Surveillance as public matter

Revisiting sousveillance through devices and leaks

van der Velden, L.C.

Publication date
2018

Document Version
Other version

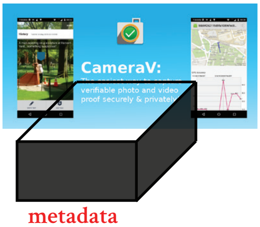
License
Other

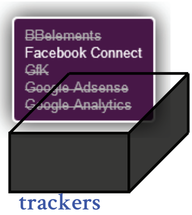
Link to publication

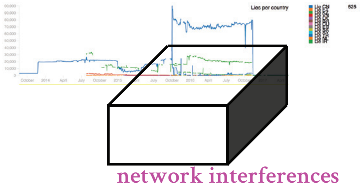
Citation for published version (APA):
van der Velden, L. C. (2018). *Surveillance as public matter: Revisiting sousveillance through devices and leaks*. [Thesis, fully internal, Universiteit van Amsterdam].

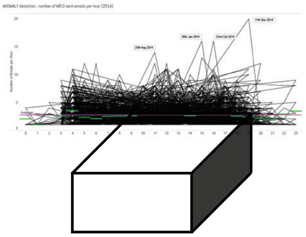
Surveillance as Public Matter

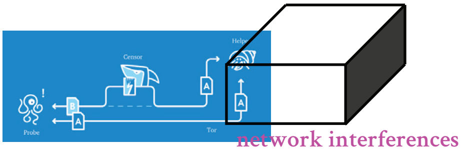
Revisiting surveillance through devices and leaks

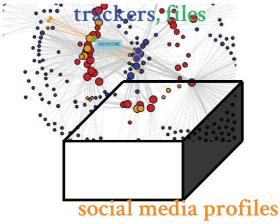






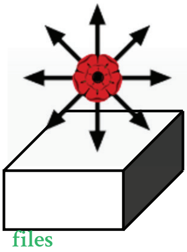

ANOMALY detection : number of MR.D sent emails per hour (2014)





Lonneke van der Velden

Cryptome 38 July-December 2015
Cryptome 37 January-June 2015
Cryptome 36 July-December 2014
Cryptome 35 January-June 2014
Cryptome 34 July-December 2013
Cryptome 33 January-June 2013
Cryptome 32 July-December 2012
Cryptome 31 January-June 2012
Cryptome 30 July-December 2011
Cryptome 29 January-June 2011
Cryptome 28 July-December 2010
Cryptome 27 January-June 2010
files



WikiLeaks
Vault 7: Archimedes
Today, May 5th 2017, WikiLeaks publishes Archimedes, a tool used by the CIA to attack a computer inside a Local Area Network
5 May 2017
files

Surveillance as public matter

Revisiting sousveillance through devices and leaks

ACADEMISCH PROEFSCHRIFT
ter verkrijging van de graad van doctor
aan de Universiteit van Amsterdam
op gezag van de Rector Magnificus
prof. dr. ir. K.I.J. Maex
ten overstaan van een door het College voor Promoties ingestelde
commissie, in het openbaar te verdedigen in de Agnietenkapel
op donderdag 8 februari 2018, te 10:00 uur

door

Lonneke Cathelijne van der Velden
geboren te Bukumbi, Tanzania

Promotiecommissie:

Promotor:	
Prof. dr. R.A. Rogers	Universiteit van Amsterdam
Overige leden:	
Prof. dr. B. Roessler	Universiteit van Amsterdam
Prof. dr. A.A. M'charek	Universiteit van Amsterdam
Prof. dr. H.O. Dijstelbloem	Universiteit van Amsterdam
Prof. dr. N. Helberger	Universiteit van Amsterdam
Prof. dr. S. Wyatt	Universiteit Maastricht
Dr. N.S. Marres	University of Warwick
Faculteit:	Faculteit der Geesteswetenschappen

Table of contents

Acknowledgements

Many persons helped shaping this thesis. First of all I would like to thank Richard Rogers for his supervision and for offering me such a lively research environment. I want to thank Noortje Marres for hosting me as a visiting fellow at CSISP at Goldsmiths College. The many workshops and discussions there have been inspirational and crucial for my thesis. Thomas Poell helped me tremendously on several occasions and especially with sharpening the conclusion of the thesis. I want to thank Geert Lovink for his expertise, the inspiring events at the INC, and his motivational comments when I had gotten stuck in one my chapters. Stefania Milan was a great motivator and reviewer during the final phases. A few people were always willing to help with technological or juridical questions; Matthijs Koot, Erik Borra, Emile den Tex, Rejo Zenger and Frederik Zuiderveen Borgesius.

