Surveillance as public matter

Revisiting sousveillance through devices and leaks

van der Velden, L.C.

Publication date
2018

Document Version
Other version

License
Other

7 Conclusion

The materiality of surveillance made public

7.1 Back to the research question and approach

In this study, I moved from explaining the role of socio-technical devices in 'making surveillance public', towards my own research into surveillance. The main thing this dissertation shows, is that when technologies of surveillance are problematized, they become, as it were, 'datafied' in a particular way and reshaped into publically accessible (research) material. In other words, surveillance is turned into 'public matter'. In this concluding chapter, I retrace the trajectory of my argument and I discuss its implications. I start by explaining how I operationalised the central concern of the dissertation. I then summarise the main insights of the previous chapters and I explain how they contribute to Surveillance Studies and ANT's focus on material publics. Next, I discuss how the thesis opens a further research agenda for studies into the materiality of surveillance publics. Lastly I reflect upon the practical implications of this study.

On the most general level, this dissertation discusses interventions through which surveillance is 'made public'. Public interest for this topic is related to a number of recent high-profile public disclosures of surveillance practices. Mechanisms of surveillance might become visible, but they are, however, often not well understood. As scholars before me have argued, concepts of surveillance have difficulties keeping up with rapidly developing technologpical developments (Haggerty and Ericson 2000). Famously, the 2013 NSA revelations by Edward Snowden put internet surveillance on the map for a broad audience. The NSA affair was world news, and still today, it is the large, more spectacular 'leaks' that determine the image people have of surveillance. However, as I state in the introduction to this thesis, there are many more, less high profile, projects endeavouring to bring instances of data monitoring to the fore. These projects use many methods, technologies and strategies that render the workings of surveillance visible. These projects provide innovative and productive

ways of understanding surveillance. Since surveillance consists of technical and often obscure processes, this 'rendering visible' inevitably requires a form of translation. By focussing on these translation processes, I have provided a range of answers to the main research question: How is surveillance made public?

Central to the dissertation are projects that render (digital) surveillance visible and knowable. As highlighted in chapter one (§1.2), surveillance scholars have asked why 'the public' is largely mute concerning issues of surveillance (Ball, Haggerty and Lyon 2012, 4). They wonder whether the public understands the problem sufficiently. In contrast, I argue that we should pay explicit attention to those projects (Marres 2012a, 28), however small, that attempt to make the subject matter of surveillance into a 'public matter' (Latour 2005a, 14) in order to provide insight in the many ways in which surveillance can be understood. These smaller publics are not always vocal and opinionated, sometimes they use technological practices to make their point, or they mobilise technologically to form communities. In order to better grasp the contributions of these publics, we need to include technical and material ways of addressing (surveillance) problems in our analysis.

To this end, the dissertation discusses four projects that make surveillance public. The first is InformaCam, an app which makes mobile phone users aware of the circulation of (meta)data when they upload images to the web. The second case study deals with a set of leaks about surveillance that were published by WikiLeaks. The third case study focuses on Ghostery, an online browser plugin which makes online trackers visible and researchable. The fourth case study delves into the publication of the NSA files. Whereas InformaCam and Ghostery can be seen as 'detection devices' that signal moments in which internet users are or can be tracked, the publications by WikiLeaks and the NSA disclosures are 'leaks' that have produced file-based online repositories of surveillance material.

In the area of 'surveillance studies', these kinds of projects belong to the type of practices categorised as 'sousveillance' (Mann 2004), which refers to 'surveillance from below'. 'Sousveillance' conducts surveillance, but inversely: targeting authorities and often exposing surveillance practices and/or infrastructures themselves. It would seem that sousveillance is ideally suited to provide conceptual analysis of my cases studies. However, my claim is that the literature on sousveillance leaves some important dimensions unexplored. The notion of sousveillance assumes that the mere making visible of surveillance practices will result in a change in power relations. By focussing on visibility, sousveillance analyses tend to focus on only one dimension of what these interventions establish. It generally passes over the insight

of surveillance scholars that part of the power of surveillance resides in making things visible in a *stable* way, through, for instance, knowledge infrastructures and databases (Simon 2005, 12). In short, the study of sousveillance would benefit from a different approach and a different conceptual vocabulary that also pays attention to the 'back end' stories of sousveillance projects: How exactly do they make surveillance visible? What are their methods? And what can be learned from these projects? What are long-term strategies, implications and effects?

