' (Poster, 1995), 'Omnicon' (Groombridge, 2002), and 'Neopanopticon' (Mann et al., 2003).

David Lyon (2007) contends that the concepts of the Panopticon have been overused (pp. 46–47). Whereas Foucault applied the concept merely to circumscribed spaces, the deterritorialisation that comes with technologies of global reach as well as the increased mobility of individuals raise questions in how far the observer is still able to control each single subject. Moreover, Lyon argues that modern surveillance is not confined to one single purpose but can be manifold and is subject to changes in the future (Lyon, 2006, p. 28; Haggerty & Ericson, 2006, p. 18). A more recent account by Shoshana Zuboff holds that surveillance is no longer bound to observing actual behaviour in a certain setting, but has shifted towards the manipulation of future behaviour with an all-encompassing scope, however, without the totalitarian means of violence (2015; 2019). This suggests that the Panopticon is rather out-dated, as it describes a surveillance structure with clear demarcations of space, purpose, and effect and works under mechanisms of repression.

Despite the aforementioned problematic elements of the Panopticon metaphor, there are also elements that hold true in modern surveillance structures. One of the elements is Foucault's notion of power/knowledge. In modern surveillance operations power/knowledge is created by the systemic collection and processing of data from diverse sources. This information is subject to a process of selection, analysis, categorisation, and classification. All of these processes have in common that they are subject to human decision-making, determining what data is gathered, how it is analysed, and how information outcomes are interpreted. Data processing is, hence, never neutral and cannot work without biases or sometimes even arbitrariness. With the rise of Big Data and Artificial Intelligence (AI), new insights are garnered from great datasets that may include statistical, societal, or historic biases (Friedman & Nissenbaum, 1996; boyd & Crawford, 2012). Profiles that are created for each individual might thus be marked by errors and misinterpretations. Furthermore, how people are classified and to what kind of decisions these classifications lead, is also subject of decision-making by those with access to the data. All of this suggests that knowledge is to some degree created or shaped by observers.

The increasing usage of personal data in the observation of individuals, their actions, and communication, has been termed 'dataveillance' by Roger A. Clarke (1988). David Lyon then described modern surveillance structures as a system for "social sorting". He holds that the categorisation and classification of data poses risks of a "digital divide", meaning that "information itself can be the means of creating divisions" (Lyon, 2003, p. 2). Due to systematic categorisation conducted through algorithms, individuals can wrongfully be classified, for example as "eligible" or "ineligible" for jobs and loans or as "criminals" or "suspects" even though they have not acted or are not about to act in any illegal way. Categorisation and, even more so prediction removes the legal presumption of innocence, making individuals suspects until they themselves have proven otherwise. In a world where every click, purchase, read, like, comment, and often even move is tracked via technologies, it becomes easier to divide people into endless categories, subgroups, and 'sub-subgroups'. These groups are not static but fluid depending on who is in charge of classification and categorisation and what aims they pursue.

Theories that have emerged in reaction to the 'Panoptic overload' have tried to distance themselves from fixed spaces and a traditional hierarchy by introducing the notion of networks. Modern surveillance structures are increasingly complex and encompass a multitude of actors, who are all interconnected. According to Gilles Deleuze and Félix Guattari, today's surveillance system is of a rhizomic structure characterised by two major attributes: "its phenomenal growth through expanding uses, and its levelling effect on hierarchies" (Haggerty & Ercison, 2000, p. 615). Within such a complex and wide-ranging system, total surveillance has become impossible to conduct. Haggerty and Ericson took up that notion and described surveillance structures as so-called 'assemblages' defined as a machine that ...

> *"... operates by abstracting human bodies from their territorial settings and separating them into a series of discrete flows. These flows are then reassembled into distinct 'data doubles' which can then be scrutinised and targeted for intervention." (Haggerty & Ericson, 2000, p. 606)*

The two scholars assume that assemblages can overlap and consist of many smaller assemblages. Therefore, they support the idea of a deterritorialised, complex and interconnected surveillance structure.

Zygmunt Bauman first introduced the concept of surveillance via seduction. Accordingly, people voluntarily give away their data in exchange for a product or service. Therefore, consumer seduction replaces repression, since "conduct is made manageable, predictable and hence non-threatening, by a multiplication of needs rather than by a tightening of norms" (Bauman, 1987, p. 168). What Baumann has described can be found in a more enhanced version in Shoshana Zuboff's account of 'surveillance capitalism' (2015, 2019). Zuboff lays out that surveillance capitalism is based on practices of data extraction, accumulation, and analysis aimed at behavioural modification. She holds that the relationship between corporations (like Google) and the population is one without reciprocity, because companies extract data and circumvent meaningful agreement of data subjects. While the network theorists claim surveillance has experienced a levelling effect in hierarchies, Zuboff argues that there is a strong information and power asymmetry between those being in charge of data extraction and analysis and those being subject to it. She claims that surveillance capitalism leads to a redistribution of privacy rights, where rights are accumulated in the hands of surveillance capitalists, while the population loses control over what is to remain secret (Zuboff, 2015, p. 83). Zuboff argues that under surveillance capitalism, "[i]t is no longer enough to automate information flows *about us*; the goal now is to *automate us*" (Zuboff, 2019, p. 19).

