Surveillance as public matter

Revisiting sousveillance through devices and leaks

van der Velden, L.C.

Publication date
2018

Document Version
Other version

License
Other

Link to publication

1 Tackling internet surveillance

1.1 Introduction: Getting to know the field

It was only after participating in workshops about surveillance technologies that I noted that a particular attitude towards technologies often called ‘hacking’ was directed towards surveillance problems, and that it practiced particular ways of ‘knowing surveillance’. People would not only dissect what surveillance was made of, technically speaking, but they would continue to give it their own twist. For example, a workshop organised by ‘net artist’ Heath Bunting on digital identities and citizenship (see also Fletcher et al. 2011) built on his research into the various digital databases that form the building blocks of contemporary corporate and governmental surveillance. Bunting mapped the databases in which people are included or excluded. He subsequently re-appropriated them for subversive ends: via his workshops he helped participants to design, create and ‘take on’ alternative identities. If one knows that being registered in data database X gives you access to service Y, one can build new identities from scratch. This allowed people to create fictive identities that can do real things. In other words, by creatively using the knowledge about databases these workshops explore the options to live through the surveillance society in a different manner.

Other workshops combine this emphasis on insight and agency by teaching people how to intervene through code and devices. For instance, people like Julian Oliver and Danja Vasiliev (see also Zandbergen, April 2013) offer workshops in the basic steps of hacking. These workshops allow people to play with basic hacking tools such as ‘network sniffers’ that allow one to read network traffic. In this way, participants are invited to practice surveillance themselves, which, in turn generates insight. Workshops like these make networked communication tangible and understandable and show one how easy surveillance can be conducted if communication is not encrypted by users or service providers.

There are also online projects that ‘demonstrate’ surveillance is taking place. They take the shape of reports or visualisations of (systematic) examples of data monitoring and interception, such as the ‘Open Observatory of Network Interference’ (OONI), which measures network interferences. Others visualise online tracking in real time, for example the browser add-on ‘Lightbeam’ shows you which third parties are actively tracking you on the web. In some cases, these and similar mapping projects are combined with technological modifications to interrupt or block data monitoring by installing plugins or using encryption. Again here, rendering surveillance visible is closely connected not only to the capacity to form insight, but also to the capacity to subvert.

Such interventions that have data monitoring as their target constitute rich and interesting objects of study. They ‘display’ what is going on behind the front-end of the computer and articulate data monitoring practices as a problem worthy of public attention and action. Moreover, this knowledge is not necessarily acquired or shared within academic institutions, but in settings such as art institutions, hacker conferences, and technology collectives, both offline and online. Despite not being part of the ‘official’ knowledge institutions, these interventions produce their own knowledge repositories and provide occasions to share and learn about concrete surveillance practices. For somebody coming from Science and Technology Studies and Philosophy, this was a most interesting intersection: a particular niche of knowledge practices conducted in the public domain, in need of further exploration.

These workshops, including their emphasis on insight and agency, and their aspiration to make a critical intervention in relation to contemporary practices of surveillance, inspired the topic of this dissertation. In this dissertation, I present an analysis of a variety of interventions that all share a common concern: to tackle surveillance. This chapter is dedicated to outlining what it means, practically and conceptually, to ‘tackle surveillance.’ I then proceed to explain how Surveillance Studies have theorised such interventions, and how they have struggled with the concept of surveillance itself. Throughout the chapter I argue that the concepts within Surveillance Studies are not addressing important aspects of these interventions, like their particular methods. In short, if we want to understand an important range of critical internet practices we need another way of looking. I conclude this chapter by suggesting that we need a different conceptual vocabulary. In subsequent chapters, I provide and implement this vocabulary.

1.1.1 Critical interventions with internet technologies

According to anthropologists and media critics, critical interventions with the internet are part and parcel of a particular internet 'milieu'. Writing in the early 2000s, Geert Lovink theorised the emergence of 'critical internet culture': 'critical Internet culture can positioned at the crossroads of visual art, social movements, pop culture and academic research. Its interdisciplinary intention is to both intervene and contribute to the development of new media' (Lovink 2002, 17). Since then, several terms have been brought forward to describe critical or interventionist and technology-oriented acts (often laid out in manifestos). For example, the notion of 'tactical media' was coined in the late 1990s to refer to exactly those kinds of media practices that are interventionist and subversive, and often include an artistic touch (Carcia and Lovink1997). Another one is 'critical engineering', referring to an approach in which dependencies on technology are exposed and dismantled, and often proceeding without authorisation from those who produce the technology in question. As the Critical Engineering Working Group (2011) states: 'The greater the dependence on a technology the greater the need to study and expose its inner workings, regardless of ownership or legal provision'. An even more politically loaded term is 'hacktivism', a term that describes (disruptive) hacking in order to effectuate political and social change (Cult of the Dead Cow 2001).

This interventionist dimension is one of the core elements of what anthropologist Gabriella Coleman defines as 'hacker culture' (Coleman 2013). She uses the term to speak about practices that exhibit a subversive attitude towards computers and networked culture (see also Lovink and Riemens 2013; Maxigas 2014a). The term 'hacker' might be most strongly associated with criminal acts. Coleman, however, transcends the stereotypical image of the masked, hooded hacker bent over a battered laptop in a darkened room, and uses the term to refer to 'computer aficionados driven by an inquisitive passion for tinkering and learning technical systems, and frequently committed to an ethical version of information freedom' (Coleman 2013, 3). Coleman further specifies her understanding of hackers when she discusses how hackers practice a 'politics of technology'. Sociologists of science and technology have in the past conceptualised the capacity of technology to be the site of political ordering and contestation. Coleman refers to Langdon Winner's famous work 'Do Artifacts Have Politics?' (1980), in which Langdon Winner presents the Long Island bridge as a tool for social segregation: through its height, the materiality of the bridge could prevent public transport from going through (as the buses were too high). She argues that, like bridges, the internet is also part of an infrastructure, a site of ordering, and that hackers take part in this process:

> Winner famously states, the politics of technology are about "ways of building order in our world," then hacker and geek politics are geared toward reordering the technologies and infrastructures that have become part of the fabric of every- day life. A close corollary is that geeks and hackers often care deeply about and intervene in a networked infrastructure that can be, at some level, reordered without asking permission of any institution or actor. In contrast to other large-scale technologies and infrastructures, like the highway system, the Internet is to some degree modifiable and is a site of active struggle. (Coleman 2011, 515)

According to her definition of hacker culture, hackers aim to keep this infrastructure open. Along similar lines, anthropologist and science studies scholar Christopher Kelty (2008) identifies the rise a typical form of politics in the free software moment (1970-1990s). He uses the term 'geeks' to describe its participants. Kelty argued that struggle on the internet is often about the 'site' itself: the internet, and to an open internet in particular. According to Kelty geeks are concerned about surveillance and censorship because they would be devastating for principles of the internet itself and how it is lived (Kelty 2008, 5).