The alternative approach I develop is informed by 'Actor-Network Theory' (ANT), also known as a 'sociology of translations' (Callon 2004; Latour 1983; Law 1992; Marres 2005). Specifically, I employ the ANT-inspired concept of the 'social-technical device' (see §2.3.2). This refers to how human and non-human elements interact and make specific forms of action possible (Callon and Muniesa 2005). The socio-technical device establishes specific forms of translations. It guides me in focusing on the instruments through which surveillance is brought into view, the transformations that take place along the trajectory of making surveillance visible, and the importance of the different settings in which this happens. I follow the suggestion by Latour to stay close to the language of the actors and Mol's perspective on ANT as an adaptable repository: terms should be sensitive to the practices at stake (see §2.3.1).

Since my interest is in a 'public' translation, my approach is especially influenced by literature about devices that 'make things public' (Latour and Weibel 2005; Marres 2012a). Following ideas about 'material publics' (Marres 2012a; Marres and Lezaun 2011) I am specifically interested in how devices participate in and mediate the emergence of specific public forms (Marres 2012a, 9) (see §2.3.3). The concepts that I build on in the case studies highlight specific material dimensions of these public interventions. Specifically, these are the concepts of 'forensics' (Weizman et al. 2010) and 'material witnessing' (Schuppli forthcoming), 'transparency devices' (Barry 2010; Ruppert 2015), 'data publics' (Ruppert 2015) and 'material participation' (Marres 2012b). These are all variations of concepts that express how material practices and the public are interrelated. I use a variety of concepts, instead of one dedicated concept, in order to maximally emphasise the specificity of each case. For example: inserting metadata into a trajectory of 'proof' is the most significant move that InformaCam aims to make; hence I use the notion of forensics. WikiLeaks puts forward simultaneously transparency as well as analytic promises of the publication of datasets; hence, I depart from the vocabulary of transparency devices and data publics. Ghostery is a tool for empowerment and participation plus it has participated as a research device in my own research project; hence, 'material participation'. I

use the cases as 'lessons' to attune my vocabulary (Mol 2010, 257) by suggesting additions and rephrasing terms when the case requires so, such as 'forensic device' (InformaCam), 'radical expertise' (WikiLeaks), and 'issue device' (Ghostery). In the last case study (NSA disclosures), I mobilise the notions of 'leakage' and 'insertion' to signal the materiality of surveillance networks and how that could inform our thinking about surveillance and publics in the context of surveillance.

In summary, I look at sousveillance interventions as problematizations in which surveillance is brought to the fore through particular and contextually embedded translations. I tackle the question of 'how surveillance is made public' by combining an empirical inquiry on how surveillance is traced, made visible and understandable with a conceptual search for new, practically situated, vocabularies to address surveillance practices and countermeasures.

Each case helps me to work out a specific theme. By 'following the circulation of particular objects, technologies and formats of participation among different settings and practices' (Marres 2012a, XV) the cases provide the following insights: the InformaCam project shows that surveillance is 'hacked' and turned into publically available working material (especially relevant for human rights activists), WikiLeaks shows that the analysis of leaked data requires a radical expertise (which results in questions about sharing those skills), Ghostery shows that making surveillance public results in 'issuefied' data repositories, and the NSA files show that surveillance devices in the public require new notions to address the materiality of surveillance networks (and ways of dealing with them). These themes have led me to conclude that sousveillance turns surveillance into 'public matter': meaning publically relevant research material, tied to particular issues. Making surveillance public and thereby opening it up as 'working material' for the public resonates with how critical internet cultures often treat online material. In a variety of manners, critical internet cultures present material and subsequently allow and invite the public to modify it, participate in it or engage with it for various ends. In the following sections, this point is discussed in more detail.