3. Discussion

The previous section shows that scholars have provided many theoretical conceptions of surveillance. While not all of them provide comprehensive theories, they all add some insights to surveillance studies. Most apparent in the evolution from a panoptic to post-panoptic surveillance structure is the change from territorial to deterritorialised forms of surveillance and a turn away from unidirectional, vertical hierarchies. Network theories show that modern surveillance encompasses a multitude of actors who are observer and observed at the same time. However, what is missing from these theoretical accounts is a more focused consideration of power relations and hierarchies in an age of modern digital technologies. Notably, some scholars have acknowledged that power relations still exist. For instance, Lyon noted that surveillance is always related to questions of power and its distribution (2007, p. 20). Haggerty claims that groups are differentially positioned to be able to exploit surveillance potentialities and social cleavages. He argues that hierarchies have changed but are still important in establishing and reinforcing social inequalities. (2006, p. 29) Yet, neither Lyon nor Haggerty have provided a more detailed account of power relations in surveillance practices. Zuboff then reintroduces power as a central notion of surveillance. Her theory, however, takes an overarching perspective, for it aims to explain a new economic-political system (Galič et al., 2017, p. 24), in which power domination of Big Tech plays a central role. Overall, the surveillance accounts presented here do not include a focused analysis of power relations.

Furthermore, existing theories often try to explain surveillance on a macro-level – that is: the societal or systemic level. However, a macro-level focus does not differentiate between the various actors that differ in their position, motives, capacities, and means. Since these are crucial factors influencing power relationships, a macro-level approach does not consider the fact that surveillance operations can take different scopes and effects depending on the actors in play. In order to be able to analyse the power relations and their implications in surveillance structures, it is therefore necessary to examine surveillance at a meso-level. Research at the meso-level studies the experiences of groups and the interactions between groups (Blackstone, 2012). There are several reasons, why such an approach is crucial in theorising surveillance.

First, the surveillance system has become wide and complex and is increasingly decentralised. In such a system, each meso-level actor shapes the organisational structure as well as the form different forms of surveillance can take. Moreover, as discussed above, meso-level analysis yields insights into the variation of motives, scopes, and mechanisms of surveillance. Third, a meso-level approach brings into focus the social dynamics or patterns of interaction. Fourth, insights from a meso-level analysis can disclose ethical and socio-political problems, for inequalities in the power distribution can lead to the violation of fundamental rights for certain groups. Therefore, focusing on a smaller unit of analysis is a crucial task in explaining modern surveillance.

4. Power in surveillance

This paper aims to provide some theoretical considerations and a methodological framework that focuses on the politics of surveillance. While politics can be defined in a variety of ways, in this paper it is understood as the science or practice of the distribution of power within a given community and the relationships within or between groups of people. Politics of surveillance, hence, concentrates on the power relationships between different actors involved in surveillance and tries to explain how far power is distributed in the surveillance system.

Power itself is a concept that is highly debated in the political science literature. Power has been theorised *inter alia* in terms of hegemony (Cox, 1993), pluralism (Dahl, 2005), elitism (Mill, 1958), and feminism (MacKinnon, 1983). Depending on the theory, power is defined as a means, a resource, or a position of will (Sadan, 2004). Max Weber, for instance, described power as "the probability that an actor within a social relationship would be in a position to carry out his will despite resistance to it" (ibid, p. 35). Others explain it as a "possibility of inducing forces" or "potential influence" (Raven, 1993,

p. 228). Power, hence, refers to a potentiality or ability to influence others in a way that serves one's own interest or will. In this paper, it is assumed that the nature and scope of surveillance is influenced by power relationships, hence, the ability of actors to have an influence on others. This paper bases its considerations on the idea that there are three main determinants for power in the surveillance context of the modern digital world: i) power is enhanced via resources, since digital technologies play a major part as enablers and mediators of modern surveillance activities; ii) power is enhanced via an actor's position in the societal structure, as certain formal (or informal) positions in society may legitimise surveillance and the exertion of control (or may help in resisting surveillance); and iii) power is enhanced by influencing or determining the debate by defining the problem and controlling its framing, thereby deciding what is important or unimportant.