The literature about interventions concerning the internet and their environments addresses a few important themes on which I will elaborate below: first of all, the widely-shared concern relating to surveillance; second, the emergence of particular methods and approaches; and third, the specificity of how publics are mediated through technological interventions.

1.1.2 Surveillance, methods and publics

Anthropologists such as Coleman and Kelty have stressed that despite the differences in (ideological) discourses and professional backgrounds, hacker practices share concerns relating to surveillance and censorship.[4] However, these shared concerns do not form one particular political program. Even though techno-liberalism has put a dominant stamp on internet culture (Kelty 2008, 55), scholars of hacking point out

[4] I write on purpose that these are perceived recurrent concerns, and not commonly shared concerns. Within the hacker forums it is in fact debated whether surveillance is and should be a priority concern when internet networks need to be established in the first place. Again others argue that especially in the countries with a marginal internet infrastructure, surveillance risks are even higher (Gonggrijp 2014).

the many ideological incoherencies within (contemporary) hacker communities. For instance, Coleman argues that hacker politics can have both liberal and Marxist tendencies (Coleman 2011, 514). In short, not all hackers are techno-libertarians. See for instance the hacker events hosted in Calafou (Spain), an ‘eco-industrial, post-capitalist colony based on a cooperativist model’ (Maxigas 2014b, 148), and attempts to connect digital commons initiatives with institutional policies aiming at social and economic inclusion in Barcelona (Mayo Fuster Morell interviewed by Transnational Institute (2017)). Kelty confirms that people that work with and build free software come from diverging political and professional backgrounds. It is important to emphasise that hacking is not necessarily a politically harmonious process,[5] and that when we discuss practices that can be associated with hacking, we should not presuppose a single (coherent) group in terms of societal vision.

This diversity notwithstanding, Coleman stresses the prevalence of certain ‘commitments’ among hackers to ‘some version of information freedom’ (Coleman 2011, 512-13). Kelty states that geeks share a common history of concern about legal and technical attempts at surveillance and censorship (Kelty 2008). There is a documented history of technical interventions to circumvent surveillance, censorship, or perceived censorship in the form of copyright restrictions (Coleman 2009, Kelty 2008). In sum, interventions concerning surveillance can be seen as important examples of critical internet practices. This dissertation continues along that line of argumentation by analysing contemporary interventions that share a concern about surveillance; yet do not necessarily constitute a single political ideology (and which is also not part of my study).

Second, this critical internet milieu provides a breeding space for experimental methods and approaches. It is important to note that there is an infrastructure for knowledge exchange. People are networked through various meet-ups, conferences and working spaces. There are laboratory-like places like ‘hacklabs’, ‘fablabs’ and ‘makerspaces’ (Maxigas 2014a), conferences (some attracting more than 10.000 visitors such as the Chaos Computer Club Conference (Chaos Computer Club 2016), event-based collaborations such as ‘hackathons’ (meet-ups in which people come together to ‘hack a problem’ or to ‘build’ a tool or network), online platforms to review and build on each others code, such as GitHub, and discussion channels such as Internet Relay Chat (IRC)-channels and mailing lists. These infrastructures are

[5] For critical analyses of hacking, hacktivism and problems of exclusion and diversity, and attempts to redefine hacking practices through those criticisms, see D’Ignazio et al. (2016), Hache (2014, 171), and Tanczer (2015).

'cooperative channels' of hackers (Coleman 2013, 210) and they serve as moments for knowledge exchange and social encounters.

Such places, settings and encounters allow, according to Lovink and Rossiter, for the emergence of specific and recurrent methods (Lovink and Rossiter 2011). New platforms for collaboration and forms of knowledge production may develop in the niches and margins of network cultures (as opposed to institutionalised and commonly-known platforms that have millions of users). However, over time, also these alternative practices may to become standards or 'protocols' – by habit. Lovink and Rossiter call this process 'seriality':

> Hacklabs, barcamps, unconferencing, book sprints, mobile research platforms – these are all formats that through the work of seriality have become standards for network cultures. (…) Their hit-and-run quality might give the appearance of some kind of spontaneous flash-mob style raid, but in fact they are carefully planned weeks, months and sometimes years in advance. Despite the extended planning duration and intensive meeting space of these formats, they are notable for the way in which they occupy the vanguard of knowledge production. (Lovink and Rossiter 2011, 433)

Similarly, McQuillan refers to 'hack-based citizen science' as 'artisan science' (2013, n.p.), knowledge practices contextualised in hacker and occupational spaces that have the potentiality to provide prototypes for alternative futures. The (for many people) incomprehensible terms given to these events (e.g. 'barcamps', 'unconference') indicate already the existence of specific esoteric 'styles'.[6] This is not just hipster jargon: research has shown important differences between the various 'labs', such as makerspaces versus hackerspaces, in terms of approaches to the politics of technology (Maxigas 2014a). Some of the more 'radical tech activist' groups are also organised in an unconventional way, working deliberately outside of corporate or state institutions and on the basis of 'collective organising principles' (Milan 2013, 12). The formats can institutionalise though, as also indicated by Lovink and Rossiter. One example of a format that grew out of the niches and transformed into a more widely shared standard practice is the 'hackathon'. It is a format for collaborative knowledge-production associated with hacker practices but increasingly governments and companies tend to deploy hackathons as way to organise citizen participation and data gathering (see also McQuillan 2014). Important for this dissertation is the attention that scholars have devoted to the specific socio-material

[6] A barcamp is a user-generated conference built on open (technology) formats. A so called 'unconference' departs from the general format of a conference because it has no predetermined speakers program but sets the program on the fly.

instrumentations through which things are ‘done in a certain way’. As I will show, paying attention to models of knowledge practices is also relevant for understanding how surveillance is made public in critical internet cultures.

