MEDIATIZATION STUDIES 1/2018 DOI: 10.17951/ms.2018.1.2.85-101

MAREILE KAUFMANN

Department of Criminology and Sociology of Law, University of Oslo, Norway

Mareile.kaufmann@jus.uio.no

"Now you see me – now you don't!" – Practices and purposes of hacking online surveillance

Abstract. This paper describes how hacking can be the act of redefining what is seen and not seen in the context of online surveillance. Based on a qualitative interview study with 22 hackers, it discusses the many practices and purposes of 'hacking online surveillance', with a specific focus on the techniques of disappearing from view while continuing to be online. Not only do these techniques vary in style and the expertise involved, but they all fulfill multiple functions. They are more than just a coded statement against the uneven powers of surveillance, they are tactics of the everyday life, moments of analytical creativity and reflection, instances of pleasure and play, affective encounters, identity work and forms of communication. The paper dedicates space to these sometimes overlapping and sometimes differing conceptualizations of 'hacking online surveillance' by using methodologies that consciously seek out the nonlinear and the multiple.

Key words: Internet, hacking, surveillance, data, obfuscation, politics, play, affect

Introduction

It may be too romantic to portray hackers as illusionists, but this paper describes the ways in which hacking can be a performance of redefining what is seen and what is not seen in the context of dataveillance. If dataveillance means watching populations by tracking their digital data traces, then hacking this form of veillance moves close to "illudere", which means to "mock" and "play against" (Online Etymology Dictionary 2003). Similar to an illusion in the context of sensory perceptions, hacking can deceive the way in which information is usually organized and interpreted. It can become an act of hiding information by making data resemble other kinds of data, or by turning it into information that can be seen and tracked, because it does not reveal anything meaningful.

This article seeks to better understand these acts of redefining what is seen and not seen in the context of online surveillance as *one* aspect of the much larger practice of hacking. In doing so, it questions the dominant representations of hackers as either criminal (e.g. Furnell, Warren 1999; Rost, Glass 2010) or as counter-cultural (Kubitschko 2015) and activist (Schrock 2016). It analyzes the multiple ways in which hackers interrogate online surveillance or dataveillance, and how they argue about these acts. In specific, it looks at those kinds of hacks that are enacted while hackers continue to share data online.

Brunton and Nissenbaum started the more general conversation about protesting dataveillance in 2011, when they wrote about practices of "obfuscation" (2011; 2015). In an environment where users of digital services neither get to choose whether they want to be surveilled or not, nor are they aware about the way in which information about them is analyzed, obfuscation occurs as a defense mechanism (ibid.). Brunton and Nissenbaum define it as "adding noise to an existing collection of data in order to make the collection more ambiguous, confusing, harder to use, and therefore less valuable" (2011, online). The way in which Brunton and Nissenbaum characterize different ways of obfuscating information is helpful in structuring the practices of avoiding the kind of dataveillance that this article presents. However, this paper adds more nuances to this conversation. Firstly, it discusses the practices of interrogating dataveillance and online surveillance as a form of *hacking*, which is broadly defined as the "reappropriation of an object or a system for another purpose than originally intended" (Zarzycki 2018, online). In doing so, it also moves away from the idea that data is made "less valuable" (Brunton and Nissenbaum 2011, online) through these hacks. Rather, the value of data is re-defined through such hacks, made less valuable for some and more valuable for others. With that, the article ambiguates the clear categories through which Brunton and Nissenbaum analyze and discuss techniques of resisting dataveillance. At a political level, for example, Brunton and Nissenbaum associate obfuscation with "weak" and sneaky forms of protest (ibid.). They consider it a "last resort" as they highlight a number of problematic features: obfuscation tends to be dishonest, its users want to receive services without contributing to their functioning, and some techniques pollute valuable online space (ibid.). This paper discusses the meanings and implications of hacking dataveillance as more multifaceted than that. The empirical analysis presented in this paper shows that hackers are well aware about the pros and cons of interrogating online veillance and discuss them amongst each other. As a result, hacking dataveillance is much more than 'weak' political protest. Hacking dataveillance does not necessarily follow a binary understanding of surveillance and countering surveillance. These media practices are also tactics of the everyday life, moments of analytical creativity and reflection, instances of pleasure and play, affective encounters, identity work and highly personal forms of communication.

The paper develops this argument, first by introducing the reader to ongoing discourses about hacking. While it provides a basic definition of hacking, it emphasizes

the importance of analyzing the multiplicities and ambiguities of hacking practices. The subsequent part explains how such a study of multiplicity was conducted via the methodological route of *attuning to mess*. After that, the paper presents its analytical findings, an overview of different techniques or media practices of hacking dataveillance, which are then made sense of vis-à-vis different theoretical strands. These theories lead us away from straightforward readings of hacking surveillance as political protest towards alternative readings. Showing the plurality of these practices and their purposes is no attempt to paint a complete picture of hacking. It is rather the opposite, it attempts to invite heterogeneous interpretations and provoke standardized positions about hacking as "either lauded or denounced" as Coleman and Golub critically remark (2008, p. 256).