5. Theorising surveillance: Multidirectional hierarchies in an undefined sphere

Theorists like Deleuze, Guattari, Haggerty and Ericson convincingly described the surveillance structure as a network. While I argue that Deleuze's and Guattari's image of a horizontally spreading rhizome does not fully capture the scope of modern surveillance, the principal notion of a network is valid. Nevertheless, I suggest that the surveillance structure should be viewed as an undefined multidimensional sphere, in which actors are interconnected (reasons will be explained below). "Undefined" in this context means that it is not a closed system but open to expansion. The connections between the diverse actors do not all represent factual links, but can also be mere potential links that have not been activated yet (but could be activated anytime).

Haggerty and Ericson explained that "assemblages" consist of a multiplicity of heterogeneous objects, comprising "discrete flows of an essentially limitless range of other phenomena such as people, signs, chemicals, knowledge and institutions" (Haggerty & Ericson, 2000, p. 607). In my theoretical understanding, such a conception compounds surveillance entities (i.e., the actors within surveillance practices) with knowledge and data. Such a picture of an assemblage is not wrong *per se*, since actors and information are obviously linked. However, it makes an understanding of the organisation of a surveillance system more difficult.

Therefore, I suggest a different conception of a surveillance system that differentiates between actors and information. More precisely, in the sphere of surveillance there are what I call "conglomerates" of surveillance entities. These entities hold information about themselves and others (therefore are connected to certain information and data, but these remain on a different level in the background of this analysis). Basically, these conglomerates represent a corporation of certain surveillance actors. They overlap with others and can be found in diverse compositions. Furthermore, they comprise several layers. For instance, in the first layer are all actors from the same group. These may be corporate actors, state actors or citizens/consumers. For instance, the group of state actors could comprise *inter alia* the police, intelligence agencies, the military, and international political bodies. Actors of the same actor group usually have similar motives and means for their specific surveillance practices and, therefore, tend to be highly connected with each other. They can cooperate with each other for example by exchanging data, tools, and expertise. The second layer of the conglomerate then also comprises actors of different groups in cooperation (such as state and corporate actors). Such cooperation usually happens when these actors have the same or similar aims for observation or when the different actors realise that they can gain benefits for their own group only by collaborating with others, even though the aims might be different.[3] It should be noted that the compositions of the conglomerates may change very fast.

Picturing the surveillance structure as an undefined multidimensional network with conglomerates operating at different levels differs from horizontal networks in two respects: First, the multidimensional character enables the simultaneous existence of a multitude of compositions of actors that bundle in the conglomerates, a capacity a horizontal network is limited in. Second, in a horizontally-spread network all nodes (actors) must be connected. However, I argue that actors are interconnected to varying degrees. Some connections are "tighter" than others, therefore, within the sphere one can detect different densities of the surveillance network. The more ties there are within a certain conglomerate and the stronger the ties are, the more dependent the actors are on each other. As discussed before, all actors involved in surveillance practices carry the role of the observer and the observed at the same time (Haggerty, 2006). Therefore, in a surveillance system there are always at least two ties connecting two actors, one for depicting the surveillance operations in direction of actor A and one depicting the surveillance operations in direction of actor B. Depending on the motives, capacities, and means, for instance, one tie can be stronger than the other and, thus, depict an enhanced power position in relation to the other.

In order to assess the power relations between different actors, in the next part of this paper, I make a first suggestion for an analytical and hence methodological framework by means of a list of questions serving as indicators that ought to be discussed and further developed by scholars within the field. These questions are divided into two groups: first, questions being posed out of the perspective of the observer, and second, questions being posed out of the perspective of the observed. Although there is not one single observer and one single observed in the overall surveillance structure, one can still make the distinction between 'watcher' and 'watched' when looking at relationships between two specific actors. As Lyon noted: "The fact that there are two parties, watcher and watched, is important but often overlooked." (2007, p. 3) To ask questions out of these two perspectives, therefore, gives valuable insights into the position, motives, purposes, capabilities, and tools that each actor has to conduct surveillance and exert influence over others (from the perspective of the observer) and, on the other hand, to hide, protect, or resist surveillance activities and influence (from the perspective of the observed). Obviously, one needs to do the assessment twice, putting actor A first in the position of the observer and then into the position of the observed. The net balance of the results will provide a picture of who is dominating in the relationship. Since the considerations made in this paper are currently only of theoretical nature and require the application in empirical cases, the indicators are formulated as hypotheses. Some of them may seem rather tautological, however their inclusion is necessary in order to provide a complete picture of the (potentially) differing power relations and thus enable a comprehensive meso-level analysis.