Third, this scholarly work on hacker, geek, and network cultures suggests that technical interventions with the internet matter for how we should think about the publics emerging from these interventions. Kelty even coined a dedicated term to give expression to the activities of what he calls geeks: the ‘recursive public.’ The notion of ‘recursiveness’ is meant to give expression to the, according to him, driving forces of many geek practice. According to Kelty, geeks express a drive and deploy tactics to keep the internet open (Kelty 2008, 29). In social imaginaries that circulate among geeks, censorship (and surveillance by its effect) would harm the decentralised and open internet infrastructure (55) which also allows for the modes of association of geeks. Within this narrative, surveillance and censorship is considered as damaging and something to be tackled (51). Therefore the geek public refers to itself because it aims to maintain its own infrastructural conditions; hence, ‘the recursive public’. From his point of view, interventions via internet technologies are techno-political interventions that co-constitute a very specific public.

Even though Kelty might be generalising a bit, his notion of the recursive public aims to take serious the practical work and political sentiments of the people he has studied. By using this technical term of ‘recursion’, he not only expresses what he thinks geeks do; since the term also resonates with programming language, he also speaks to the technical aspects of their work. Coleman alludes to a similar point when she connects hacker practices to hacker publics. She mentions that technological ‘configurations’ co-shape hacker publics, although she adds that this happens not in a deterministic way ‘since hackers do not exist in isolation but are deeply entangled in various distinct institutional and cultural webs and economic processes’ (Coleman 2011, 512). Lovink and Rossiter (2012) in their manifesto-style of writing argue that thinking about media in general should incorporate the (collaborative) practices of network cultures, in order to keep ‘concept production’ (within media studies) vital and engaged with its subject matter. This dissertation shares this agenda. Concept production around specific interventions with the internet should speak to the practices at stake. The relation between ‘how surveillance is made public’ and how we subsequently talk about this public formation should be clear.

1.1.3 Making surveillance public

I have briefly sketched these scholarly reflections critical internet practices, partly with an introductory purpose, but also because the three issues discussed above – surveillance being perceived as a problem, the emergence of specific methods, and the specificity of publics – are fundamental concerns in this dissertation. The interventions that are the subject of this dissertation can be approached productively by keeping these concerns in mind. They return in the form of questions about very concrete instances. These include the subject matter of surveillance as problematic (Which aspects of data monitoring are selected and tackled? How is surveillance perceived through these interventions?); the methods through which this subject matter is turned into a perceivable problem (What instruments or methods are being used to make things visible?), and an appreciation for a specific terminology of publics (What do those methods mean for the notions we assign to this intervention?) Taken together, these concerns provide guidelines for my overall research question: *How is surveillance made public?*

To address the above-mentioned concerns I merge two fields of study, which I think are most suitable for the job. In a nutshell, I draw Surveillance Studies (§ 1.2) and STS (chapter two) together to study and theorise a particular kind of 'intervention' with the internet that media scholars have highlighted as important to critical internet and hacker cultures.

First, the field of Surveillance Studies provides extensive analysis of the *subject matter of surveillance*. Surveillance Studies has reflected on the concept of surveillance, and, most importantly, has theorised interventions that 'expose' surveillance, under the header of 'sousveillance' (Mann 2004). In the rest of this chapter, I will critically discuss this concept, its theoretical lineage, and its limitations. This criticism of 'sousveillance' is followed by a discussion of conceptual revisions within Surveillance Studies. Specifically, I will focus onthe notion of the assemblage (Haggerty and Ericson 2000) and discuss to what extent it provides an alternative.

Next, to account for the methods, or the *how* in the research question, I draw on the field of Science and Technology Studies (STS). STS is a field that has scientific knowledge and technology development at its core and therefore provides analytical tools to study methods and instruments of knowledge production. In doing that I will draw in particular on approaches from Actor Network Theory (ANT), also known as a study of 'translations' (Latour 2005b), and on its notion of the 'device' (Callon 2004).

It is also through drawing on ANT that I account for the theorisation of how surveillance is being *made public* (Latour and Weibel 2005). This is because ANT has informed a strand of philosophical thinking that has theorised how 'things being made public' feed into to 'how the public is made' (Marres and Lezaun 2011). These reflections on STS, ANT, and ANT's notion of the material public, will be discussed in the second chapter. But first, let us reflect on Surveillance Studies.

1.2 Surveillance studies

'Surveillance Studies' is not a discipline. It should rather be understood as a research area bound by a topic of interest. According to David Murakami Wood (at the time of writing the editor-in-Chief of the journal *Surveillance & Society*) surveillance studies is 'a transdisciplinary field that draws from sociology, psychology, organization studies, science and technology studies, information science, criminology, law, political science and geography' (2007, 245). Surveillance studies is, according to the editors of the *Routledge Handbook of Surveillance Studies,* a field 'in becoming' since the last two decades (Ball, Haggerty and Lyon 2012, 1). Signs of this growth are the emergence of Handbooks (such as the aforementioned), Introductions (like David Lyon's *Surveillance Studies: An Overview* (2007)), Readers (for instance *The Surveillance Studies Reader* by Sien Hier and Josh Greenberg (2007), and the critical evaluation of such attempts to summarise the field (Murakami Wood 2009). There are mapping projects that geographically plot surveillance experts and projects. For example see the Google Maps visualisation of surveillance scholars and projects, on the website of the Surveillance Studies Forschernetzwerk (2013).

A few key points of reference emerge from this meta-literature. As inspiring predecessors of surveillance studies feature Karl Marx, Max Weber, George Simmel (as referred to in Marx 2012, xxvii), Anthony Giddens, and James Rule (in Ball, Haggerty and Lyon 2012, 4-5; Murakami Wood 2007, 245). Historian of ideas and philosopher Michel Foucault has been of great influence to the field (Ball, Haggerty and Lyon 2012, 4; Marx 2012, xxviii; Murakami Wood 2009). He is, according to Gary Marx 'the dominant grandfather' (Marx 2012, xxvii) and Ball, Haggerty and Lyon go so far as to lament the existence of '"Foucault obsessed" stereotypes' (2012, 5). Contemporary thinkers include scholars such as Oscar Gandy, Mark Poster, Gary Marx, David Lyon, and even more current, Kirstie Ball, Kevin Haggerty, and David Murakami Wood.