Understanding hacking – without shortcuts

If we study academic debates about hacking, we find no agreement about the figure of the hacker. Rather, we find a broad variety of practices and ethical codes that are associated with hacking, and an inclination to agree on certain traits (cf. Coleman 2017; Coleman, Golub 2008; Söderberg, Delfanti 2015). What ties practices of hacking together is the idea of disassembling, rethinking and "re-appropriating" a standard (cf. Zarzycki 2018), which is "guided by a crafting sensibility" (Coleman 2017, p. 92). This necessarily involves autonomous ways of thinking, while solutions are approached "with technical know-how and ability, but also with some degree of agility, guile, and even disrespect" (ibid.). Even though technology may be central to the ways in which hackers express themselves (Coleman, Golub 2008), the level of technical expertise varies and does not have to involve coding skills. What is more characteristic of hacking is the moment of playing with and re-appropriating anything that seems to be a given – an attitude that is also expressed by the greater hacker and maker culture (Richterich, Wenz 2017).

When it comes to the political significance of hacking, there is a tendency to take shortcuts or sides. Among the most prevalent of such shortcuts is the framing of hacking as a cyber-crime and -terrorism. Here, hackers find their place on "the dark side of software engineering" (Rost, Glass 2010, p. 113), where they "represent a well-known threat" (Furnell, Warren 1999, p. 28). Such partial accounts of hacking, in turn, inspire literature that portrays it as a practice that creates social value, but is politically exploited to heighten control in cyberspace (Nissenbaum 2004). This literature ties in with (early) accounts of hacktivism, i.e. computerized activism, which Wray (1998) collects with terms such as "grassroots infowar", "electronic civil disobedience" and "politicized hacking" in the "rubric of extraparliamentarian direct action Net politics, where extraparliamentarian is taken to mean (…) the grassroots politics of social movement" (Wray 1998, online). Yet, Taylor (2005) critically analyzes

that the technological skills involved in hacktivism and other forms of direct action Net politics could also be co-opted for productive needs in the capitalist system. Similarly, Coleman and Golub (2008) dissolve these polarized views on hacking as either crime or a social movement when they carve out the many conflicting strands in the liberalist agenda that is associated with hacking. Hacker cultures are "under constant negotiation and reformulation and replete with points of contention" (ibid., p. 255). Equally, Jordan's *Genealogy of Hacking* describes it as "different, sometimes incompatible, material practices" (2017, p. 528; s. also Söderberg, Delfanti 2015). That is to say, our understanding of hacking is not exhaustive if we describe hacking as either "political" (cf. Söderberg 2017) or "mundane" (Davies 2018). Instead, we should read varying accounts of hacking as an inspiration; they broaden our understanding of hacking as practices with multiple meanings. In the context of online surveillance, for example, the framing of hacking as political practice has already many facets: it is discussed as "data activism and advocacy" (Schrock 2016), as "resistance" (Leistert 2012) and as counter-culture to surveillance (Kubitschko 2015). While the paper at hand is likely to be associated with these latter readings of hacking, it makes a more conscious effort to complicate even these diverse descriptions of hacking in the context of surveillance. The techniques and meanings that hacking takes in the situation of dataveillance are analyzed using Vicky Squire's methodological avenue of "attuning to mess" (2013).

Making things complicated: methodological fine-tuning

We have seen that one-dimensional accounts of hacking cannot be attributed to the phenomenon itself. They can be the result of the rules at play in academic publication economies, i.e. the limited amount of words available in an article. Simplified portrayals of hacking can also be the result of thematic focus, for example, when the intention is to challenge a specific representation of hacking, but they can also be the consequence of methodological choice. Even in the context of dataveillance, which is only one of many situations in which hacking is enacted, hacking is not a simple practice of countering surveillance. It takes on many forms and fulfills equally many functions.

In order to study this multiplicity I chose to conduct 22 interviews with hackers in Germany, Austria and Switzerland that I recruited via a snowball-sampling method. The sample ranged from loosely associated members of hacker clubs to more experienced hackers. Most interviews were conducted one-to-one, while a few interviewees preferred a group-setting. However, none of the interviews were conducted face-to-face, all of them were enabled via different software packages for reasons that I will expand on below. The interviews varied in length from 45 minutes up to 2.5 hours, and followed a guide that was refined throughout the project. The interview-guide was structured in a way that allowed me to explore concrete practices of disputing

dataveillance, but also motivations and symbolisms tied to these media practices. Interviews not conducted in English were translated for the sake of citation. The choice to conduct qualitative research with in-depth interviews gave me the opportunity to ask for details and prompt reflections and explanations concerning the interviewee's online practices. I transcribed and coded all interviews according to thematic clusters in a software model for qualitative research. I organized this analytic phase and the clustering of the interview material with the aim of rendering the prevalent understandings of hacking dataveillance more heterogeneous. Indeed, when studying a multi-layered practice, it is striking how methodological choice constitutes knowledge production. Walking the pathway of "methodological managerialism" (Law, Singleton 2005, p. 333) – a framework that makes empirical material fit into neat and regular categories, would have reduced this paper's exploration to maybe one of the many layers that the material revealed. A complex research object, however, surprises us and frustrates our investigations, because it is "messier than a disciplined mindset might presume" (Squire 2013, p. 37). As such, it challenges us to attune to this "mess" (2013).