7.2 From sousveillance to surveillance as public matter

The main conclusion of the thesis can be broken down in the following statements and contributions to the study of surveillance: (1) Sousveillance practices do not only entail practices of visibility only, but they also present a research dimension through which surveillance is turned into data. Surveillance is 'datafied' and can be analysed. This is important for sousveillance studies because it could

help us to understand and potentially improve relevance and success of sousveillance practices; (2) There is diversity of working styles through which surveillance data are produced and disclosed. This means that the way we get to understand surveillance should be understood as depending on the specific issue-spaces and modes of working in which the projects operate; (3) Sousveillance practitioners produce surveillance as 'public matter' in a dual sense. Surveillance as public matter should express the empirical insight that surveillance is turned into 'publically relevant' research material. This notion of public matter as public material situates material action explicitly in the context of the creative dynamics of critical internet culture: making things public does not just mean making things 'knowable', it also allows for the creation of new things. But this might also mean that transformations are bound to those that define this as matter of concern.

In what follows, I elaborate more on these three points and discuss how they contribute to existing literature.

7.2.1 Datafying surveillance

The dissertation takes a device-centred approach with a focus on knowledge production. This has allowed me, first of all, to show that the various surveillance awareness projects have research dimensions. This is illustrated most clearly in the chapters on Informacam, Ghosterty and Wikileaks (chapters three, four and five).[81] In all instances, rendering surveillance practices visible is never a process of simply uncovering surveillance, or rendering it 'transparent' as we commonly understand the term. Surveillance is made public through the deployment of devices that also add data to the phenomenon that they target. InformaCam does so through the help of libraries of metadata structures, by 'ingraining' categories into the metadata' (personal communication with Holmes, 2013). WikiLeaks does it through cleaning data, adding categories, indexes and facilitating connections between different datasets, by 'adding value to datasets' (Harrisson 2015, 157). Ghostery builds libraries of trackers, measures and ranks them through a periodic table (see 'Ghostery's tracker ranking visualisation', figure 4 in chapter five). In other words, the projects produce a datafication of surveillance: 'making surveillance public' entails processes of data enrichment in which surveillance is contextualised and re-appropriated.

By stressing the research dimension, I aim, in the first instance,

81 I do not discuss chapter six yet because it reflects primarily upon the public presence of surveillance technologies and how that impacts surveillance theory.

to contribute to surveillance studies, and especially to the study of 'sousveillance': grassroots forms of 'surveillance from below'. As described in the first chapter (§1.3), sousveillance analyses generally frame sousveillance as a form of 'reflectionism' (Mann 2004), raising awareness through instances of turning surveillance back on the ones that are usually in charge of the power to see. This notion of power is understood as an 'inversed panopticism', referring to a particular visibility technique that is most famously deployed by the architectural model of the panopticon which was theorised in the late seventies by Michel Foucault (1991). However, on a theoretical level, many sousveillance analyses do not address the point that power, in panoptic theory, stemmed from a combination of the visibility of the human subject with the inclusion of the human population in a number of registers (Simon 2005). Therefore, sousveillance analyses should also inquire into the registers or databases of sousveillance. This is what I add to existing sousveillance studies: by looking at the 'production side' of sousveillance I show that sousveillance practitioners do something comparable to the knowledge production side of surveillance.

