Media and Communication (ISSN: 2183-2439)
2015, Volume 3, Issue 2, Pages 77-87
Doi: 10.17645/mac.v3i2.281

Article

The Role of Hackers in Countering Surveillance and Promoting Democracy

Sebastian Kubitschko

Centre for Media, Communication and Information Research, University of Bremen, 28359 Bremen, Germany;
E-Mail: sebastian.kubitschko@uni-bremen.de

Submitted: 1 April 2015 | In Revised Form: 25 June 2015 | Accepted: 23 July 2015 |
Published: 30 September 2015

Abstract
Practices related to media technologies and infrastructures (MTI) are an increasingly important part of democratic constellations in general and of surveillance tactics in particular. This article does not seek to discuss surveillance *per se*, but instead to open a new line of inquiry by presenting qualitative research on the Chaos Computer Club (CCC)—one of the world's largest and Europe's oldest hacker organizations. Despite the longstanding conception of hacking as infused with political significance, the scope and style of hackers' engagement with emerging issues related to surveillance remains poorly understood. The rationale of this paper is to examine the CCC as a civil society organization that counter-acts contemporary assemblages of surveillance in two ways: first, by de-constructing existing technology and by supporting, building, maintaining and using alternative media technologies and infrastructures that enable more secure and anonymous communication; and second, by articulating their expertise related to contemporary MTI to a wide range of audiences, publics and actors. Highlighting the significance of "privacy" for the health of democracy, I argue that the hacker organization is co-determining "interstitial spaces within information processing practices" (Cohen, 2012, p. 1931), and by doing so is acting on indispensable structural features of contemporary democratic constellations.

Keywords
big data; civil society organization; counter-power; democracy; hacker; locative media; media technologies and infrastructures; participatory media; privacy; surveillance

Issue
This article is part of the special issue "Surveillance: Critical Analysis and Current Challenges", edited by James Schwoch (Northwestern University, USA), John Laprise (Independent Researcher) and Ivory Mills (Northwestern University, USA).

1. Introduction: A Brief Outline of the Current Surveillance Scenario

Over the past decade, we have witnessed a drastic intensification of both the spread and use of media technologies and infrastructures (MTI). Education, work, politics, consumption, and socialization are but a few central spheres of life that are deeply infiltrated by digitization today. Practices related to or oriented towards MTI penetrate people's daily habits and routines to an unprecedented degree. This ongoing process has altered and, in many cases, multiplied people's ability to connect with each other, and has had a tremendous influence on the way people engage with the world at large (Couldry, 2012; Hepp, 2012). At the same time, networked technologies also enable a wide range of agencies and institutions to exercise control at a distance as well as to collect, sort, analyze and exploit the tremendous amounts of data that accumulate across mediated interactions. In many cases, this has resulted in a "collect everything" approach that is generally understood as surveillance; which, for now, is broadly defined as attention that is "purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence, or protection"(Murakami et al., 2006, p. 4). Surveillance, according to David Lyon, connotes any "collection or processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been garnered" (2001, p. 2). One

could look at the past decades and list both the beneficial and the problematic effects of technology. Yet, the story I want to tell in this article is somewhat more complicated and tries to avoid making overly sharp fractionations. Steering a middle ground in the current discussion on surveillance is by no means an easy task to perform as the debate is (over)loaded with accusations, idealizations, and a generous portion of ideology. This is particularly the case since Edward Snowden's revelations have expanded the notion of surveillance beyond a rather small expert discourse, and have instead catapulted the issue into the mainstream by increasing the level of media, public and political debate.

An accessible way to begin this analysis is to think about the spaces and places we experience surveillance first hand. Here, one might diagnose surveillance as a phenomenon that is most pressing in urban environments, as it is in the city and its surroundings where the highest number of surveillance forms and modes come together—video surveillance, license plate scanners, airports screenings, surveillance satellites and drones, as well as a number of other remote sensing and processing devices. Due to the invention and use of complex technical systems, it is no longer impossible to track and assess the simultaneous movements of tens of thousands of people through a major city. In fact, as scholars have argued convincingly, the ever-increasing surveillance in publicly accessible spaces, such as shopping malls, city streets and places for public transport, changes the ways in which power is exercised in urban space (Koskela, 2000). As a consequence, surveillance contributes to the production of the urban. The city is without a doubt a telling example that demonstrates that the intensification of digitalization often goes along with the amplification of surveillance (see Graham, 2004). Yet, as the above reference to contemporary MTI indicates, the "track record" of surveillance goes far beyond spatial and physical boundaries like urban environments. This, to acknowledge the history of the debate, is not necessarily a new observation as such. In his book on the impact of electronic data processing on personal privacy in the late 1960s, Jeremy Rosenberg stated that, "With the advance of technology, centralized data accumulation becomes easier, the reward for intrusion is increased, and control shifts to still fewer people" (Rosenberg, 1969, p. 1). Yet, times have changed drastically. In particular, the convergence and pervasiveness of MTI that have been developed and disseminated over the past two decades, enable surveillance attention to be continuous, widely distributed, and persistent. Considering today's vast (largely automated) computer power and the quasi-omnipresence of digital devices, the surveillance apparatuses that are currently in place, as well as those that are emerging and spreading, are historically distinctive.