For example, the sampling of hard-to-reach subjects such as hackers is a surprising process. I started out with a snowball sampling method, writing invitations to the mailing lists of several dozen local Chaos Computer Clubs. The replies I received were unexpected: not I – the interviewer – would pose questions to potential research subjects, but the hackers posed their questions first. Despite a rather detailed information sheet about the project and the approval of the Norwegian research ethics authorities (NSD), I had to pass various question-and-answer sessions about surveillance. In addition, I had to install specific programs on my computer in order to guarantee the interviewees' anonymity and to gain their trust. While not all interviewees were equally careful in assessing my trustworthiness, others did not continue their conversation with me after the initial invitation. As such, the interviewees ranged from extremely careful and highly anonymized subjects who would only agree to chat-based interviews in end-to-end encrypted programs to hobby hackers that would, despite the foreseen anonymization, share their real names and identities and allow an interview via Skype. Some were technically highly skilled, while others discussed more mundane techniques of disappearing from online veillance. Some interviewees conducted hacks that are considered illegal, while others disapproved of such hacks. Some interviewees prepared their arguments for the occasion, while others were simply curious or wanted to help out spontaneously.

This illustrates that the variety of knowledge and positions about surveillance not only determined the practical setting of the interview situation. The different personas, positions and hacking practices I learned about also led me to re-think my pre-conceptualizations of hacking. When I listened to how hacking is enacted and argued about, it was important to resist the "impulse to hold the object of analysis together as a coherent one" (Squire 2013: 38). Understanding hacking as a straightforward political practice, for example, would have given the project comfortable coherency.

However, it was necessary to allow the research subjects to "object to the utterances" that I would make about them (cf. Latour 2000, p. 115). It was significant, for example, how much the interviewees disagreed amongst each other about what constitutes politically and ethically correct hacking techniques. Getting to know hacking, then, also included "cutting" (Squire 2013, p. 38) into the ways in which hacking is constituted through fixed concepts – whether in scholarship or within hacker communities.

Maintaining this described openness and balancing it with precision (Squire 2013, p. 38) informed the way in which I implemented the method, i.e. how the interviews were conducted, and how I coded and interpreted the interview material. The interviews were guided by broad rather than narrow questions, the analysis by expansive rather than reductive conceptual nodes. I used theory for inspiration, which allowed theory and empirics to adapt to each other flexibly (ibid., p. 40). In this spirit, this paper deploys heterogeneous yet equally relevant theoretical approaches to discuss hacking in the context of dataveillance. Each of them sketches out one facet of a larger picture; a picture we would miss, if we were to prioritize one concept over others. We will now turn to the analysis that emerged from this approach. It introduces different techniques and media practices of hacking dataveillance.

Avoiding digital observation online – an analysis of different media practices

While all forms of hacking in the context of dataveillance deserve to be explored, this paper does not discuss hacks that make information disappear, move data traffic to networks outside the Internet (e.g. to parallel networks) or disable information traffic (e.g. with DDoS attacks). The aim of this paper was to explore practices of disputing dataveillance that are enacted *while the subjects sustain data-exchange online*. That angle was chosen, because many hackers do not want to abandon online services at the same time as they seek to interrogate them. Thus, the research project focuses on hacks that allow digital information to move through trackable channels, while tracing this information would not (or not easily) reveal the insights for which this data is surveilled. We should think of these hacks as online camouflage or coded play. Brunton and Nissenbaum's schema of obfuscation techniques (2011) serves here as a conceptual railing, but we can see that the actual implementations and the discussions of these techniques will introduce further nuances.

Encryption and steganography

The first form of interrogating observation online comes close to what Brunton and Nissenbaum would call "selective obfuscation" (2011, online). Most of these practices are based on encryption that obscures contents for some, but reveals them to a select and adept few. Generally, encryption techniques use one if not several keys to encode

information when it is sent – making it look like a random sequence of signs – and then decode it when it is received. Encryption is then a way of hacking communication standards in order to exchange information in a surveilled channel without revealing its contents. Interviewee D gave a less technical example:

> Int. D: "Stenography. (…) A way of data transmission that makes it impossible to find the data, especially not with a filter or other kinds of technology."
>
> Interviewer: "How would that work?"
>
> Int. D: "There are many ways: visual ways, languages, different logical connections to transmit a message that cannot be digitized, (…) a chat via two different chat providers, where you only send a part via each program. (…) There are so many options! In most of the cases I know, you as a private person create a key and once the other understands it, you can use it as a communication means. That's the point: you can only communicate with that one person that you want to communicate with."
>
> Interviewer: "And those keys are not necessarily created via a programming language, but also include social codes? (…) Do you know of other hackers using that?"
>
> Int. D: "Many! For example, for indicating time, you only send a (…) digital picture of an analogue watch with the time. That is practical, because you could communicate a time without creating a direct association."

Thus, steganography is an often social, sometimes socio-technical secret code that conceals the content of a message or even the fact that a message is being sent. Sending pictures instead of words can be one such practice. Other low-tech codes include the use of leet-speak, also written as "1337" (Int. D), in which some characters are replaced by other stand-ins that can include numbers, symbols or other alphabetic characters. It is a popular code used already to create screen names. danah boyd's (2014) work on social steganography gives us another example: teenagers who seek to escape their parents' surveillance mention the use of song lyrics to communicate situations, feelings and opinions. These lyrics would only be meaningful to those who quote and read them. More sophisticated forms of steganography use algorithms that apply the chosen code automatically to the information you share online.