As I also explained in the first chapter (§1.4), panoptic theory is regarded as out-dated. It is unable to accommodate the networked behaviour of contemporary digital technologies. If we update our vocabulary to the more contemporary notion of 'surveillant assemblage' (Haggerty and Ericson 2000), which, according to many surveillance scholars is more useful to address the distributed behaviour of surveillance networks, the focus changes. Haggerty and Ericson made the notion of 'centres of calculation' relevant for surveillance assemblage theory. The 'centre of calculation' is a Latourian concept (as quoted in Haggerty and Ericson 2000, 613; see also §2.1), which they use to refer to the places or institutions where data are being reassembled and analysed. These centres of calculations have become the new nodes of power in times when surveillance practices become distributed (Haggerty and Ericson 2000, 613). So, phrased in the vocabulary of 'surveillant assemblages' we can say that my case studies show that *sousveillant assemblages* have 'centres of calculation' too. Looking at these centres of calculation gives further insights into how sousveillance consists of more than interventions on the level of visibility.

By using the notion of the device (a derivation of assemblage) as an analytic guidance into a study of translations, this thesis shows how sousveillance practitioners are building databases and designing methods to allow a more stable form of knowledge production. Sousveillance practitioners produce data and use instruments and experiments for keeping their knowledge about surveillance stable in order to produce more than a single isolated intervention of 'watching back'. Paying attention to this 'research' side of sousveillance enriches

sousveillance studies because it can say more about how such projects have an impact beyond singular exposures. InformaCam serves as a good illustration: by accommodating legal requirements in advance of data collection it attempts to become prefigurative of future truth claims. The developers also aim for 'demonstration projects' in order to have their proposed formats circulate to wider (legal) audiences. As the history of science has shown, making experiments replicable is a known technique for making a device work (Shaping and Schaffer 1985; Barry 1999). Looking at these activities could therefore show how sousveillance projects attempt to 'set the standards' (Lovink and Rossiter 2011) and can become (as InformaCam calls for) juridically relevant.

Device-centred approaches also stress the question in what way devices matter for the way issues are articulated (Marres 2012a). To address this question, I show how, in the case of Ghostery, surveillance 'as a problem' is understood through this particular device. Ghostery is pushing online tracking to the realm of ethical consumerism. Its vision can be summarised in a two statements: tracking is something we have to live with and it is a condition for contemporary digital life that possibly can be 'bettered'. Ghostery's analysis and evaluation of tracking do not go beyond that: it does not imagine a world in which tracking can be banned. Let's take another example by looking at my discussion of the other device InformaCam. In this case, the technical affordances of devices turn out to matter not only for what constitutes surveillance. They also matter for what constitutes *sousveillance.* InformaCam serves as the most obvious example of how a device can change the playing field for sousveillance actors because of its technical affordances: it makes space for proof to emerge. Since cameras have become tracking devices, this changes the whole playing field for both surveillance and sousveillance. InformaCam does away with the 'gaze' as a primary locus of power, and transforms the question of power into an 'art of looking', into a skill of determining 'which data counts'. In other words, sousveillance practitioners need to become skilful data curators.

However, it is equally important to realise that this change in mode of operating is made possible due to a combination of things: the phone as a tracking device, the app that makes intentional data collection possible, and the composition of libraries and databases, which in turn make it possible to bridge to other fields such as the domain of law. The first three case studies all show that knowledge infrastructures or 'libraries' on the back end play an important role. WikiLeaks even calls itself a library at this point (WikiLeaks 2016). In short, the way these devices articulate and shape the issue of surveillance is inherently tied to the construction of knowledge infrastructures.

7.2.2 The production of surveillance data

The case studies show that the approaches of disclosing surveillance are very diverse and differently situated. There are many processes of data enrichment that use a variety of styles.[82] This makes sense since the working environment for a human rights focused organisation such as InformaCam differs from the intelligence-driven context with which Wikileaks interacts, which in turn differs from a company such as Ghostery that operates in a setting defined by consumerism. They operate in their own specific issue space with different targets, adversaries, alliances and they articulate different hopes (with respect to the data they produce). This results in different ways of handling data.