There are also three collectives that I want to thank in particular. The Digital Methods (DMI) team has been supportive with feedback, especially Sabine Niederer and Liliana Bounegru who on multiple occasions were respondents to my papers presented during the DMI workshops, and Anne Helmond and Esther Weltevrede with whom I talked a lot about tracking research. The DATACTIVE team gave me great and critical comments. I also want to thank the digital rights organisation Bits of Freedom for being so knowledgeable and up to date with new developments. I am part of the board of Bits of Freedom and I have found it to be an enriching experience to be part of this organisation.

There is a whole list of people that provided me with ideas and input for writing, or with feedback to papers in the making. I might not have remembered everybody, but special thanks to Maxigas, Niels ten Oever, Susan Schuppli, Shela Sheikh, Tamira Combrink, Martin Boekhout, Frederike Kaltheuner, Becky Kazansky, Sam Gregory, Harlo Holmes, Natan Freitas, Heath Bunting, Birgitta Jonsdottir, Victor Toom, Francisca Grommé, Sacha van Geffen, Jurre van Bergen, Douwe Schmidt, and Marc Tuters.

Furthermore, chapter three, five, and six have appeared in respectively *Big Data & Society*, *NECSUS: European Journal for Media Studies*, and *Surveillance & Society*. I am grateful for the anonymous peer reviewers of these journals whose feedback has been incorporated in several of the chapters of this PhD.

The visualisation on the cover is designed by Carlo de Gaetano and Frederica Bardelli and is part of an ongoing collaborative project of visualising projects that tackle surveillance which will hopefully

have an online follow up. The boxes represent the different styles of tackling surveillance and the icons on the background are screenshots from various interventions that can be found online.[I] I want to thank Dolan Jones & Holly Harman for copy editing, and Wendy Springer for helping me with my messy reference system.

I would like to thank Femke Kaulingfreks for convincing me, years ago, to write about a new topic that I liked, which resulted in my PhD proposal. I greatly thank the Amsterdam School for Cultural Analysis for funding the PhD and for being such a welcoming research school.

Finally I want to thank my family and friends for their support. Ernst van den Hemel has been a great partner, supporter, and reviewer for almost every chapter in the PhD, and he helped me with final editorial comments. I want to thank my parents for being so supportive, my paranymphs Tamira Combrink and Mara Joustra for their organisational help and little Lu for keeping up the good spirit.

Amsterdam, January 2018

[I] The icons of the interventions on the front cover originate from (from left top to right bottom) CameraV, Ghostery, Chokepoint Project, Open Observatory of Network Interference, Share Lab, IC Watch, Cryptome, ProjectPM, WikiLeaks. Those on the back include Privacy Cafe (Netherlands), Cryptoparty (Chili; entodaspartes.org), TOR, OTR, PGP, Signal, Google Alarm, Ad Nauseam

List of figures

Figure 9. Companies operating third party elements in the Website Register of the Dutch Government.
Dorling Map, Digital Methods Initiative, August 2012.
Sources: Website Register Rijksoverheid; Ghostery; Tracker Tracker Tool.

The map shows which companies operate the most trackers in the Website Register. The nodes refer to third party elements (3pes) as indicated by Ghostery. The size indicates the 'share in 3pes' which companies have in the total amount of 856 3pes. The register contained 1110 websites in total. Elements that occurred less than five times are not listed in the legend.

Figure 10. Network of websites and trackers in the Website Register of the Dutch government.
Gephi visualisation, September 2012.
Sources: Website Register Rijksoverheid; Ghostery; Tracker Tracker Tool.

The map shows which websites use the same trackers. The coloured nodes are third party elements. The grey nodes are the domain names. The names of the websites are deleted for reasons of clarity, except for the cluster on the bottom in order to illustrate the purpose of the map. For instance, nuclearforensics.eu and forensicinstitute.nl are connected with WebTrends and Google Analytics.