Moreover, it should be noted that the results of this analysis are only of qualitative character, since the answers to the questions cannot be easily quantified. However, this framework does not aim to provide the user with precise power levels in form of a number or rank, but shall only make clear that actors within the surveillance system are in different power positions and that hierarchies still exist. The main question that should stay in focus of the analysis is: How much power does the surveiller hold over the surveilled and how much power does the surveilled hold in order to avoid the surveillance? These questions must be answered for actor A being in the position of the observer as well as for being in the position of the

[3] Actors within the surveillance structure – whether from the same or different actor group – can in fact be in competition with each other (e.g., companies may compete in the market for consumer data (consumer surveillance) that they either use for their own business goals or use for gaining profit when selling this data to third parties). In these instances, rival actors may either use surveillance to gain a competitive advantage, which would infer that the potential connection or link between the actors is activated. Alternatively, when surveillance is not conducted between the competing parties, the link is simply inactive.

observed. The sub-questions that are to be answered out of each of the two perspectives will offer insights into this main question. I will outline the sub-questions and explain – sometimes by using illustrative examples – what the respective question implicates.

6. Proposing a methodological framework

6.1. Power assessment: Observer

How many and what kind of resources does the observer have?

This question determines what kind of financial and personnel resources as well as resources in terms of expertise the observer can use. Having financial resources enables the observer to invest in staff, expertise/education, and the development as well as the acquirement of tools. Expertise is a resource that needs to be renewed constantly. With newly emerging technologies and surveillance operations, the observer needs to make sure to invest in gaining advanced expertise. For instance, Google (Alphabet), a company with vast amounts of resources, is able to invest in the best-skilled people, the development, and acquirement of tools as well as political influence (via lobbyism). The usage of these resources has in the past increased Google's power position because it is able to achieve (and keep) market dominance and, thereby, its (capitalist) surveillance scope.

Indicator/Hypothesis: The more resources the actor has, the higher tends to be his power level.

To what extent does the formal position of the observing actor give legitimacy to surveillance and the exercise of control of the observed?

State actors are good examples to explain that some actors are in better positions to exert power because they are in a formal position of authority or of control of certain resources or information. Such formal positions can generate the ability to coerce or reward (Raven, 1993). National Intelligence Agencies for instance have the formal role and authority to safeguard the nation by using intelligence capacities. In these cases, other actors such as citizens or private entities like companies are in a weaker power position, because they do not have the same or a similar formal position. A citizen resisting the surveillance of such formal authorities may have little chances to make a claim against surveillance. Interesting empirical results may be gained when looking at the formal positions of state actors and private entities like companies. While state actors are in the formal position of authority and of control, it is often argued that some corporate actors such as Big Tech companies have acquired a factual position of power, because they control digital infrastructures and information by possessing massive amounts of data (Sætra et al., 2021; Fernandez et al., 2020; Hawley, 2021).

Indicator/Hypothesis: Actors being in a formal position of authority and control tend to have higher power levels.

What tools does the observer have to collect, analyse, and use data about the observed?

In addition to the resources described above, the observer receives considerable power by the usage of technologies, especially data processing tools. They enable the collection, analysis, and categorisation of information tailored for the observer's purposes even if data is collected in vast amounts. In an era of Big Data, information is in many instances collected for other purposes than surveillance, but provides immense potential for surveillance activities when fed into the right tools to process the data and put the insights gained from them to use. New technologies like AI open up new possibilities to analyse massive amounts of data hitherto impossible to process. Thereby, surveillance is decreasingly exercised with pre-determined targets. Rather, Big Data and AI enable surveillance of the masses to find the most promising and possibly even more targets for surveillance. (Eubanks, 2018) Using such technologies, hence, increases the power of the observer, since it makes data collection and analysis more efficient. As Lyon states: “Those who have the capacity to influence how people are classified and categorised tend to be in positions of greater power than those who do not.” (2007, p. 26) This is because they do not only decide who and what is to be observed, but also “what kind of data is being generated and in what form or format, how and where it is amassed and used, by whom, for what purpose, and for whose benefit” (Fischer & Streinz, 2021, p. 4) as well as how the insights from that data are interpreted. Fischer and Streinz call this the ‘power to datafy’ (ibid).

Indicator/Hypothesis: The better, more advanced, and far-reaching the tools used for surveillance practices, the higher tends to be the observer’s power level.

What motive does the observer have to conduct surveillance?

Surveillance can be used for purposes such as to influence, manage, protect, direct, manipulate, make profit, or control. The motives for surveillance are, thus, manifold. Nevertheless, depending on the motive, surveillance can take different forms and have more or less severe effects. The severity of effects is determined *inter alia* by the extent to which surveillance influences individuals in their life or life decisions. For example, when corporations use consumers’ data for product improvement, the effect might be rather minor or even benefit the observed. However, if corporations exploit vulnerabilities like emotional states or economic deprivation to sell products or services a consumer might not choose otherwise, the motive changes to manipulation. Even more severe effects may occur when watchers have motives of control. For instance, public administrations are increasingly using automated decision-making (ADM) tools to determine who receives social benefits. Such motives have considerably more influence on an individual’s life, since people might be excluded from receiving services their well-being may be dependent on (see, e.g., de la Garca, 2020). An interesting empirical case is the Danish government’s ADM system *Udbetaling Danmark* that was set up to centralise the payment of welfare benefits and that has access to personal data of millions of citizens. The system was found to conduct “systematic surveillance” and to pay 325.000 households lower housing benefits than they were entitled to. After these revelations, the public discussed the “UDK’s power” intensively (Chiusi et al., 2020, pp. 49–50).