Not all forms of encryption are considered a hack. In fact, the readers of this article are probably quite familiar with some such techniques, as for example e-mail encryption via PGP-certificates.

> "I am sure that TOR is no longer secure anymore (…) especially if you don't know how to use it and laypeople use it too, then it's hard to say that it's secure. The only thing that I actually feel is secure, is e-mail encryption with PGP. PGP is still uncrackable, there is nothing happening there, but anything else, VPA… there is nothing… GSM, GPS information, all of this is somehow hackable." (Int. H)

Using PGP does not require advanced technical knowledge and has in fact become itself a communication standard in some communities. It is nonetheless an important tool for most interviewees to establish online privacy. Especially selecting the encryption key is a conscious choice and a matter of trust: from whom do I get the encryption keys? Who else understood them already? Can the keys be hacked again? Many interviewees trusted only open source keys, since these would not be owned by parties with commercial interests.

The problem that most informants mentioned in relation to PGP was that its users would always be identifiable. Since PGP is a certificate attached to email-conversations, its users would ironically stick out and gain more visibility.

> "What I do most often in practice is to encrypt my data, but the problem is of course that my metadata is still visible, which means that someone who is watching me can – with a little bit of statistics and some solid assumptions – draw conclusions about my communication. If I encrypt my mails and I am active in a political group, then it's possible to recognize – just by surveilling the data traffic – the decision-making structures. If one can recognize specific communication patterns, you can deduce something about the contents of these communications, for example: every Saturday when you want to organize the info-table in the city center, it's the same three people talking to each other." (Int. G)

Some interviewees would thus avoid using PGP and deploy other forms of hacking communication standards.

Making messages disappear in excess traffic

One technique is to generate random Internet traffic in order to hide one's message in the mass of information. It comes close to what Brunton and Nissenbaum call "time-based obfuscation" (2011), where the processing of data for meaningful content is done under time pressure and any irrelevant information distracts from finding the results. However, it differs from time-based obfuscation, too, since not all forms of hiding messages in random traffic are based on extending the time needed to analyze information. They build on the assumption that no one would use the necessary amount of resources to filter out the meaningful from the non-meaningful messages.

> Int. J: "There is a fun browser-plug-in that generates random traffic, but I don't use it. I'm not a fan of it."
>
> Interviewer: "Why not?"
>
> Int. J: "Good question (…) somehow the limits are reached. I made a certain threat-model for myself, asking whom do I actually want to defend myself against? I could also defend myself against the NSA, but in that case we would not be able speak to each other today. My threat model is not that a three-letter agency invests money into attacking me as a single person."

Further, hiding one's messages in data traffic is not necessarily trusted, because some algorithms may be able to filter out meaningful messages. Interviewee G mentions yet a different, an ethical reason:

> "The problem is that in order to disappear you need to generate incredible amounts of traffic. I think that is not a great idea, because in a network where bandwidth is a scarce resource, creating (…) traffic like that is not sensible. (…) In general, it is a good idea to hide in the masses, but the question is whether it is actually doable. Especially if it produces a lot of white noise – just so that people don't see what you do." (Int. G)

Repurposing standard communication pathways

When asked where hackers still find un-surveilled room online, they tend to mention 'The Onion Router' (TOR) (Int. A; F; K; M). They describe it as a place where interruption by surveillers is less likely. In fact, Interviewee I commented about TOR:

> "If you define 'an unsurveilled space online' as a place where no one passively watches while people are actively communicating, then such a place does not exist. But there are online spaces in which governmental actors cannot exercise censorship."

Brunton and Nissenbaum defined TOR as cooperative obfuscation (2011), since is cannot be fulfilled by single actors. Instead, TOR is based on the network effect: information is not simply sent from sender A to receiver B, but it takes roundabouts via three different senders and receivers worldwide, before it arrives at the intended receiver. This makes it harder to identify whom sent what kind of message to whom. As such, TOR would be a technique of hacking and repurposing standard communication pathways online. The more people offer nodes through which information can be sent, the harder it is to track or predict the paths that messages take. However, some interviewees considered TOR insecure, since the entry and exit nodes would still be trackable (Int. H, L, Q, R), others considered using TOR as "disproportionate" – it would be too massive a tool to gain privacy (Int. L).

Masking

A more radical set of techniques is similar to what Brunton and Nissenbaum label "ambiguating obfuscation" (2011). The idea is here to render an individual's data "permanently dubious" (ibid.). Such techniques hack the standards of information that is usually shared or communicated about oneself. This is why the hack is also called masking. It is not very different from disguising oneself as it involves the consistent use of false IDs or of several accounts for different kinds of topics.

> "You can find so many things in Google about me that it just does not make any sense anymore (…). It's a different identity – the person I am online does not match me anymore. And I do like that!" (Int. O)

A similar technique is to mask location data or computer addresses. Even though such moves seem simple at first, they not only meet the challenge of growing regulations, terms and conditions on most platforms, but the consistent use of several masks requires dedicated and well-planned online behavior.