The InformaCam group operates in a human rights setting informed by free software culture. They combine modes of working and knowing from both milieus. They do interventions with sensory metadata by linking them to the legal domain through legal formats and they incorporate human rights ethics in their design. They also want to mobilise formats from the free software sphere, such as licences for tagging human rights data. They have, as it were, 'hacked' the surveillance risks and endeavour to open the data up for everyone who has access to digital equipment. By doing so, they have invented something new: a method of (sensory) forensics. Their approach merges a free software hacker's approach with human rights thinking. As a result, the InformaCam project 'moulds metadata' according to their relevance to operations of proof and ethics.

WikiLeaks' working field is (mass) state intelligence. It combines styles of hacking, journalism and counter-intelligence. The content of the datasets requires contextual knowledge and an awareness of secrecy. Whereas an intuitive way of approaching datasets would be reading data that are present, WikiLeaks' instructions tell you to be aware of the data that are not present (such as implicit knowledge and hidden knowledge). Instead of presenting simple and clear transparency, Wikileaks' instructions for searching its data stimulate its public to think 'via the secret'.

Conversely, for Ghostery, web tracking is part and parcel of consumer culture. Ghostery categorises the trackers on the basis of their tracking behaviour and uses computational methods to assess how often trackers are encountered. Following the logic of tracking companies, Ghostery adds ranking analytics to the material. It views trackers as elements that can be mined. It labels online trackers, mapping them

82 The fact that the thesis shows diversity in styles is maybe not surprising: it is often simply part of doing case study research and STS-work tends to highlight diversity as an argument against technological determinism (Beaulieu, Scharnhorst and Wouters 2007, 675).

according to concerns of ethical consumerism. The way Ghostery approaches trackers corresponds to how the project understands trackers as positioned in the world, and what should be done about it. Trackers become materialised like elements in the environment: protect yourself or improve them through ethical regulations and standards.

In tackling surveillance, these projects produce issuefied data, which means that surveillance is taken up in diverse configurations of understanding. A feel for these different configurations could contribute to studies into the different forms of 'computational objectivity' (Gates 2013, 252) in sousveillance practices. Brucato (2015) touches upon this issue when writing about the 'production of transparency'. What my case studies add to this emerging research orientation is the insight that developers engaged with sousveillance can be very self-reflective about their own forms of truth production. Some participants in sousveillance are well versed in theories of knowledge production themselves and re-insert those theories in their projects. As discussed in the chapter on InformaCam, developers reflect upon how they 'ingrain' categories into the metadata. In the chapter about WikiLeaks, I discussed that some WikiLeaks spokespersons have written about how they 'add value' to datasets. Studies into computational objectivity of sousveillance should, therefore, take into account developers' self-reflexivity in truth construction processes.

7.2.3 Surveillance as public matter

In the previous sections I outlined how surveillance data are produced in a diversity of ways and how surveillance data are made available online for public use. Surveillance awareness projects not only make the 'issue' of surveillance public, but they also make the 'material' public, and in doing so they enable practices of significant public relevance. Let me list the dimensions of public relevance per chapter. InformaCam transforms metadata tracking using public tools in the service of human rights. WikiLeaks curates surveillance databases and has pioneered methods for radical data literacy, which could enable people to develop new skills to form an understanding of, interact with and draw conclusions from secret knowledge. Ghostery produces online research material for anyone interested in studying the tracking landscape. The NSA disclosures are widely acknowledged to be of utmost public relevance. Besides the legislative repercussions of the disclosures (which is not the focus of this thesis), they have shaken the foundations of existing public and academic knowledge of surveillance. The case 'Leaky apps and data shots' about the NSA files has not yet been discussed in detail in this conclusion. The narrative I have told focuses less on the

methods by which the files have made surveillance public, and more on outlining the consequences of making public a range of surveillance techniques. The NSA files inform our conception about surveillance and stimulate us to rethink the way critical and collective practices can take shape in the context of surveillance. Whereas the 'detection devices' transform data monitoring technologies into online available tools for forensics and research, the leaks become input for radical literacy, and by being turned into a public repository, surveillance material challenges surveillance theory and opens up new research trajectories.