List of tables

Introduction

Surveillance as a contemporary issue

In June 2013, former NSA contractor Edward Snowden disclosed details of NSA mass-surveillance programs sparking widespread public outrage. Snowden released a series of classified documents that reported on global surveillance programs developed by the NSA (and other state agencies such as the British GCHQ), which familiarised the public with a range of sophisticated interception technologies and systems for data monitoring. The most striking example given by Snowden was the ‘PRISM-program’ through which the NSA was able to tap into the servers of the largest internet corporations.[1] The leaks explicated how common, everyday consumer technologies such as apps, plugins and regular security updates serve as sources for data harvesting and analysis for the NSA. Privacy and security became public concerns, rather than the reserve of lawyers and advocacy organisations. In the aftermath of the affair, journalists discussed what kinds of concepts would be suitable to describe this phenomenon (Berger 2014; PEN American Center 2014), and news outlets focussed on the available tools for enforcing online privacy (Dredge 2013; Wood 2014). The Chaos Computer Club, Europe’s largest association of hackers stated to be ‘speechless’ after the disclosures (30C3, 2013). Their yearly Chaos Communication Congress had no motto, indicating that even these experts thought that this phenomenon required a moment of reflection. The NSA affair, momentarily at least, stimulated people to reconsider internet surveillance and its implications for social life.

Surveillance is a complex phenomenon that is not easy to see or feel, yet, it is important. Surveillance scholars have been arguing for decades that surveillance is ‘the dominant organizing practice of late modernity’ (Ball, Haggerty and Lyon 2012, 1). According to them, developments in data handling have lead to changes ‘on a scale comparable to the changes brought by industrialization, globalization or the historical rise of urbanization’ (ibid.). At the same time they have pointed to the difficulty of tackling surveillance due to its ubiquity and normalization

[1] Microsoft, Yahoo, Google, Facebook, AOL, Skype, PalTalk, YouTube en Apple.

(ibid., 9). Because if surveillance is everywhere and normal, it becomes harder to grasp the problem.

Therefore, my central question in the dissertation is: How is surveillance made public? The NSA affair is one key example of how surveillance is being 'made public': these revelations made surveillance visible, politicised and a topic of fierce public debate. Edward Snowden is probably the most famous and infamous anti-surveillance activist and whistle-blower.[2] However, there are other examples of efforts through which surveillance is being made visible which operate in less public spheres. There is a broad plethora of technologies, tactics, and strategies employed by people concerned with surveillance that try to highlight these issues. Similar to awareness raising for environmental and medical issues, many projects raise awareness about surveillance: they bring data monitoring to the fore for individual internet users and larger publics. Some of these projects provide also countermeasures. Informational and tactical activism which deals with internet surveillance is my central concern. Therefore, in this PhD thesis the NSA disclosures form part of a larger story in which surveillance is rendered visible at different scales and by different methods.

This PhD thesis takes as its starting point changing practices of surveillance, and reflects upon the implications thereof for the dynamic field of Surveillance Studies. The interdisciplinary field of 'Surveillance Studies' looks at 'surveillance' as a shared research orientation. My point of departure is the aforementioned problem of 'tackling surveillance': Which particular tactics and knowledge practices are required in order to make the phenomenon of surveillance tangible and public? This study claims that in light of recent rapid developments and disclosures of practices of surveillance, an updated perspective on how things are made public is required.

This focus on 'making public' is borrowed from the exhibition and subsequent publication *Making Things Public: Atmospheres of Democracy* (Latour and Weibel 2005) and scholarly work in the field of Science & Technology Studies (STS) which followed. This line of scholarly work explores the 'material dimensions' of contemporary publics (Marres and Lezaun 2011; Marres 2012a; Ruppert 2015). The emphasis on material means that this strand of thinking pays particular attention to the active role of devices and material artefacts in shaping how publics and public problems are organised and articulated. I take this perspective from STS and bring it into conversation with the field of surveillance studies. I discuss several interventions that render surveillance visible in the public domain and pay extra attention to the

[2] The United States have charged him of violating the Espionage Act of 1917, but his intervention has been recognised by numerous awards and nominations (Wikipedia 2016).

devices that are deployed in these endeavours.

This conversation is productive because insights into the materiality of publics, especially those articulated in STS, are particularly useful to think about interventions regarding surveillance: since surveillance consists of technical and often secret processes, ‘rendering surveillance visible’ inevitably requires a form of translation. In this translation, devices can play a formative role. Mobilising notions of what can be considered ‘material publics’ for surveillance studies allows me to not only show some of the material dimensions of how surveillance is rendered ‘visible’, but also explain how surveillance is re-appropriated and repurposed. In the process of turning surveillance into a matter of concern, surveillance becomes ‘datafied’ itself. As a consequence, ‘surveillance data’ becomes a resource for public purposes. I use the term ‘public matter’ to describe the double effect of rendering visible and creating material to be used in new manners.