Indicator/Hypothesis: Depending on the motive, the effects of surveillance can be more or less severe.[4] The more severe the effects of surveillance are, the higher tends to be the power level of the observer.

For what (additional) purposes can the observer use the data? In how far can data be abused, meaning used for other purposes than those officially declared to?

Even though surveillance operations are usually declared to have one specific purpose, modern surveillance is marked by a process of repurposing often conducted behind the scenes. Innes (2001) called this process ‘function creep’, whereby “devices and laws justified for one purpose find new applications not originally part of their mandate” (Haggerty & Ericson, 2006, p.18). For example, whereas black boxes in cars initially functioned to deploy airbags during a crash, they are now also used for criminal investigation collecting data *inter alia* on speed or whether the seatbelt was fastened. (ibid) Such processes are worrisome, as they often happen via unpublicised bureaucratic reforms, therefore, lacking transparency and accountability. Therefore, people would need to regularly check laws, terms and conditions as well

[4] It should be noted that an assessment of the severity of risk or harm may be challenging in certain instances, since many harms such as rights violations cannot easily be quantified and are subject of interpretation.

as privacy settings of the services they use in order to stay informed about the changes undertaken – a task almost impossible to fulfil as an ordinary citizen/consumer. In recent years repurposing has become current practice also across companies and other actors. Data collected by one party is sold or shared with third parties who might use the data for completely different purposes, a process often unknown to the data subject. These additional or changed purposes might go beyond the agreement that the individual has consciously made with the surveilling entity. This increases the risk that surveillance practices are abused for purposes unwanted to the observed and, hence, gives the observer a significant amount of power. (See an empirical case study of data brokers and the imbalance of power vis-à-vis consumers in Crain, 2018.)

Indicator/Hypothesis: The less transparent it is for what purposes surveillance activities are used and the more purposes are changed and added, the higher tends to be the observer's power level.

In how far is the surveiller capable of connecting with other observers and receive more data? In how far is he able to centralise surveillance operations?

Centralisation is a process to combine forces and is, thus, power enhancing. Whereas centralisation often means that power lies in one single authority, centralisation can also signify that several actors engage in cooperation and are, thus, able to achieve higher or other aims. Since the surveillance structure is no longer monopolistic, centralisation in surveillance operations is limited to the latter form. Consequently, if surveillance actors cooperate for example by exchanging data, expertise, and tools, they expand their surveillance power. They have higher sums of financial resources and they multiply the purposes of surveillance by giving collected data to other actors who might use them for different aims. Collection and selection processes, therefore, only need to be conducted by one instead of many actors simultaneously. Cooperation by corporate actors can also lead to higher market shares or when citizens join forces with civil society organisations, collaboration may increase power through heightened public visibility and pressure.

Indicator/Hypothesis: The more centralised surveillance operations are and the more actors cooperate with each other, the higher tends to be the observer's power level.

6.2. Power assessment: Observed

In how far does the watched cooperate in his surveillance? What role do seduction and voluntary action play in the surveillance conducted?

Surveillance works best with the cooperation of those who are subject to it (Lyon, 2007, p. 27). Therefore, in order to conduct surveillance as effectively as possible, observers have acquired new means for surveillance. In the commercial realm, surveillance works with a process of 'seduction' (Bauman, 1987) and behavioural manipulation (Zuboff, 2015). People voluntarily give away their data because they receive a product, service, or other benefit for it. Therefore, they are 'seduced' to cooperate in the surveillance practice. According to Lyon, it depends on the level of knowledgeability and willing participation how well surveillance works. He describes knowledgeability as the ability to be aware about the surveillance and to react to it in ways that could at least mitigate whatever negative effects are believed to be present (2007, p. 27). If the level of knowledgeability is low and the level of willing participation rather high, people voluntarily cooperate in the surveillance activities and, consequently, give more power to the observer.

Indicator: The more the observed voluntarily or unconsciously cooperates with the observer, the higher tends to be the observer's power level.

In how far does the formal or informal position of the observed actor help in hiding from or resisting surveillance?