As the previous section outlined, the registers by which surveillance data are shaped and analysed are formatted by devices and are issue-specific. Data are treated in different ways, depending on the working environment in which they are taken up. Therefore, surveillance becomes a 'public matter' in two senses: referring (a) to material that can be used for public ends; and (b) to the way the material is shaped in a specific way, depending on its working habits and issue space.

In other words, surveillance is made tangible, something that people can act upon, and this transformation is bound to the devices that constitute modes of witnessing and to the issue formats of implicated actors. The notion of surveillance as 'public matter' that I develop in this dissertation incorporates a concern for the materiality of hacker practices (Coleman 2011; Kelty 2008; Lovink and Rossiter 2011) with a more ANT inspired material publics research agenda (Marres and Lezaun 2011). Specifically, studies into hacker and critical internet culture have stressed particular values as reference points (such as freedom of information, open infrastructures, and particular modes of working (see §1.1.2). What I want to stress here is a dimension involved in the process of making things public that resonates with what 'public things' often become in critical internet cultures: public code that can be changed. People provide public code, and invite users to adapt, appropriate and further develop it. As I show, surveillance undergoes a similar transformation: surveillance is transformed into working material belonging to the public.[83]

Authors writing about artistic interventions with invisible infrastructures have argued that making things visible is not so much about the elements suddenly to be seen and known (in other words: 'transparency's promise'), but it might even more about giving people the possibility to develop new relationships to the issues that these

83 See also initiatives on the intersection of art, research and journalism that call for 'commoning secret knowledge' in the context of the Snowden files. ("Signals: Exhibition of the Snowden Files in Art, Media and Archives" 2017).

elements connect to (Mattern 2013). As discussed by Marres (2012a, 30) informational participation and material action are closely intertwined. This means that informational activism does not need to lead to questions about informational citizenship only. Along similar lines, making surveillance public allows for the production of public material that people can use for inventive practices, and possibly the formation of 'tactical' publics. Hence, when surveillance is made public, the public status of the material opens up again new questions and concerns and around these, new publics can emerge.

In contrast with ANT-informed studies that trace issue publics and material publics as configurations of democratic participation and/or institutional deficits (Latour 2005a, Marres 2005; Marres and Lezaun 2011; Marres 2012a), I have situated the act of making public within critical internet cultures in order to highlight another dimension of the material public. By following what happens to 'surveillance data' I have reflected upon what this situatedness in critical internet culture means for the material. Public material is a resource for re-appropriation. Making public is therefore also making public for future and collective use, and possibly for tactical use.

7.3 Future research agenda: surveillance publics

Alongside these three series of contributions to the academic study of surveillance and material publics, the dissertation reveals a field of study that warrants further research into surveillance publics. This can be dissected in a more theoretical and practical agenda. I discuss the theoretical agenda in this paragraph; the practical agenda is discussed in §7.4.

When taking the devices discussed in the chapters into account, a striking insight is that making things public and making things private can go together. To give a few examples: InformaCam produces two kinds of images: images without metadata which can be posted on the web, and images with contextual metadata which are only supposed to be shared (and stored) through encrypted channels and with trusted persons. Ghostery is a tool that 'makes trackers public', but at the same time it is a Privacy Enhancing Technology. WikiLeaks combines publication strategies with encryption. The communication about the NSA files took place through e-mail encryption. These interventions emerge from a socio-technical environment in which privacy, secrecy and intelligence practices co-determine how things are done (see §1.1.2). This indicates an interesting tension that could be investigated further. As I argued in chapter six about the NSA disclosures, we should reconceptualise publics in the context of surveillance, by rethinking

the role and impact of devices that are usually only seen as privacy-enhancing technologies for the individual. Instead, we could investigate how they also contribute in forming collectives or publics (as also proposed by Gehl 2014 and Lovink and Rasch 2013). How do these tools constitute sociality? To what extent is the use of encryption a 'public-enhancing technology'? In our analyses, we should include those technological responses to surveillance that we usually do not associate with forming publics in a classic sense. For instance, technologies of tracing: How do people trace and counter complicated interception technologies such as data injections? Can collaborative tracing also bind these investigators as a collective? What imaginaries arise out of the interactions with these technologies? This research trajectory could benefit from insights from studies on hacker, crypto or techno collectives (Coleman 2012; Kelty 2008; Lovink and Rossiter 2011; Maxigas 2014a; Milan 2013).