One of the most laborious forms of masking is to trick surveillance algorithms by feeding them diverging, unexpected or inconsistent datasets:

> "These are only algorithms! One has to know the algorithm, but (…) I do reverse engineering. (…) I try to find source codes and once I have them, I can trick it. It's difficult, but doable. (…) Sometimes it takes months, but it works, even if is a self-learning algorithm. I know how to program AI algorithms, so I see every day how that works, how the statistics work – it's only a few equations. It is very difficult to find all the parameters, but the people who programmed them in the first place knew what they trained the algorithm to know." (Int. O)

Not all interviewees agreed that this is a simple or a sensible hack, because most algorithms' workings are currently trade secrets that are hard to crack and not easy to circumvent. In addition, some self-learning algorithms may be able to filter users out anyway. Those who worked with this technique admitted that feeding algorithms inconsistent datasets would have to be done constantly, which requires a lot of effort and limits the user's freedoms.

Brunton and Nissenbaum's categorization of obfuscation (2011; 2015) was indeed a helpful tool to structure the different techniques used to hack dataveillance online. However, the analysis conducted in this paper emphasized that these techniques are not passive means of disappearance and of rendering messages obscure as Brunton and Nissenbaum's use of the term "obfuscation" implies (ibid.). Rather, they are active forms of avoiding observation by some, but also an invitation to be seen and understood by others. These practices are not just about concealing one's information, they are hacks in the sense of decoding and repurposing online communication standards, which are pre-determined by technological specifications and human usage. Further, the description here has shown that there are internal debates among hacker cultures about the intentions, the sensibilities, the constructive and destructive potential, as well as the ethics of deploying such techniques. These are not only academic evaluations outside hacker cultures, but these debates are well-embedded inside hacker cultures, too. Such discussions and the dilemmas that some of the interviewees indicated also highlight the difficulty of separating the techniques from each other. Many techniques are used in parallel, and, more importantly, most hacking practices depend

on a combination of cooperative, selective and ambiguative techniques. As a result, they do not fulfill the simple function of protesting online veillance by obscuring data, but combine many, sometimes even discrepant functions. Based on these insights, this paper now moves on to a discussion of hacking dataveillance.

Discussion: weaving theory into the many techniques of hacking dataveillance

The techniques described above are more than just a form of hiding digitally or tricking algorithms. Rather, they fulfill many functions, some of which complement and some challenge each other. The paper describes and illustrates these by tying the interview material and the analyzed techniques to different theoretical concepts.

Hacking dataveillance as a tactic of everyday life

If we let ourselves be inspired by Michel de Certeau (1984), hacking dataveillance can be a tactic of the everyday life. The *everyday* is here not to be interpreted negatively. Rather, the "multitude of "tactics" articulated in the details of everyday life" (ibid., p. xv) are understood as a form of interrogating the powerful strategies of institutions; these are a re-appropriation, subversion and individualization of given or mainstream cultures. People who interrogate power structures with mundane practices are thus not passive, but creative in their everyday actions. One of the famous examples that de Certeau gives us matches the practice of hacking dataveillance very well. In the chapter *Walking the city* he discusses New York's World Trade Center as representing the "all-seeing power" and New York's street grids "down below" (ibid., p. 94) as the given structures that ordinary people will have to walk in their everyday lives. If we compare this situation to life online, surveillance can never be as total as "seeing the whole" (ibid., p. 93) picture from above. Yet, the trackability of information is one of the basic conditions of Internet traffic (Kaufmann and Jeandesboz 2016). With that, it is also the precondition for surveillance: whoever has the capacity to track, store and process information that users produce in their everyday lives lifts themselves into a position of seeing the data and data traffic necessary to organize its users. That is at least what surveillers seem to believe. The "scopic drive" that produced the Manhattan architectures (ibid.) now also generates online surveillance techniques. De Certeau's study of the everyday practices of walking the streets, however, finds that people do not relate to the street grid in predictable ways. They improvise, the take surprising turns, they create shortcuts; they produce techniques "that are foreign to the "geometrical" or "geographical" space of visual, panoptic, or theoretical constructions" (ibid., p. 94). The hacking moves described above are not foreign to the geometries of dataveillance. Yet, by "[e]scaping the imaginary totalizations produced by the eye, the everyday has a certain strangeness that does not surface, or whose surface is only

its upper limit, outlining itself against the visible" (ibid.). Much in the same way, the techniques described above escape the imaginary totalizations of dataveillance. Even if hackers are not necessarily comparable to ordinary people, they hack as part of their everyday life and sometimes they even use techniques that are considered mundane. Everyday life, then, is a way of relating to the given rules and standards of accessing and communicating on the Internet, but it is productive of tactics that never quite take these rules as a given. In the spirit of hacking and making these rules are re-interpreted and used to escape the view of dataveillers, sometimes as a purposeful tactic (e.g. by using a self-developed code), sometimes as a routine (e.g. by using PGP certificates by default).