During my PhD research I have encountered both optimistic stories about the power and effects of anti- or counter-surveillance activism (Mann and Ferenbok 2013; Van ‘t Hof et al. 2012), and pessimistic conclusions that the overall effect of this form of activism in terms of system change is minimal (Monahan 2006). The impact of this kind of activism is not always easy to measure. These projects operate in a difficult context in which surveillance is being normalised, and legitimated as a counter against terrorism.[3] It is also not my aim to do an impact assessment on this form of activism. This study allows me to tell another story about interventions with surveillance which results in a different (potentially collaborative) position. Surveillance as public matter means acknowledging the contribution that these interventions make or could make to surveillance research itself.

The dissertation is structured as follows: Chapter one is dedicated to “Tackling internet surveillance”. The chapter starts with a few short examples of tackling surveillance on a practical level. I briefly introduce these interventions that expose surveillance in order to introduce my main research concerns. I will outline the environments in which these projects are developed by situating these projects as part of ‘critical internet cultures’ and ‘hacker cultures’ (Coleman 2013; Lovink 2002; McQuillan 2013). I subsequently discuss the field of Surveillance Studies, because it has tackled surveillance, including those who counter it, on a more conceptual level. The field of Surveillance Studies has surveillance as its core subject matter, and I discuss how my objects of study relate to its dominant concerns. Specifically, I will

[3] See for instance the interview with the Head of the Dutch intelligence agency Rob Bertholee in *De Volkskrant* who equates defending privacy with ‘permitting’ the potential happening of terrorist attacks (Modderkolk 2016).

highlight problems with the concept of 'sousveillance.' 'Sousveillance' is a term that captures the practice of 'surveillance from below' or indeed 'watching the watchers'. However, I argue that the use of the concept of sousveillance is limited, especially if one wants to study and theorise a particular dimension of sousveillance: the research activities and methods by its practitioners. Moreover, the notion of sousveillance is also ultimately related to the notion of panoptic power (Foucault 1977), and many within surveillance studies have called for conceptual revisions beyond the panopticon against the background of new information technologies (Caluya 2010; Deleuze 1992; Haggerty and Ericson 2000; Lyon 2006; Murakami Wood 2007; Simon 2005). I focus primarily on the argument that the notion of the 'assemblage' could be productive for surveillance studies (Haggerty and Ericson 2000; Lyon 2006). I extend this discussion by posing the question how assemblage theory would work out for the (activist) counterpart of surveillance – sousveillance – but I also argue that we need to specify the assemblage repertoire. That is, we need concepts to account for the various critical internet practices and methods that expose surveillance. The chapter concludes therefore with a proposal to revisit sousveillance in different terms, terms that can account for the processes behind 'making surveillance public'.

In chapter two, "Devices for making surveillance public", I build upon the challenges outlined in chapter one. Specifically, I propose to take inspiration from STS, and assemblage-oriented approaches in the form of Actor Network Theory (ANT), for the study of sousveillance. This is in line with a call for methodological diversification in surveillance studies in the past (Martin, Van Brakel and Bernhard 2009; Wood 2003; Murakami Wood 2007) and with an on-going movement of including ANT in surveillance studies (Ball 2002; Grommé 2015; Martin, Brakel and Bernhard 2009; Murakami Wood 2007; Timan 2013). I contribute to that movement by providing a detailed discussion of which particular version of ANT is productive for surveillance studies, considering my particular subject matter. I consider ANT as an approach that helps to make space for the vocabularies and ideas of actors under study in the framing of the analysis (Latour 2015) and as an adaptable repository of terms that allows for theoretical shifting (Mol 2010). Important for my work is the way ANT has put forward the notion of the 'device' and the way ANT approaches have produced descriptions of trajectories of 'making things public' (Latour and Weibel 2005). The notion of 'material publics' is especially crucial to the dissertation because it helps conceptualising the role of 'surveillance data' in the public. In other words, this dissertation presents an argument of how including ANT into surveillance studies can be made productive. The result is a different vocabulary and therefore a different way of working with sousveillance. I conclude chapter two by introducing my case studies, the issues around data collection they address, and how ANT feeds into that.