In the following section, I will explicate what exactly makes our times distinctive by highlighting the delicate relationship between surveillance, privacy and the health of contemporary democratic constellations. I argue that hacker organizations like the Chaos Computer Club are one among a range of actors that counter-act contemporary assemblages of surveillance and by doing so act on indispensable structural features of democratic constellations. To develop this argument, the article is divided into three sections. In the first, I discuss three elements—popular online platforms, locative media and big data—that I consider determinative for contemporary surveillance contexts, and then analyze the increasingly symbiotic relationship between government agencies and corporations when it comes to surveillance tactics and practices. In the second section, I focus on the notion of privacy and why it matters for democracy at large. Finally, I use these concepts to examine a qualitative case study of the Chaos Computer Club.

2. Online Platforms, Locative Media and Big Data

Let me start by illuminating three elements that have intensified since the early 2000s and that have lastingly influenced both the way people experience surveillance as well as the way it is practiced. First, *popular online platforms*. The past years have seen an unprecedented triumphal march of a range of platforms that are often referred to as "social media" (see van Dijck, 2013). Considering the ambivalent evolution of the term—coming out of a business background—and the possible interpretation that all other media might be non- or even anti-social, I consider it more appropriate to use the term popular online platforms (see Gillespie, 2010) instead of social media. The main purpose of these platforms is to enable and simplify networking practices via mediated communication. To accomplish their goal, they heavily rely on personal data shared by the user. In accordance with this procedure scholars consider online "social networking" as a set of practices that are inherently based on self-surveillance (Fuchs et al., 2012). In addition, corporations make explicit use of online platforms to monitor and discuss strategies for responding to activists' initiatives (Uldam, 2014). In fact, popular online platforms have become part of people's daily routines to such an extent that they have become an imminent component of and an ideal environment for surveillance. This is not least the case because a small number of centralized communication platforms are much easier to browse, analyze and gain access to than decentralized infrastructures.

Second*, locative media*. With the transformation of mobile media from a communication tool into a multimodal device accompanied by global positioning systems enabling users to share information about one's whereabouts, locative media play a critical role in emerging modes of surveillance (Hjorth, 2013). Geotagging, location search and detection services amplified by portable and wearable devices like smartphones, tablet

computers and smartwatches create new forms of co-presence that disrupt old binaries between online and offline (Schwartz & Halegoua, 2014). The potential to create new levels of surveillance is further enhanced by the fact that locative media intersect with online platforms in many ways because a growing number of services harvest their users' location information. Taking into account that it is exactly the way people use devices, platforms and services that create unprecedentedly large data bodies, scholars have argued that surveillance to a large extent has become participatory (Albrechtslund, 2008). One can sharpen this line of thought by pointing out that the rhetoric of the participatory turn actively exempts surveillance from legal and social control, resulting in a model of surveillance that is light, politically nimble, relatively impervious to regulatory constraint and even casts surveillance in an unambiguously progressive light (Cohen, 2015/forthcoming). Ironically, then, so-called participatory media are intimately connected with surveillance.

Third*, "big data"*. Big data—a notion that not only describes the sheer amount of data but also denotes automated, software-based data gathering, management and analytic capabilities—is best considered the missing piece to the puzzle called surveillance. After all, that is what surveillance is all about: solving a puzzle by bringing the fitting pieces consisting of data material together. Contemporary MTI allow for massive, latent data collection and sophisticated computational modeling (Tufekci, 2014). As Andrejevic and Gates write about the correlations of big data and surveillance: "Even if the underlying goal of capturing information for the pursuit of some form of advantage, leverage, or control remains constant, conventional understandings of the operation of surveillance and its social consequences are being reconfigured by the 'big data' paradigm" (Andrejevic & Gates, 2014, p. 185). Due to the need to interrogate vast quantities of data in very short times, surveillance tactics and strategies today necessarily rely on automated data collection, data analysis, and database management to correlate personal behavior, carve out relevant patterns and to extract metadata. Accordingly, big data is not only reliant on algorithms but also expands their regulatory power (see Beer, 2009; Bucher, 2012). While algorithms have been part of computing since the days of Turing, what we are currently witnessing is the marriage of (big) data and algorithms. One consequence of this convergence is the intrusion of algorithms in everyday life, which aim to analyze incredibly detailed physical, transactional, and behavioral data about people (Pasquale, 2015). Overall, big data play a critical role in turning many aspects of people's daily life into computerized data, thus enabling actors that have adequate resources to carry out surveillance on an unprecedented scale.