Gary Marx demarcates surveillance studies from other, what he calls '"studies" fields' as follows:

> Surveillance studies as a growing epistemic community is unlike most other "studies" fields. It is not based on a geographical region, ethnicity, gender or life style (e.g. as with urban or women's studies). Nor is it based on a single disciplinary, theoretical or methodological perspective (e.g. sociology, postmodernism or survey research). Rather it is based on a family of behaviors all dealing in some way with information about the individual (whether uniquely identified or not) or about groups. The social significance of the activity is in crossing or failing to cross the borders of the person—factors which can be central to life chances, self-concept and democracy. (Marx 2012, xxviii)

This 'family of behaviours' overlaps with many other fields of research. In that sense the field is still open to a myriad of approaches and methods (ibid., xxvii).

Because of the multiform make-up of the field, narratives that try to bring 'order' in the field may vary. Sociologist David Lyon in his book *Surveillance Studies: An Overview* distinguishes various 'sites', or 'areas' of surveillance' (2007, 25). These are 'military discipline and intelligence', 'state administration and the census', 'work monitoring and supervision', 'policing and crime control', and 'consumption and making up consumers'. Geography-oriented scholars theorise the spatial elements of surveillance and the change of surveillance architectures (Murakami Wood 2007). Naturally, scholars do not always agree; for example, the relevance of the notion of 'privacy' and how it relates to surveillance is a contested topic (Bennett 2011; Stalder 2002). According to the editors of the Surveillance Studies Handbook, one of the 'greatest surprises' for surveillance scholars is the 'muted public response' to contemporary surveillance (Ball, Haggerty and Lyon 2012, 4). This thesis responds to this last concern, but rather in an affirmative way: we should pay extra attention to concretely articulated public responses. However, instead of dismissing the general public and its (lack of) response, I am interested in the interventions conducted by localised – from Kelty's perspective 'recursive' – publics that actually *do* stage the problem.

The notion of 'surveillance' is itself a complicated umbrella term. According to surveillance scholars, the complication with the term begins with the kinds of actors that are conducting surveillance: colloquially speaking, surveillance refers to monitoring by the state, but many scholars include consumer surveillance by corporations (Lyon 2007, 40; Pridmore 2012), and many have argued that corporate data monitoring and state surveillance merge together (Lyon 2013). For Donaldson and Wood, surveillance is not just about gathering data, but it refers very specifically to 'ordering processes that control information, and possibilities for activity and action' (2004, 380). For them, therefore, surveillance has a steering or managing effect. Others, however, point to the fact that surveillance scholars have to be attentive to the fact they themselves capture things as being ‘surveillance’. The editors of the *Handbook of Surveillance Studies* state the following:

> Surveillance scholars should also reflect on the ontological, epistemological and political consequences of classifying something as being of surveillance. While surveillance theory de-normalizes and problematizes attempts by the powerful to amass information about populations, surveillance scholars need to be mindful about what is lost as part of that surveillance-theoretical endeavor. (Ball, Haggerty and Lyon 2012, 9)

In other words, considering something as surveillance practice, and analysing it within a conceptual framework of surveillance, is already an epistemological decision. The way this dissertation tries to mediate this problem is by making space for knowledge claims about and definitions of data monitoring provided by actors that are engaged in tackling surveillance, and thereby giving them a role in the process of concept production (Lovink and Rossiter 2012) about their work and their subject matter.

In what follows I argue that we need to reformulate two important strands in the surveillance literature, those that have ‘sousveillance’ and ‘surveillant assemblages’ as core concepts. These strands, on the one hand, provide important foundations for understanding surveillance and counter measures. At the same time, if we take into account the rapid developments in the technologies that take part in contemporary surveillance networks, the objects that have made us conceptualise surveillance, and insights into (methods emerging from) critical internet culture that target surveillance, it becomes clear that an update is urgently needed. The next few sections are dedicated to presenting these two strands of surveillance literature, and I will provide arguments for this update.

1.3 Sousveillance

Whenever when I engaged with surveillance scholars and exchanged thoughts about my work, they would often tell me that what I was looking at is ‘sousveillance’. And indeed, that term partly captures the practices that I want to discuss. They are interventions that expose and tackle surveillance by ‘bringing it under public scrutiny’, and they also involve a participatory, ‘bottom up’ dimension, these are all things that are associated with ‘sousveillance’. It is therefore necessary to relate to this concept. I will do so by first explaining the term, and discuss its advantages and limitations, after which I explain why I use a different analytical vocabulary in my case studies. The term was coined about a decade ago by Steve Mann and refers to 'surveillance from below' (hence, the French word 'sous'). Sousveillance is an activity through which individuals under surveillance repurpose technologies to generate awareness about surveillance processes (Mann, Nolan and Wellman 2003). This kind of (activist or subversive) response to surveillance differs from other counter-surveillance initiatives such as (policy) pressure groups or technical attempts to hide data (Lyon 1994, 162) because of its approach: using surveillance-like methods to expose surveillance. The projects I have examined can be situated in this niche of surveillance studies because they 'target monitoring practices' by exposing them.

Mann offers the following definition of sousveillance:

> Sousveillance (undersight): (1) The recording of an activity by a participant in the activity, typically by way of a human-borne camera; (2) Inverse surveillance (also known as reverse surveillance or inverted surveillance), i.e. the recording or monitoring of a high ranking official by a person of lower authority. (2004, 627)

According to Mann, surveillance means that an actor with higher authority captures content while this actor is not equal ('peer') in the process of being surveilled. In the first subcategory of sousveillance, one becomes a participant or 'a peer' within surveillance practices. He also calls this 'personal sousveillance' or a 'human-centred' form of sousveillance (ibid., 620). When conducting this type of sousveillance, persons subject themselves to recording devices though individual or community-based interventions. The second subcategory of sousveillance, 'inverse surveillance', refers to practices by which people use surveillance technologies to monitor (surveying) authorities. He also calls this 'hierarchical sousveillance' (ibid.) because the person that does the recording is not being surveilled. Mann defines sousveillance with these distinctions, but the term is regularly used in its second meaning (without constantly specifying it as 'inverse surveillance') (Bradshaw 2013; Fernback 2013; Reilly 2015; Van Buuren 2014), or it is framed in more loose terms as 'watching the watchers'.