It is important to pay attention to the kinds of concepts and imaginaries of surveillance that are mobilised in specific assemblages., We should not only look for the famous, most-well known surveillance concepts but we should also pay attention to concepts that are specific and tied to very concrete technological practices. As I showed in my discussion of the NSA disclosures, a disjuncture exists between concepts of surveillance and the technologies that conduct surveillance. I suggested two alternative concepts, leakage and insertion, that cover particular modes by which data can be gathered. Leakage is an appropriate term when referring to technologies by which people share all sorts of data over unencrypted channels (for instance, by using 'leaky apps'). Insertion is useful for thinking about methods of intrusion by which networks or computers are actively approached (for instance, malware or mass scale 'data injections'). As I argued, it is important to link up more closely to malware research in collaboration with hackers and security researchers, in order to be able to develop a conceptual vocabulary that is even more informed by the technological features of surveillance methods and to understand the devices that they use.

Finally, it is important to think about the kind of expertise surveillance publics produce. In the chapter on the transparency devices of WikiLeaks I concluded that there is a certain tension in, and maybe challenge for, radical expertise. There is a radical dimension to the knowledge WikiLeaks produces: the huge data WikiLeaks releases in the public domain one is not supposed to see, and therefore making sense of this data requires special analytic skills and approaches. At the same time, Wikileaks expects data subjects to treat and read the data in a disciplined way. Therefore, there is an inherent tension in the way in which Wikileaks 'leaks' and 'reads' data. Although its form of leaking is radical, its way of reading is not: Reading orderly data used

to be associated with an enlightened and civil public that behaves well (Barry 2010, §26). The ordering of numbers and rationality is associated with a socially disciplined audience. But how do ordering devices produce these unruly publics, the uncontained publics (the publics more similar to controversial issue publics that point at fundamental problems)? And with what effects? When does radical expertise lead to radical data publics that take their own course? Since the completion of this research, numerous WikiLeaks-related controversies have highlighted that these are urgent and timely questions.[84] More research into examples of radical expertise, or maybe into the history of radical scientists and librarians, could help understanding potential alternative imaginaries about the promises of data in relation to order and disorder.

7.4 Material research agenda: Collaborative knowledge production

There is also a material dimension to the research agenda that arises out of this dissertation. Stressing that surveillance becomes public matter means emphasising the need for a discussion about the circulation and curation of these datasets. What are the practical implications of the presence of surveillance data as public material? What are the implications of having access to surveillance data?

First of all, Rather than seeing interventions with surveillance as only objects of study, and evaluating sousveillance as either a counterweight to surveillance (Mann 2013; Van 't Hof 2010) or failing to correct to the system (Monahan 2006), one can consider them as research projects that share, or could share if they want to, their knowledge, problems and material. I also stated that this enrichment is played out, not only on an empirical level but also on a conceptual level. Surveillance scholars that want to conceptualise contemporary surveillance need input from those that are able to detect and capture contemporary surveillance processes. In short, scholars could greatly benefit from collaboration.