Hacking dataveillance as a moment of analytical creativity and reflection that can be political

When rationalized and deliberately chosen, such quotidian techniques tend to become a political practice. Hacking is a political culture – at least in the sense that it has produced concrete impacts and artifacts: manifestos, games, publications, agreements, including anything from supporting legal structure to illegal transgressions and "envisioning alternatives that will be central to debates about possible legal futures" (Coleman, Galub 2008, p. 272). However, within academic literature, there is a tendency to discuss hacking as an ethical political practice (Nissenbaum 2004; Schrock 2016). The word ethical carries the connotation of being politically correct: hacking is considered ethical, for example, when it is used to make a statement about uneven power-balances. In some cases, the innocent 'white hat' is used to describe the practice of revealing holes in security scripts. Such descriptions of hacking as ethical political practice tend to polarize: they turn political acts into either good or bad, for or against, ethical or unethical. It would be easy to interpret the techniques described above as either dubious practices or as political acts of resisting surveillance. Both accounts, however, would nourish the dyadic understanding of the arms race between surveillance and resistance (Gilliom, Monahan 2012). Indeed, hacking in the context of dataveillance is a moment of creative reflection that is political – not least because many interviewees deliberated about the implications of choosing a particular technique over another. Yet, the epistemological stance of the paper is that there is no merit in making hackers take sides: either that of the surveilling parties or the surveilled, of being a power- or counter-power, of being conform or resistant. In light of the techniques and arguments described above, hacking can be understood as a practice of interrogating technologies – for whatever purpose. The actual practice of asking questions and re-appropriating infrastructures, is what makes it political. In order to be political, these interrogations do not have to be coordinated or follow a unified ethical code. They can and do involve "multiple disagreements about conceptions of rights, autonomy, and dispositions of acceptability" (cf. Huysmans 2016, p. 91). Interestingly, hacking as a political moment

ties in with de Certeau's everyday tactics, since such interrogations can be banal acts enveloped in everyday life, but they are re-interpretative and curious in nature. There is political power in "diffuse little practices and things in their own right" (ibid., p. 92). Without recognizing their political significance, it would be easy to dismiss the curiosity that drives the many techniques described above. Moreover, it is crucial to tie the political curiosity that inspires hacking dataveillance to the everyday, since that curiosity would otherwise feed the same 'politics of suspicion', 'calls for transparency' and grand narratives of 'uncovering secrets' that motivate dataveillance in the first place (cf. Huysmans 2016, p. 92).

The curiosity involved in the re-interpretative techniques of hacking also emphasizes that they can be a moment of analytical creativity. It is not by chance that Coleman subtitles hacking the "weapons of the geek" (Coleman 2015). Even though the vocabulary of weapons and defense feeds the polarizing notions that this paper argues against, it became clear from the interviews that hacking at least requires analytic, sometimes 'geeky' know-how, which also implies that it is done for fun. Especially the practices described above are a creative and analytic engagement with visibility.

Hacking dataveillance as an instance of pleasure and play

When Sicart writes about the performative pleasure of tinkering with software and procedures "to figure out what they do" (2014, p. 97; cf. Int. O), he describes a moment of coded play or play with code. He goes even further when he states:

In fact, there are arguably performative pleasures in the computational processes themselves. They are systems, but they are open to performing with them or performing themselves in a creative, expressive way, an openness in which they are playful (ibid.).

The interviewees clearly enjoyed working with computing systems in the first place. More specifically, some mentioned the pleasures of challenging existing forms of dataveillance by circumventing them, by redefining the codes and languages such surveillance systems would be set out to monitor (cf. Int. D; O). Such analytic creativity is one of the drivers of the hacker and maker culture at large (cf. Richterich, Wenz 2017). It is in line with Sicart's ideas of "play as a dance of resistance and appropriation, of creation and destruction of order" (Sicart 2014, p. 98). Even in the context of dataveillance, hacking is never just resistance. Here, play means both, playing systems and playing with systems. Computing systems give the pleasure of bound experience and play is the pleasure of breaking with these boundaries to make them your own (ibid.). Playing with surveillance systems allows players to "reambiguate" (ibid.) them. The idea that online communication follows specific standards is what provides surveillers with explanatory patterns on the one hand. On the other hand, standards are precisely what allows hackers to play: to disrupt standards and reambiguate such patterns. Tinkering with standards entails that algorithms and software codes can no longer identify the patterns they are set out to find. Hacking dataveillance is thus not only

an everyday or a political practice of interrogating given codes. From a perspective of play, it renders dataveillance into a sometimes even pleasurable game of hide-and-seek, of creating secret languages, of tricking algorithmic systems, of tinkering with code and inventing riddles that only dedicated counterparts can solve.