The notion of sousveillance is based on the assumption that 'technologies of seeing' are powerful. It is the idea of an 'inversed panopticism' that lies at the root of the notion of sousveillance (Mann, Nolan and Wellman 2003, 332). The figure of the 'panopticon' is according to many scholars in surveillance studies out-dated (to which I return in the next section). However, to understand how my study is situated in relation to sousveillance analyses, it is crucial to state clearly the concept. In *Discipline and Punish: The Birth of the Prison*

(1977) Foucault used the carceral architecture of the panopticon as an exemplar to describe the emergence of a new form of power in the late eighteenth century. His theorising drew on the panopticon as envisioned by the utilitarian legal philosopher Jeremy Bentham. Through its architecture of visible cells around a central tower the panopticon would force the prisoners to behave themselves even in the absence of the guards. The possibility of being watched would provide an efficient power mechanism that would render the use of physical pressure obsolete. According to Foucault, various technologies of visibility and registration, resembling the panoptic model, emerged in settings such as schools, factories and clinics in France of the eighteenth century. They made differences between people visible, and this simultaneously enabled the emergence of a normal/abnormal binary, which in turn stimulated changes in behaviour. In this way, panoptic techniques contributed to disciplinary processes by which human subjects formed themselves towards a normalising gaze. Foucault's work has been fundamental to theorising within surveillance studies (Ball, Haggerty and Lyon 2012, 5; Haggerty 2006; Murakami Wood 2007; Murakami Wood 2009; Marx 2012, xxvii). Moreover, it is the inversion of panopticism that is captured with the term sousveillance: 'Just as the panopticon operates through potential or implied surveillance, so sousveillance might also operate through the credible threat of its existence' (Bakir 2010, 157).

In a critical reflection on surveillance theories, Bart Simon (2005) describes how, after Foucault, two versions of Foucault's surveillance narrative can be traced which developed into two branches of research.[7] One narrative is inspired by the mechanism that facilitated the watching over the inmates in the panopticon. This narrative stresses *the power game of visibility*: How do people behave when being watched? This has informed studies into normalisation. The other narrative is about the watchers, and it has stressed the techniques of supervision and administration (ibid., 5). It has emphasised *the power of the panoptic gaze*: how do the watchers construct knowledge? Within the study of new media technologies, the latter narrative has influenced studies concerned with the power of databases and social sorting (the categorisation of groups of people). Simon explains that the strength of Foucault's theory of power was derived from the coupling of the two narratives. Foucault's analysis pointed out that persons under supervision perceived themselves appealed to the (research) techniques that fed the mechanics of administration. Therefore, the emerging complex of observation and registration technologies enabled

[7] He calls these narratives 'panoptic sorts', borrowing the term from the work of Oscar Gandy's *The Panoptic Sort: A Political Economy Of Personal Information* (1993).

simultaneously the study *and* the constitution of a population (ibid., 12).[8] According to Simon, the first strand of studies after Foucault has disregarded the process of knowledge construction, while the second has neglected the importance of the subject being or feeling visible (the process of 'interpellation'). Simon argues that the second narrative, 'the power of the panoptic gaze', is the more prevalent within surveillance studies.

Interestingly, most *sousveillance* literature has emphasised the game of visibility, linking up to the first surveillance narrative. By definition, personal sousveillance is focussed on the construction of subjectivity conditioned by surveillance, and the effects of being monitored (which can also be done in an experimental or playful way). Typical examples that figure in sousveillance analyses include: self-recording and confronting others with being recordable (Mann 2004), publishing (video) recordings online to expose people's bad behaviour (Dennis 2008), self-surveillance as a form of self-defence (against identity theft) or personal safety (ibid.), and responses to being visible on mobile cameras versus CCTV (Timan and Oudshoorn 2012). Sousveillance is also seen as a method for presenting alternative narratives, such as alternative views on riots (Reilly 2015) and the creative rewriting of city life (Cardullo 2014). The more confronting (or 'hierarchical') forms of sousveillance aim to bring about instances of awareness about (misuse by) authoritative powers. Examples include the publication and dissemination of incidents of police violence (Bradshaw 2013; Fernback 2013; Mann, Nolan and Wellman 2003). One famous and recurrent sousveillance example is the video of the beating of Rodney King by the police in Los Angeles, which was recorded and published by a bystander (Mann, Nolan and Wellman 2003, 333). It is one of the most famous instances of citizen documentation of racial police violence. Other examples are (secret) mobile phone recordings (see Bakir (2009) on the illegally captured footage of Saddam Hussein's execution), leaked military recordings (such as the publication of the Collateral Murder video by WikiLeaks (Mortensen 2014)), and whistle blowing in general (Van Buuren 2013). This hierarchical form of sousveillance can include actions against corporations as well, for example protests against data collection, such as Facebook protest groups directed against Facebook (Fernback 2013).