In such collaborations, it is crucial to be aware of the diverse styles interaction with surveillance data. Issue devices bring surveillance into view according to a certain register of what is important to

84 Take for instance 'Pizzagate' refering to a specific conspiracy reading of the John Podesta e-mails, released by WikiLeaks in 2016, or the Clinton files, which played a big role in the public debate about the US elections in 2016. Both are not datasets about surveillance, and thus fall out of the scope of this thesis. However, they put on the table questions about thin lines between conspiracy and radical expertise, which both deal with secret/unauthorised knowledge.

observe, and they take part in particular alliances. Thus, when using the material we need to realise that the knowledge one produces is tied, to some extent, to this particular configuration. It is important to take this into account because there is also contestation about the configurations in which surveillance is made public. For instance, not everyone appreciates Ghostery's being in between a privacy-tool and a consultant for the advertising industry. It is important to reflect upon how this feeds back in the researcher's work, and to take a step back to see which other devices and actors can do certain jobs equally well, or better. Even more controversial is WikiLeaks' recent role in the 2016 elections in the United States. In short, when using surveillance awareness projects as research devices, a discussion about data ethics in relation to data politics should be addressed.

Moreover, next to being of instrumental value for the social sciences and humanities, there are also good public reasons to support surveillance awareness initiatives. As I started off with in the introduction, surveillance disclosures, such as the NSA affair, can force large publics to rethink surveillance 'as a problem'. However, three years after Snowden, it seems that this rethinking exercise has somewhat disappeared from the public eye again. Surveillance is still frequently framed as an effective counter-measure to terrorist threats. Surveillance awareness projects are continuing their difficult and, in these times, politically sensitive and frequently unappreciated task. These collectives often function on a voluntary or temporary basis and many have no sustainable ways of funding or infrastructure. What follows is that we need to think about how to support and maybe even develop such projects. During my conversations with security researchers and colleagues, this was a frequently mentioned concern. My dissertation further highlights the need not just for doing research about, but also a more sustained interaction with, coalitions for material publics that engage with monitoring practices. In these final paragraphs, I would like to briefly outline what some of the more practical implications of my analysis brings to this debate.

This dissertation joins the voices of those within and beyond academia who have reflected upon what needs to happen practically with surveillance 'as an issue' and the curation of (leaked) data about surveillance. In light of the public and academic need to bring expertise together in order to better understand surveillance, I support the calls for some sort of institutionalisation of knowledge and research practices concerning surveillance. For example, the Dutch news outlet De Correspondent suggested that the issue of surveillance is in need of an 'institution' analogous to what the IPCC is for climate change (Mommers and Martijn 2016). Others, such as the Berliner Gazette, have argued that libraries should be the sites for the curation of

surveillance data (regarding the NSA disclosures specifically), which would allow research for activists and archivists (Apitz 2015).

As I have outlined above, both the field and topic are dynamic. Therefore, I suggest that academic organisations could contribute conceptually and materially to such ideas by supporting and/or funding a project that combines the tasks of a 'classical' knowledge institute with those of a participatory, activist platform, focussing on surveillance. Such a project could provide an infrastructure at the intersection of technical (awareness and crypto) practices and surveillance studies, and disciplines with a related interest. It could bring together, and learn from, the various manuals, toolboxes and software that are produced by activists, (radical) experts and journalists that trace surveillance and it could translate this material into an educational program on (critical) data literacy. It should engage with on-going ethical discussions about leaked and open data. We need to think about how surveillance detection software can become accessible for those without programming skills. Participants would be able to bring together relevant research material that should be prioritised for investigative purposes. Furthermore, it would not only need to focus on successful initiatives, but could also analyse trajectories of failing: Why and under what circumstances does documentation make or not make a difference?

This dissertation raises important questions for such a project: How does data production become tied to evidentiary procedures? What kinds of skillsets are needed to conduct this kind of research and how can these skills be learned? This includes technical skillsets, but also insights into the histories of secret knowledge or data that we are not used to seeing or noticing. Finally, fine-tuning conceptual vocabularies to the material practices under study is key in order to be able to more effectively design interventions. In short, such a platform could bring together histories, practices and conceptual implications of data politics and formation of radical data publics. I hope this dissertation, and my work as an engaged researcher can contribute to constructing such lasting platforms for collaboration and digital politics.