Contrary to the ability to exert influence via a formal position of authority and control, it is also possible that formal or informal positions may help in hiding from or resisting surveillance. Due to their formal position, journalists for instance are protected from certain forms of surveillance in order to safeguard a free press and protect them from state intervention and control. Thus, journalists as well as their informants are formally in a position to enjoy some form of secrecy and privacy. The revelations about the Pegasus spyware in 2021 led to a massive outcry that journalists and their informants may not be safe from surveillance by state actors leading to the call to protect the free press (Di Salvo, 2021; One Free Press Coalition, 2021). On the other hand, it may be exactly informal positions that may generate an advantage to hide and resist surveillance. For instance, individuals without a formal position of authority may be better able to hide behind digital profiles or pseudonyms and use digital technologies to hide in the masses and avoid directed surveillance.

Indicator/Hypothesis: Actors being in certain formal or informal positions may have higher abilities (power) to hide from or resist surveillance operations.

What means does the surveilled have to avoid, refuse, or fight surveillance?

Instead of cooperating with the watcher, the watched could theoretically avoid or refuse surveillance. In order to do so the observed requires the possibility of opting out of surveillance operations. Theoretically, surveillance exercised by companies could be avoided. However, in modern times such an opt-out seems nearly impossible, as many products and services are needed in everyday life situations such as work, social life, and bureaucracy and are, thus, paramount for social and public participation.

Instead of avoiding or refusing surveillance there is also the option of resisting or fighting surveillance. There are several kinds of resistance: political resistance in form of demonstrations, petitions and pro-privacy advocacy groups; everyday resistance as a form of circumventing surveillance (Gilliom & Monahan, 2012); and technological protection in form of *inter alia* firewalls, software that detects viruses and spyware on the devices, protection from hackers, the usage of external servers, the changing of one's own IP-address, and the utilisation of fake accounts. Producing 'data noise' to conceal one's true identity, preferences, and behaviour online is also a form of surveillance resistance. Furthermore, protective measures require knowledge, skills, and resources. Hence, depending on the endowment with these resources some actors are better able to resist or protect themselves from surveillance than others. An example of political resistance is the "*Reclaim your Face*" campaign against facial recognition and other biometric identification technologies led by a number of civil society organisations across Europe,[5] whose demands have been taken up by the European Parliament (European Parliament, 2021).

Indicator/Hypothesis: The more means an actor has to resist or protect themselves from surveillance practices, the higher tends to be his power level.

In how far is the observed able to centralise resistance forces against the surveiller?

This question aims at the countermovement to centralisation of surveillance operations. Just as centralisation of surveillance measures can increase the power of the observer(s), centralisation in resistance forces can augment the power of the observed. However, centralisation is dependent on the mobilisation of people. Whereas there are some pro-privacy groups, internet platforms, and alternative service providers offering surveillance-resistant products/services, they usually lack effects of mobilisation. Due

[5] Information on the campaign available at: https://reclaimyourface.eu/.

to the network effect, companies like Whatsapp (under the head of Facebook) have been successful in binding users to their service, for there is no use in utilising an alternative more privacy-friendly service provider if friends and family do not switch, too. In social and political movements, the problem of mobilisation is even greater. People are usually hard to be motivated to actively fight against certain processes, especially when they regard them as being futile or normal. Furthermore, mobilisation also requires resources. State actors and corporate actors therefore have an advantage compared to individuals or civic organisations, since they have more means available to mobilise and hence centralise resistance forces against surveillance directed at them.

Indicator/Hypothesis: The more means the observed has to centralise resistance forces against surveillance, the higher tends to be his power level.

What is the degree of transparency of the surveilled?

Although surveillance operations are usually conducted for one specific purpose by one actor and, therefore, generate only partial information, the multiplicity of actors exercising surveillance makes the surveilled increasingly transparent. The sum of all surveillance activities combined, hence, determines the degree of transparency. As we have discussed before, there is a trend to increasingly integrate surveillance operations. Thus, the higher the degree of transparency, the higher is the risk that information and data can be combined and, hence, that the effects of anonymisation of data slowly diminish. Furthermore, Big Data enables to generate highly sensitive information about people even from non-personal data. This gives the observing entities more information and hence increased power over the observed.

Indicator/Hypothesis: The more surveillance operations an object is exposed to, the lower tends to be his power level.

In how far is it transparent for the surveilled how he is surveilled, what kind of data is collected, how it is used and for what purposes?

One of the most severe problems in the surveillance debate is that modern day surveillance mainly happens without sufficient transparency for the subjects of surveillance. Where surveillance operations are opaque, it is not possible to know about (the scope of) surveillance, let alone check and control the observers or resist surveillance. In the realm of security, access to information is most often limited for reasons of 'national security' – a narrative commonly employed in the surveillance debate. Consequently, the public or even control organs of national parliaments cannot effectively check and control security agencies. In the commercial realm, motives and practices of surveillance are often hidden in complex legal texts, such as terms and conditions or privacy policies. Although the European Union's General Data Protection Regulation (GDPR) has aimed to improve transparency concerning data collection and processing, privacy policies and informed consent pop-ups online sometimes remain nibulous or are even deliberately designed to circumvent an informed choice of users. Consequently, people are still not always properly informed what data is given away for what purposes. With a lack of transparency about surveillance operations observers can hide their intentions, which increases the possibility for repurposing and abuse.