Personal sousveillance can lead to personal confrontation with those formally in the position of the watcher and subsequently have a reflexive dimension: such interventions are 'bringing into question the very act of surveillance itself' (Mann, Nolan and Wellman 2003, 337). In the readings of hierarchical sousveillance, the possibility of

[8] In Foucault's terms (1991), the 'politico-anatomy' (138) of the body intersected with a 'macro-physics of power' (160).

sousveillance (and therefore the threat of permanent visibility) is already considered to be a counterforce (Bradshaw 2013, 459; Mann and Ferenbok 2013, 29) or even a tool for keeping authorities in check (Van Buuren 2013, 251). They entail, as Brucato notes sceptically (2015, 457) a 'promise of accountability'. Such readings of sousveillance remain within panopticism as a visibility effect: they focus on the subversion, and even the equalisation, of the power relations that would stem from the power to see. Here it is interesting to return to Bart Simon's analysis of the panopticon as both an instrument of visibility as an instrument of knowledge construction. According to him, the panopticon, for Foucault, is an 'epistemological device for producing knowledge about the social world' (Simon 2005, 12). It is an instrument, a kind of microscope (ibid.). Furthermore, it does not only induce effects 'on the ground' by making people visible, but it also *enables* visibility by its construction. Simon explains the process by which the supervisors are enabled to see, by referring to how the workings of the microscope are explained in the sociology of science:

> To 'see' an object under a microscope requires the transformation of that object (Hacking 1983; Latour 1987; Gooday 1991). It is dissected, separated, isolated from the larger wholes of which it is a part. It is then prepared for display, fixatives may be added, cross-sections taken, and so on... the process is not at all ad hoc but the result of the application of skill in accordance with detailed protocols. This is what allows the object to be compared to others and to a general body of knowledge. The visible object is, in effect, a by-product of all these operations. (Simon 2005, 12)

If the supervisor engaged in panoptic methods needed instruments of registration and comparison to make surveillance work, surely the practitioners of sousveillance need them as well. This calls for the question: How does an instance of exposure become a fact, something that captures surveillance and/or violence in a more systemic way? In analyses of sousveillance, more often than not, the camera and video content figure as central objects in the argument. Whether visual data or not, the analyses often talk about instances of capturing data and methods for disseminating information. But how do sousveillance practitioners compare material and set up the conditions for the comparison of their (surveillance) objects? What constitutes the database of the sousveillance practitioners? In other words, what is their 'lab'? If surveillance scholars may have focused little on power games of visibility (Simon 2005), sousveillance scholars rarely focus on the ways in which knowledge is produced and functions in sousveillance practices.

Mann himself is quite exceptional in this regard. He turned his body into a research method. For decades he wore computing devices on his body and was thusly able to compare behavioural responses to his personal surveillance from people in various settings. He experimented with different kinds of designs of wearable cameras to measure the different responses. [9] In other words, he turned his own bodily movements into an ethno-methodological method, a form of ‘action research’ (Mann 2004, 625).[10] Next to Mann’s perspective on sousveillance as a research approach, there are a few other studies that do highlight data production and management, which is obviously part of sousveillance processes (Bakir 2010, 21). Cardullo (2014) mentions data management activities, and Brucato (2015) refers to how the production of sousveillance images is situated and bound to a point of view. Nevertheless, the sousveillance literature only scarcely refers to how sousveillance practitioners construct knowledge. That body of work is therefore not the best source for finding analytical tools to study this phenomenon.

An important takeaway from the sousveillance literature is that actors ‘on the ground’ can deploy and redirect surveillance technologies in their own ways. However, a major problem with the concept of sousveillance is conceptual consistency and balance. In general, lines of inquiry using the concept of ‘sousveillance’ leave out an important part of the power-axis in surveillance, by assuming that rendering surveillance visible suffices. Although Mann himself has shown that the practice of sousveillance can also function as a research machine, this analysis has not been sufficiently influential. My work aims to fill that gap by not looking at the reflexive effects of encounters by which the watchers are being watched, nor at the possible reflexive and disciplining effects of sousveillance, but by shifting focus to the instruments of those that tackle surveillance, to the objects that they select and their methods for bringing surveillance into view.

A second problem with sousveillance theory is that it heavily builds on panoptic theory of which many surveillance scholars argue it is of limited use. This will be discussed in more detail in the next section. After that I explain how my own research approach aims to move beyond these challenges.

[9] See his disclaimer about this artistic method of research versus one that would conform to academic (and ethical) requirements (Mann 2004, 621)

[10] As Bakir explains, Mann’s ‘method’ was inspired by Garfinkel’s breaching experiments as a form of ethno-methodological research (2010, 16). Garfinkel proposed that breaching, conducting unexpected or disruptive forms of behaviour, was a way of studying social norms. The reactions resulting from these experiments are indicative of (hidden) social assumptions and organisation.

1.4 Revisiting surveillance concepts

Much of the surveillance (and sousveillance) literature builds on a particular reading of the panoptic figure that has been critically debated in the past two decades. This central debate is about its usefulness as a guiding metaphor in studying contemporary surveillance practices. Surveillance scholars in the past few decades have scetched how the (mass) adoption of digital technologies have challenged surveillance theory. Surveillance scholars stress, for instance, that contemporary surveillance is not just about the direct supervision of individual human beings by human beings. According to Haggerty (2006), only a fraction of contemporary surveillance deals with monitoring 'human beings in any conventional sense' (30). Instead, surveillance is often concerned with non-human entities. Public safety is is guarded by smart cameras registering events triggered by unexpected movements. Search engines on the web perform present-day customer research. Moreover, the targets of surveillance are not merely human beings (Adey 2004, Donaldson and Wood 2004; Haggerty 2006). Examples of common non-human targets of surveillance are products in supermarkets (Grommé 2015), or suitcases in airports, objects to be sorted out in order to regulate mobility (Adey 2004). Credit companies monitor user data such as browser types and screen resolution, as possible indicators of creditworthiness (Deville and Van der Velden 2015). State agencies follow web objects such as Google cookies for intelligence purposes (Soltani, Peterson and Gellman 2013b).

The inclusion of non-human activity in the analysis of surveillance enriches the picture of contemporary surveillance, but it also makes the processes harder to grasp. Surveillance works through merging different kinds of data, such as various sense impressions, historical data, digital and corporal traces. Technical apparatuses enable surveillance to go beyond what is directly visible and they transpose data in time and space (Marx 2002, 12). For instance, digital technologies and tracking technologies, such as GPS or RFID technologies, make it possible to connect behavioural data, such as movement patterns, with, for instance, historical or demographical information. Subsequently, this information, or bits of it, can be stored in databanks that provide a frame of reference for further analysis (Rathenau 2007). The combination of several types of surveillance is expected to produce meaningful information: or, as Gary Marx (2004) asserts, 'Meaning may reside in cross-classifying discrete sources of data (as with computer matching and profiling) that in and of themselves are not of revealing' (ibid., 21). Contemporary surveillance is, therefore, less concerned with what is shown by one specific individual at a certain moment, but is increasingly directed to settings and patterns of relationships, and, particularly in the case of crime or disease prevention, to relevant contexts and potentially dangerous environments (Rathenau 2007). In other words, contemporary surveillance practices converge into complex socio-material networks, in which both processes of collecting and reassembling data take place in a diffused manner.