Hacking dataveillance as an affective encounter

There is excitement, enthusiasm, amusement, thrill, concentration and tension when specific techniques of hacking dataveillance are put into practice. In addition, the choice to interrogate dataveillance in the first place is also filled with many emotions. Hacking is not just a rational practice, but a somatic experience – especially in a context that is as emotionally laden as online surveillance. Even though the empirical data collected for this article does not include observations, the Interviewees did mention the emotional landscapes that are tied to hacking dataveillance. In the context of online surveillance they experienced "pressures" (Int. A, B), "fear" (Int. C), "problematic notions of comfort" (Int. A), "naiveté" (Int. I) and "credulity" (Int. B), but also "Ohnmacht" (Int. A; translation: "powerlessness") and even "creeping pain levels" (Int. C). Hacking is in turn associated with the emotions and somatic excitements of "activism" (Int. A; K), "self-empowerment" (Int. A), "being constructive" (Int. I), "necessary disobedience"[1], "egoistic self-protection" (Int. S) and "self-defense" (Int. G, N, R). They elicit the joys of "developing something further" (Int. D), "being awake" (Int. N), "setting an example" (Int. Q), the energies of "willpower" (Int. F), "pride" (Int. O) at the same time as different forms of "venting anger" (Int. H). In the specific context of dataveillance hacking is thus not just a set of analytical techniques or interrogations, both of which emphasize the rational aspects of hacking, but it is a more extensive physical experience. We can conceptualize these different emotional landscapes described above as a field of tension, as a back-and-forth between being acted upon, being incited to act and actual action. If we look at the back-and-forth between dataveillance and hacking the same, we can understand this dynamic through the affective encounter. This encounter happens in this vast emotional landscape where different actions (e.g. surveillance) trigger different emotions and reactions (e.g. hacking surveillance). In this landscape, affect is the onset for action. Massumi characterizes affect as a pre-conscious incitement, as capacity to act, "a state of suspense, potentially of disruption" (1995, p. 86). Affect is that which precedes emotions, but fills the body with the capacity to do something. This moment of incitement is what eventually leads to action and the emotional experience of hacking dataveillance. This somatic and intimate dimension is also no stranger to Sicart's theory of play. Play, especially when performed as hacking dataveillance, is "appropriation, expression, and a personal affair" (Sicart 2014, p. 100).

[1] (Int. A, B, C, D, E, F, G, H, J, K, L, M, N, O, P, Q, S agree on this, but some of them mention that hacking is not always civil disobedience, and it is not necessarily desirable)

Hacking dataveillance as identity work and a form of communication

The link from wanting to protect personal information to understanding hacking dataveillance as a "personal affair" (ibid.) is not very difficult to make. The Interviewees did talk about the personal dimension of the practices they enacted. Many of them considered, for example, the actual choice of technique as personal. It expresses one's opinions about surveillance at large, but also one's standpoint within the hacker community. Choosing open source code, for example, is a critical statement about the commercial software industry that follows its own interests and not necessarily that of its users. An example that relates to articulating standpoints within the hacker community is the abovementioned decision to either use PGP or techniques that generate traffic to make one's messages disappear. Some hacks were even developed by the interviewees, spontaneously or over long periods of time. Enacting this creativity and formulating such standpoints, then, is part of establishing a sense of self (cf. Coleman, Golub 2008, p. 271). Technology is not only a means to an end, but interacting with it, creating personal scripts for it and re-appropriating it – making it one's own – is identity work. How technology is tinkered with, to what (personal) purposes it is adapted to, and which kind of language is developed in order to communicate with select persons is closely linked to the identity of the hacker. On a more superficial level, identity work is also performed in relation to a hacker's online identity. Special forms of hacking dataveillance are literally dedicated to hacking and re-appropriating that online identity, for example by using diverse screen names and IP addresses. Others go further and create online personas that have as little as possible to do with their private person in order to escape algorithmic profiling. With a focus on the creativity and ingenuity that it requires, hacking dataveillance also becomes a tool to communicate personal skills, it establishes connections and builds networks. It is, however, more than a communicative device: it is a language with its own vocabulary and syntactic constructions. These vocabularies and syntaxes can take the shape of riddles, masks, character replacements, steganographies (boyd 2014) and other codifications.

When used as argot or as secret language, hacking expresses identity and opinion about online surveillance. As with any language, its use is inseparable from emotions and somatic experiences, but mastering it often involves analytic creativity as well as play. In many instances, hacking dataveillance is the language of political interrogation, which can be spoken loudly or gently, but, most importantly, it is spoken every day. With that, it is a living thing that changes with the many small adaptations to ever-new surveillance contexts.

Conclusions

Hackers may not be illusionists, but in the context of dataveillance hackers like to redefine what is seen and what is not seen. More specifically, they hack communication standards online in order to define who gets to see what. In doing so, they seek to distinguish between those who are allowed to track information and those who are not. Based on qualitative interview material, this paper described such techniques of hacking dataveillance with a special focus on those hacks that allow its enactors to continue to be online. These hacks were discussed and theorized, resisting the temptation to revert to the simplified and dyadic concepts of good and evil, or power and counter-power. Instead, the aim of the paper was to render such neat categories more messy, which means that it focused on the multiplicity of meanings and functions. What analysis and discussion have shown is that the media practices of encryption and steganography, of making messages disappear in excess traffic, of repurposing standard communication pathways and of masking can mean anything from politics to play, from identity work to analytical creativity, from bold statements to routines. Yet, they all signify how the issue of dataveillance is made one's own. That is to say, in all the theorizations of hacking dataveillance suggested in this paper, we find moments of taking apart, of repurposing, of creativity, affect, identity and communication. While the hacker is commonly analyzed as a stylized figure – a criminal or activist – this paper showed that such categorical readings of hacking are pervaded by the individual and the personal, because hacking dataveillance means interrogating online standards and re-appropriating them.