Chapter three, “A forensic device for activism: How activists use metadata tracking for the production of public proof”, is the first case study in which I implement this focus on devices and surveillance as public matter. This chapter is an inquiry into the ‘laboratory’ of sousveillance practitioners. InformaCam allows mobile phone users to manage metadata in images and videos. The circulation of image metadata can cause surveillance risks, but InformaCam helps human rights to capture and store the data for evidentiary purposes. In this chapter, I propose InformaCam should be interpreted more specifically as a ‘forensic device’. By using the conceptualisation of forensics as the art of public proof giving (Weizman et al. 2010) and work on devices of demonstration (Barry 1999; Callon 2004), I show how InformaCam, through a range of interventions, establishes a translation: it re-arranges metadata into a technology of evidence. It ‘hacks’ the problem of surveillance and turns it into working material for human rights activism.

Chapter four, “Transparency devices and leaked data: Sites for radical expertise?” presents a study on WikiLeaks. Whereas chapter three focused on the notion of the device, this chapter focuses on the notion of the public. WikiLeaks is the kind of organisation that in sousveillance theory serves as an example of ‘undersight’ (Van Buuren 2013). Others have said WikiLeaks carried a promise of ‘radical transparency’ (Birchall 2014; Heemsbergen 2014). This chapter provides a critical discussion of sousveillance methods, this time by focussing on the implications of leaked data. I discuss a range of ‘working practices’ relating to ‘dealing with surveillance data’ in the context of leaks. I build on the notion of the ‘data public’, implying that digital devices reconfigure the production of expertise and play a constitutive role in how a public is enacted (Ruppert 2015) and reflect upon the role of tools and data practices around Wikileaks. The argument that I develop is that WikiLeaks should be seen as an experiment in *radical expertise*. It is an experiment in unauthorised knowledge production that requires investigatory data subjects.

In Chapter five, “Turning a safety tool into a microscope: Tracking the trackers”, I show how a ‘sousveillance lab’ transforms surveillance into public material: it enables researchers to study online tracking. The browser plugin Ghostery detects online trackers and makes them visible. But it does more than give people a warning: it is also analysing the trackers. Building upon work of the Digital Methods Initiative (DMI), which specialises in repurposing web devices for research (Rogers 2009b), I use a tool that is built on top of

Ghostery, the 'Tracker Tracker', to map trackers on websites of the Dutch government. I build on Marres' work (2012b) around 'material participation' to argue that this device has a particular social-technical way of dealing with web tracking. Through the case study I reflect upon how Ghostery participates in in defining surveillance. First, it operates as an *issue device*, through its way of defining and ranking trackers, and second, as a *research device*, as a material research agent. In this way, I discuss how Ghostery, by making web tracking mechanisms transparent, empirically and conceptually, contributes to a very specific understanding of contemporary consumer surveillance.

In Chapter six "Leaky apps and data shots: Technologies of leakage and insertion in NSA surveillance", I flesh out the conceptual benefits of surveillance as public matter. The chapter deals with the NSA files, disclosed by Edward Snowden from June 2013 onwards. I build on a particular research trajectory within Surveillance Studies. Here I refer to the reconceptualisation of notions of surveillance as a response to the introduction of new technologies. I bring that discussion into conversation with the NSA files. By drawing on a set of news publications about the NSA files, I highlight two ways in which the NSA, or occasionally the GCHQ, has captured data. The first consists of a list of programs that extract data because internet technologies 'leak' data. The second is a list of 'devices that insert', for instance, malware. I have done this to conceptualise two distinct forms of movement, leakage and insertion, by which data are captured by NSA programs. Inspired by the works of Wendy Chun (2013) and Jussi Parikka (2007), I discuss the (theoretical) questions for each form and conclude by pointing out future sites of research for surveillance studies and publics in the context of surveillance.

In chapter seven, "Conclusion: The materiality of surveillance made public" I formulate conclusions about the various surveillance awareness projects regarding their different settings and their styles of activism, their contribution to sousveillance analyses in particular, and what their (socio-technical) working environment means for the kind of publics they constitute. I explicate why and how they turn surveillance into 'public matter', into 'issuefied' and public working material that critical internet cultures re-appropriate, and make practical suggestions for possible future research directions in the study of surveillance and surveillance publics.