Faced with these increasingly complex processes, many scholars within surveillance studies have argued that available theoretical frameworks have difficulties with critically assessing contemporary developments. Conceptually, surveillance studies are still struggling with the theoretical legacy of Michel Foucault's panopticism (1977). The amount of literature on the panopticon within surveillance studies is in fact overwhelming; as is panoptic jargon. Some scholars have literally extended panoptic thinking to contemporary technologies, describing for example Facebook 'behaving like' a panopticon (Westlake 2008). Others have creatively moulded the concept into various forms, including 'omnicons', 'opticons' and 'veillances' and more derivatives along these lines, as Haggerty illustrated in an extensive literature review (2006, 25-26).

At the same time, the usefulness of the panopticon as an analytic frame to understand contemporary surveillance networks is debatable. One of the most pertinent criticisms relates to the argument that the 'types' of surveillance technologies have changed. Panoptic surveillance is, as it is often understood, enabled through observations within certain physical architectonic settings bound by place and time. However, since contemporary surveillance technologies are more dynamic and network based, and because they operate very differently from the somewhat stable architectures that informed Foucault's concept of panopticism, the relevance of the concept itself is being scrutinised. As Martin, Van Brakel and Bernhard (2009) summarise, '[t]he main questions that have been raised pertain to whether the architecture of control has been superseded, whether the mechanisms of control have changed and whether the direction of the gaze has shifted elsewhere' (215).

Attempts to revise Foucauldian thought and calls for new frameworks are not new. Already in 1992, Gilles Deleuze wrote his *Postscript on the Societies of Control,* in which he argued that disciplinary societies were, at least partly, superseded by societies of 'control'. Society in the nineties had entered a new phase of global capitalism, which required a new conceptual framework. Foucault's disciplinary techniques were reformative and took place in institutions factories, hospitals and schools; whereas societies of control are embedded in new apparatuses such as computers, new organisations, such as corporations and markets, and new control mechanisms: codes that can include and exclude. In Deleuze, the axes of Foucault's biopower, the individual transforms into 'dividual' (consisting of even more smaller units) and the masses (or the population) into samples and banks (1992, 5). Foucault's analogical spaces become coded figures. In short, Deleuze's short reworking of Foucault sketches the wake of an informational regime in which one is free to move, but one's numerical body always tracked and perpetually modulated.

Within the field of surveillance studies, other work by Deleuze has been incorporated as well. Two of the most outspoken critics of the dominance of Foucauldian frameworks, Haggerty and Ericson (2000), argued that the concept of the 'assemblage' would do more justice to contemporary forms of surveillance. According to Deleuze and Guattari (2009), there are no distinct machines, only 'types of interpenetrating multiplicities' that can form an assemblage (41). This assemblage can never be reduced to its elements because they do not have a fixed meaning; they are mediated by the interrelations that together shape the assemblage. It is also due to these interactional effects that the assemblage gains agency on its own (Schuilenberg 2009, 206). For example, individual statements should not be understood in their singularity, but as part of the assemblage and operating on its behalf; the assemblage defines the conditions of possibility of language (Deleuze and Guattari 2009, 94). Haggerty and Ericson state that the notion of the assemblage is better suited to analyse the complex and heterogeneous network processes through which contemporary surveillance operates: 'Surveillance technologies do not monitor people qua individuals, but instead operate through processes of disassembling and reassembling. People are broken down into series of discrete informational flows which are stabilized and captured according to pre-established classificatory criteria' (Haggerty and Ericson 2006, 4). Thus, instead of focusing on how architectures of control constitute individuals, which is the way Foucauldian frameworks would put it, the attention shifts to understanding how complex assemblages shape streams of data.

Haggerty and Ericson continue describing what happens to the disassembled persons. They become reconstituted in digital form in places comparable to what Latour has termed 'centers of calculation' (Haggerty and Ericson 2000, 613). Centres of calculation are places such as laboratories in which knowledge is accumulated, handled and disseminated (Latour 1987). What Haggerty and Ericson mean by the term are those places of intersection in which (digital) data are reassembled and being made sense of, for example, the various corporate databases, statistical institutions, or police institutions (Haggerty and Ericson 2000, 613). As they explain: 'They are then transported to centralised locations to be reassembled and combined for institutional agendas. Cumulatively, such information constitutes our "data double", our virtual/informational profiles that circulate in various computers and contexts of practical application' (ibid.). These data doubles can be 'scrutinized' and 'targeted for intervention' (Haggerty and Ericson 2000, 606).

By now, the work Haggerty and Ericson have many followers that press for a new conceptual repertoire. In a critical discussion of this alleged paradigm shift, Caluya (2010) makes a few critical remarks about the enthusiasm with which contemporary surveillance scholars radically break with Foucault. He remarks that 'the very mention of the term in conferences immediately leads scholars to roll their eyes in boredom' (ibid. 621), but that through this hasty dismissal some subtleties of Foucault's thought might be overlooked (623). He means that those scholars have a (inappropriate) unidirectional reading of Foucault's understanding of the panopticon and neglect how panoptic techniques are situated within a whole series of arrangements of techniques and power relations. Thereby they disregard the place of the panopticon within Foucault's broader theory of microphysics of power. Also, the move to the assemblage should not be seen as a new paradigm forced upon us by the development of new technologies, but as a mode of thinking already deployed by Foucault.[11] Aware of such criticisms, Haggerty (2006) himself admits that Foucault's work is very multi-layered, but he fears nonetheless that surveillance studies will become a sort of 'Foucault studies' if one engages too much in discussions of how Foucault should be understood and what he could have meant. He persists that it is time to 'cut off the head of the king' (ibid., 27) and that scholars should stop to read panoptic attributes 'into' surveillance practices and instead take more seriously the questions that new technologies raise themselves (ibid., 32).