Indicator/Hypothesis: The lower the level of transparency for surveillance subjects, the lower the power of the observed tends to be.

7. Conclusion

This paper has addressed two major goals. First, it has offered some reflections on surveillance theory by suggesting that surveillance needs to be analysed from a meso-level perspective and needs to incorporate the examination of power relations in surveillance structures. Second, it has aimed to move from abstract theory to methodology.

Existing surveillance theories have described territorial, centralised surveillance systems with unidirectional hierarchies (Foucault's Panopticon), have distanced themselves from hierarchical structures in surveillance networks or assemblages, and have focussed on the broader impacts of surveillance capitalism in the wider political economy. While all of these conceptions bear some validity, they are missing a focused consideration of power relations at the group-level in a modern digital age. Therefore, this paper has tried to offer a theoretical account of surveillance that incorporates these two issues. Consequently, it has described a surveillance system that is structured in an undefined multidimensional sphere, where actors are all potentially linked in a network. Factual (so used or activated) linkages can differ in their strength depending on the power relation. So-called conglomerates constitute dense connections of certain actors who cooperate in an attempt to increase their surveillance potentialities. Potential links can be activated anytime, characterising the expansionary nature of the system.

Moreover, in order to move from theory to empirical analysis, this paper has proposed a methodological framework for the analysis of power relations in surveillance systems. Different actors are crucial determinants for the form of surveillance and the impacts surveillance can have. Depending on their motives and means, observers have different capabilities and capacities to exploit the surveillance potentialities. Therefore, by evaluating these capacities one can determine the differences in power levels and, hence, the dominating actor in each power relationship. It shows that some actors have considerably more power than others and that surveillance, hence, differs depending on the actor in play. Therefore, it is argued in this paper that hierarchies are still important albeit in a different manner. Hierarchies are no longer unidirectional but multidirectional. Every actor is simultaneously observer and observed.

Highly unbalanced power relations are always problematic, since they bear the threats of domination, manipulation, and abuse. The watcher becomes a powerful actor being responsible for potential discrimination, exclusion, and possibly even charge of crime – be it on grounds of truth or error. This poses ethical, political, and socioeconomic challenges, for these processes bear the potential that fundamental rights and values are violated. As Zuboff argues, modern surveillance has led to an unequal distribution of rights, where the powerful enjoy rights while the powerless are deprived of them (2015, p. 83). Vulnerable groups are most often the one's with the least amount of power and will, hence, be the ones most likely to be affected. In order to understand how power shapes the distribution of rights, it is of utter importance to identify the strong and weak powers within the surveillance system and be able to provide solutions for their regulation or protection. The methodological framework proposed here may offer the basis for conducting such an assessment. However, to validate the accuracy and usefulness of the theoretical ideas and the methodological framework, empirical case studies should now follow. Furthermore, the framework should be open to further discussion and development with scholars within the field.

Acknowledgments

The author would like to thank Prof. Dr. Ingrid Schneider for her feedback, advise, and encouragement.

The Open Access publication of this paper was supported by the Panelfit project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

References

Allen, M. (1994). 'See you in the city!' Perth's Citiplace and the space of surveillance. In Gibson, K., & Watson, S. (eds.). *Metropolis Now: Planning and the Urban in Contemporary Australia*. Australia: Pluto Press, pp. 137–147.

Bogard, W. (2006). *Surveillance assemblages and lines of flight*. In: Lyon, D. (ed.). Theorizing surveillance. Routledge, pp. 97–122.

Boyd, D., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society*, *15*(5), 662–679.

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, *31*(5), 498–512.

Clarke, R. (1993). The digital persona and its application to dataveillance. *The Information Society*, *10*(2).

Chiusi, F., et al. (2020). Automating Society Report 2020. Algorithm Watch, Bertelsmannstiftung.

Cox, R.W. (1993). Gramsci, Hegemony and International Relations: An Essay in Method. In Gill, S. *Gramsci, Historical Materialism and International Relations*. pp. 49–66.

Crain, M. (2018). The limits of transparency: Data brokers and commodification. *New Media & Society*, *20*(1), 88–104.

Dahl, R.A. (2005). *Who governs?: Democracy and power in an American city*. Yale University Press.

Danaher, G., Schirato, T., & Webb, J. (2000). *Understanding Foucault*. Sage.

De la Garca, A. (2020). *States' Automated Systems Are Trapping Citizens in Bureaucratic Nightmares With Their Lives on the Line*. Time. Available at: https://time.com/5840609/algorithm-unemployment/.