References

boyd d. (2014). *Privacy. Why do youth share so publicly?* In d. boyd (Ed.), *It's complicated. The social lives of networked teens*. Yale University Press: New Haven/London, pp. 54–76.

Brunton F., Nissenbaum H. (2011). Vernacular resistance to data collection and analysis: A political theory of obfuscation. *First Monday,* Vol. 16(5), https://doi.org/10.5210/fm.v16i5.3493, 15.09.2018.

Brunton F., Nissenbaum H. (2015). *Obfuscation: A User's Guide for Privacy and Protest*. MIT Press: Cambridge, Massachusetts.

Coleman G., Golub A. (2008). Hacker practice. Moral genres and the cultural articulation of liberalism. *Anthropological Theory,* Vol. 8(3), pp. 255–277.

Coleman G. (2015). *Hacker, Hoaxer, Whistleblower, Spy. The many faces of Anonymous*. Verso: London/New York.

Coleman G. (2017). From internet Farming to Weapons of the Geek. *Current Anthropology,* Vol. 58(S15), pp. 91–102.

Davies S. (2018). Characterizing Hacking: Mundane Engagement in US Hacker and Makerspaces. Science, *Technology and Human Values,* Vol. 43(2), pp. 171–197.

De Certeau M. (1984). *The Practice of Everyday Life*. University of California Press: Berkeley and Los Angeles.

Furnell S., Warren M. (1999). Computer hacking and cyber terrorism: the real threats in the new millennium? *Computers & Security,* Vol. 18(1), pp. 28–34.

Gilliom J., Monahan T. (2012). *Everyday resistance*. In K. Ball, K. Haggerty, D. Lyon (Eds.), *Routledge Handbook of Surveillance Studies*. Routledge: London, pp. 405–411.

Huysmans J. (2016). Democratic curiosity in times of surveillance. *European Journal of International Security,* Vol. 1(1), pp. 73 – 93.

Jordan T. (2017). A genealogy of hacking. Convergence: *The International Journal of Research into New Media and Technologies*, Vol. 23(5), pp. 528–544.

Kaufmann M., Jeandesboz J. (2016). Politics and 'the digital': From singularity to specificity. *European Journal of Social Theory,* Vol. 20(3), pp. 373–91.

Kubitschko S. (2015). The Role of Hackers in Countering Surveillance and Promoting Democracy. *Media and Communication,* Vol. 3(2), pp. 77–87.

Latour B. (2000). When things strike back. A possible contribution of 'science studies' to social sciences. *British Journal of Sociology,* Vol. 51, pp. 107–24.

Law J., Singleton V. (2005). Object lessons. *Organization*, Vol. 12(3), pp. 331–355.

Leistert O. (2012). Resistance against Cyber-Surveillance within Social Movements and how Surveillance adapts. *Surveillance & Society,* Vol. 9(4), pp. 441–456.

Massumi B. (1995). The autonomy of Affect *Cultural Critique,* Vol. 31 (2), pp. 83–109.

Nissenbaum H. (2004). Hackers and the ontology of cyberspace. *New Media & Society,* Vol. 6(2), pp. 195–217.

Online Etymology Dictionary (2003). Reviewer: W. Miller, Florida Atlantic University. Choice Issue: 41(2), http://www.etymonline.com/, 7.03.2018.

Richterich A., Wenz K. (2017). Introduction. Making and Hacking. *Digital Culture and Society,* Vol. 3(1), pp. 5–21.

Rost J., Glass R. (2010). *Hacking*. In J. Rost, R. Glass (Eds), *The Dark Side of Software Engineering*. Wiley: Hoboken, pp. 113–156.

Schrock A. (2016). Civic hacking as data activism and advocacy: A history from publicity to open government data. *New Media & Society,* Vol. 18(4), pp. 581–599.

Sicart M. (2014). *Play Matters.* MIT Press: Cambridge.

Söderberg J., Delfanti H. (2015). Hacking Hacked! The Life Cycles of Digital Innovation. *Science, Technology, & Human Values,* Vol. 40(5), pp. 793–798.

Söderberg J. (2017). Inquiring Hacking as Politics. A New Departure in Hacker Studies? *Science, Technology, & Human Values*, Vol. 42(5), pp. 969–980.

Squire V. (2013). *Attuning to Mess*. In M. Salter, C. Mutlu (Eds.), *Research Methods in Critical Security Studies. An Introduction*. Routledge: London, pp. 37–41.

Taylor P. (2005). From hackers to hacktivists: speed bumps on the global superhighway. *New Media & Society,* Vol. 7(5), pp. 625–646.

Wray S. (1998). Electronic Civil Disobedience and the World Wide Web of Hacktivism. A Mapping of Extraparliamentarian Direct Action Net Politics. *Switch: New Media Journal,* Vol. 4(2), http://switch.sjsu.edu/web/v4n2/stefan/index.html, 15.09.2018.

Zarzycki A. (2018). *Mods, Hacks, Makers: Crowdsourced Culture and Environment*. In J. Lee (Ed.), *Computational Studies on Cultural Variation and Heredity*. KAIST Research Series. Springer: Singapore, pp. 73–82.