This argument has had its impact: Leading surveillance scholar David Lyon's *Theorizing Surveillance: The Panopticon and Beyond* (2006) can be taken as a sign for a growing consensus on the limits of Foucault (Caluya 2010, 622). According to the editors of the *The Surveillance Studies Reader* the work by Haggerty and Ericson has been 'one of the most promising developments in surveillance theory over the last decade' (Hier and Greenberg 2009, 74), and it has stimulated many

[11] Caluya bases his critique on the way Deleuze and Guattari describe Foucault's understanding of assemblages and on Foucault's own analyses in his later lectures on security. In fact, in these lectures Foucault describes apparatuses of security as anticipatory through the calculation of risk and as operating through the circulation of bodies and goods. A similar argument is made in a lecture by Marc Poster (2008, March 1) when he notes that although Foucault refrains from mentioning computer related network technologies, his discourse is very much network oriented.

scholars to engage in a conceptual framework in terms of assemblages. However, despite the claim that this new assemblage-oriented paradigm would better suit contemporary technologies, it is, similar to the Panopticon, both conceptually powerful as well as contested. Indeed, critics have argued that although - or maybe because - the surveillant assemblage is a powerful concept, it remains rather abstract and obscure (Murakami Wood 2007, 256; Prainsack and Toom 2010). Prainsack and Toom, who work on the topic of DNA databases, state that the majority of the surveillance literature fails in 'locating agency' by which they mean 'to spell out who and what exactly engages in surveillance systems—both in terms of "running" surveillance tools or systems, and in terms of being surveilled—in what form, and in what setting exactly' (2010, 1119). According to these authors, the very definition of the surveillant assemblage as an agent itself leads away from an understanding of specific surveillance practices:

> inherent in Haggerty and Ericson's (2000: 606) definition that the '[surveillant] assemblage operates by abstracting human bodies from their territorial settings and separating them into a series of discrete flows' is the ascription of agency to the theoretical concept itself. (ibid.)

So where Foucault reformulated the concept of power by describing how panoptic techniques conditioned the human subject, his followers and criticasters reworked his concept of surveillance as power/knowledge into surveillant assemblages after the introduction of new media technologies.

This thesis holds with that tradition in that it takes into consideration the possibility that different technologies require different conceptual repertoires, whilst realising that this is not necessarily a full rupture with Foucault.[12] Although I sympathise with Haggerty and Ericson's move towards assemblage theory, I agree with Prainsack and Toom that the concept risks being used as merely a descriptor of unspecific and dispersed processes. Taking into account the 'epistemological warnings' given by the editors of the *Handbook of Surveillance Studies* (Ball, Haggerty and Lyon 2012, 9) I argue that there is a risk in analysing all contemporary surveillance processes as a surveillant assemblage. If we do this we risk black-boxing complexity behind a beautiful concept. Moreover, this could pose a similar problem to the study of sousveillance, or, to rephrase that phenomenon in current vocabulary of assemblage theory, the study of 'sousveillance assemblages' (Bakir, 2010, 165). This is problematic because the moments at which surveillance is tackled are exactly the moments that show us more about how surveillance works.

[12] I side with Caluya here.

It needs to be said that assemblage-inspired theory does not need to be unspecific. If the nodes of power of the surveillant assemblage are those 'centers of calculation' (Haggerty and Ericson 2000) in which data are reassembled, focusing on such places and activities is one way to concretise the study of surveillant assemblages. And sousveillance assemblages, as my case studies will show, have centres of calculation too, although we might want to call them differently, since we are not dealing with scientific laboratories or big data centres but with working spaces ('hack labs') and approaches (or 'hack-based science' (McQuillan 2013)) in the niches of network cultures.[13] The question of how to look at and provide accurate descriptions of these activities is discussed in chapter two. Before presenting my approach, I want to discuss a final evaluation of the notion of sousveillance in order to clarify how my work diverges from existing scholarly practices.

1.5 How to approach the exposure of surveillance?

Surveillance studies uses the term 'sousveillance' to talk about interventions that put surveillance under public display, and it is, in the end, the 'inversion' of the panoptic gaze that remains central to the argument (Mann and Ferenbok 2013, 29). But when I say that activists put surveillance under public scrutiny I am also interested in what 'making public' entails, firstly in terms of the way and the methods by which this is done (as argued in section 1.3), but secondly also in terms of its subject matter: what happens to the material when it 'goes public'? In other words, whereas for sousveillance 'exposing surveillance' is about an *inversion* of (panoptic) power relations, a focus on making public is about a *translation* of surveillance through particular methods and approaches. Therefore, I propose to do more than just add the study of knowledge production to sousveillance theory and make the study of sousveillant assemblages more concrete. These are useful and needed additions, but I also argue that when surveillance is 'made public' we need an analysis of what 'making public' means.

If we follow media critics and hacker anthropologists in the

[13] Moreover, Latour reserves that term for centres conducting concrete (mathematical) 'calculations' versus other centres or nodes of making visible, which he terms 'oligoptica' (Latour 2005b, 181). That term refers to smaller modes of seeing and making things seen: 'From oligoptica, sturdy but extremely narrow views of the (connected) whole are made possible – as long as connections hold' (ibid.). However, also the word oligoptica does not translate well to the people I study, while devices for making things public does (see also § 2.3.2). Besides, this notion of oligoptica, just as the notion of sousveillance, connotes too a metaphor of vision, which has already dominated surveillance theory too much.

argument that technical practices should resonate in the concepts that we use (Coleman 2011; Kelty 2008; Lovink and Rossiter 2011), this has a number of consequences for sousveillance. We need to rethink, for example, the fact that the 'camera', which has always been key to explaining sousveillance, is no longer the central instrument. Surveillance changes (as discussed in §1.4), and therefore also the 'working material' of sousveillance practitioners changes, as it now appears in the form of datasets and smart devices. Scholars have pointed out that surveillance is a popular target in hacker cultures (Coleman 2009; Kelty 2008) and that the latter are breeding spaces for experimental methods and approaches (Lovink and Rossiter). It is important to take a closer look at those knowledge practices and 'working sites', and subsequently think about how they can inform our conceptual framework.

In order to do this, I draw inspiration from Science and Technology Studies, and in particular from Actor Network Theory. This approach can help us understand how 'things being made public' feed into to 'how the public is made'.