Deleuze, G., & Guattari, F. (1987). Introduction: rhizome. *A thousand plateaus: Capitalism and schizophrenia*, 3–25.

Di Salvo, P. (2021). "We Have to act Like our Devices are Already Infected": Investigative Journalists and Internet Surveillance. *Journalism Practice*, 1–18.

European Parliament (2021). Use of artificial intelligence by the police: MEPs oppose mass surveillance. European Parliament Press Room. Available at: https://www.europarl.europa.eu/news/en/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance.

Fernandez, R., Adriaans, I., Klinge, T.J., & Hendrikse, R. (2020). The financialisation of Big Tech. *SOMO (Stichting Onderzoek Multinationale Ondernemingen)*.

Foucault, M. (1979). *Discipline and punish: the birth of the prison*. New York: Vintage Books, Part three: Discipline, 135–228.

Friedman, B., & Nissenbaum, H. (1996). Bias in computer systems. *ACM Transactions on Information Systems (TOIS)*, *14*(3), 330–347.

Galič, M., Timan, T., & Koops, B.J. (2017). Bentham, Deleuze and beyond: An overview of surveillance theories from the panopticon to participation. *Philosophy & Technology*, *30*(1), 9–37.

Gill, S. (1995). The global panopticon? The neoliberal state, economic life, and democratic surveillance. *Alternatives: Global, Local, Political*, *20*(1), 1–49.

Gilliom, J., & Monahan, T. (2012). Everyday Resistance. In Lyon, D., Ball, K., & Haggerty, K.D. *Routledge Handbook of Surveillance Studies*. Routledge.

Gutting, G. (2013), *Michel Foucault*. The Stanford Encyclopedia of Philosophy, Edward N. Zalta (ed.). Retrieved March 14, 2014 from http://plato.stanford.edu/archives/sum2013/entries/foucault/.

Groombridge, N. (2002). Crime control or crime culture TV? *Surveillance and Society*, *1*, 30–36. http://www.surveillance-and-society.org/articles1/cctvculture.pdf.

Hackley, C. (2002). The panoptic role of advertising agencies in the production of consumer culture. *Consumption, Markets and Culture*, *5*(3), 211–229.

Haggerty, K.D. (2006). *Tear down the Walls: On Demolishing the Panopticon*. In Lyon, D. (ed.). Theorizing surveillance. Routledge, pp. 23–45.

Haggerty, K.D., & Ericson, R.V. (2006). *The new politics of surveillance and visibility*. University of Toronto Press.

Haggerty, K.D., & Ericson, R.V. (2000). The surveillant assemblage. *The British Journal of Sociology*, *51*(4), 605–622.

Hawley, J. (2021). *The Tyranny of Big Tech*. Simon and Schuster.

Koskela, H. (2004). Webcams, TV Shows and Mobile phones: Empowering Exhibitionism. *Surveillance & Society*, 2.

Los, M. (2006). *Looking into the future: surveillance, globalisation and the totalitarian potential*. In Lyon, D. (ed.). Theorizing surveillance. Routledge, pp. 69–94.

Lyon, D. (2003). *Surveillance as social sorting: Privacy, risk, and digital discrimination*. Psychology Press.

Lyon, D. (ed.). (2006). *Theorizing surveillance*. Routledge.

Lyon, D. (2007). *Surveillance studies: An overview*. Polity.

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society*, *1*(2), 2053951714541861.

Mann, S., Nolan, J., & Wellman, B. (2003). Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance and Society*, *1*, 331–355.

Mathiesen, T. (1997). The viewer society michel foucault's panopticon' revisited. *Theoretical Criminology*, *1*(2), 215–234.

One Free Press Coalition (2021). Press freedom threatened by global use of spyware. In*Deutsche Welle Online*. Available at:

https://www.dw.com/en/press-freedom-threatened-by-global-use-of-spyware/a-59361580.

Poster, M. (1995). *The Second Media Age*. Cambridge: Polity Press.

Rogers, R. (2008). Consumer technology after surveillance theory. *Mind the screen: Media concepts according to Thomas Elsaesser*, 288–296.

Sætra, H.S., Coeckelbergh, M., & Danaher, J. (2021). The AI ethicist's dilemma: fighting Big Tech by supporting Big Tech. *AI and Ethics*, 1–13.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89.

Zuboff, S. (2019, January). Surveillance capitalism and the challenge of collective action. In *New labor forum* (Vol. 28, No. 1, pp. 10–29). Los Angeles: SAGE Publications.

Author biographies

Catharina Rudschies is a PhD candidate and research associate at the Department of Informatics at Hamburg University. She holds a Bachelor of Arts in European Studies from Maastricht University and graduated with a Master of Science in Politics, Economics and Philosophy from Hamburg University.