It is understood that all three elements—popular online platforms, locative media and big data—are far from disconnected from each other, but do inseparably interact with each other when it comes to surveillance. One can take popular online platforms as one example to explicate this entanglement. Given the enormous amount of interactions related to and oriented towards popular online platforms across the globe, these platforms are for the most part big data-driven media environments. At the same time, platforms today are increasingly accessed via location-based applications and devices. One can therefore conclude that surveillance as such is a big data endeavor (see Andrejevic & Gates, 2014; Tufekci, 2014). While the intimate relationship between technologies and surveillance goes at least back to evidence-producing tools like photography and telephone (Lauer, 2011), the pervasive embeddedness of media technologies and infrastructures in almost any spectrum of human life has introduced both a qualitative and quantitative difference. This observation echoes the principle that Shoshana Zuboff has convincingly outlined in her seminal writing on the *Age of the Smart Machine*: Everything that can be automated will be automated; everything that can be informated will be informated; every digital application that can be used for surveillance and control will be used for surveillance and control (Zuboff, 1988). To avoid misconceptions about this article's argument, it is important to stress that technology neither emerges out of nowhere nor does it exist in a vacuum (Garfinkel, 2001). More to the point, technology by itself does not practice surveillance; it is the actor—individual, collective, organizational, institutional—using particular technologies and the policies that set the legal frame that condition surveillance. Accordingly, it is important to note that technology also incorporates the potential for empowering citizens, making government transparent, and broadening information access (Howard, 2015). Then again, taking into consideration recent developments, this is not exactly the way things appear to evolve.

To start with, governmental surveillance and the objective to monitor citizens have a long history (Beniger, 1986). Not least since 9/11 and the declaration of the "war on terror", the desire of governmental agencies to monitor every possible communication channel has further intensified. Based on the argument that national security is at risk (Monahan, 2006), governments go as far as trying to make it legally binding for the tech-industry to install backdoors in their software and hardware. For the same apparent reason, some democratic governments even aim to explicitly counter anonymizing and cryptography services. In early 2015, Britain's Prime Minister David Cameron, for example, asked rhetorically: "[I]n our country, do we want to allow a means of communication between people…that we cannot read?". Most people in support of liberal democracy and who believe in the right of free expression would answer this question in the affirmative. Cameron in contrast stated: "My answer to

that question is: No, we must not. The first duty of any government is to keep our country and our people safe" (see Temperton, 2015). Interestingly enough, in his crypto anarchist manifesto Tim May already indicates that "[t]he State will of course try to slow or halt the spread of this technology, citing national security concerns" (May, 1992). Here it is worth noting that "[c]ryptographic techniques have been providing secrecy of message content for thousands of years" (Chaum, 1981, p. 84). Governmental discourses, as David Barnard-Wills (2012) argues in his investigation of surveillance in the United Kingdom, tend to privilege surveillance as a response to social problems. Tellingly, "predictive policing", for example, is turning crime problems into a data problem. Most prominently three-letter agencies across the globe have been busy developing new methods and tactics to gain access to as much valuable information as possible. It is understood that in many cases these agencies collaborate across national boundaries. Interestingly, when it comes to surveillance, the often stark differences between democratic and authoritarian governments become more or less negligible (Gomez, 2004). Considering the concrete practices resulting out of such strategies it can be said that institutionalized politics makes use of surveillance amongst others to monitor, censor, classify, constraining free speech and even to put people in danger worldwide (Schneier, 2015). One might even go as far as to state that the government's control of informational infrastructures that make its territory and population legible has been a feature of the modern state since its birth (Beyer & McKelvey, 2015). All the same, the state is no longer the only or most powerful actor in the field of surveillance. During the 1970s and 1980s, the general assumption was that privacy problems stemmed from the centralized control of personal information held by governments in discrete data banks (Bennett, 2008). Over the past two decades, an increasing amount of personal information has moved into corporate hands (see Whitaker, 1999). More recently, corporations involved in the manufacturing and establishing of MTI have forcefully entered the field of surveillance as they have realized the monetary opportunities of data gathering, sorting, and processing. In fact, with the rise of the data-capture industry, surveillance is becoming more and more privatized and commercialized (see Ball & Snider, 2013). Cell phone providers track their customers' location and know whom you with. In-store and online buying behaviors are constantly documented, and expose if customers are sick, unemployed, or pregnant. E-mail communication and text messaging reveal sexual orientation as well as intimate and casual friendships. Based on estimated income level, interests, and purchase decisions, data broker corporations use surveillance for personalized advertisements, news articles, search results and persuasion (Couldry & Turow, 2014). Scholars refer to these conditions as "surveillance capitalism" (Zuboff, 2015) to underline the substantial scope of contemporary dynamics.

What is critical to note is that government agencies are important secondary beneficiaries of surveillance capitalism as they routinely access and exploit flows of data for their own purpose. In many cases governments directly offload the surveillance responsibility onto private-sector operators, as is the case in telephony and internet providers' legal obligation to store data for a minimum period of time. Overall, the borders between surveillance tactics that rely on government practices and those that rely on corporate activities become more and more obsolete, establishing a symbiotic public-private surveillance partnership. Not only are both camps drawing from the same interface and information, but their practices also augment each other. Again popular online platforms are one prominent example for this tendency as they reveal how individual, institutional, market-based, security and intelligence forms of surveillance co-exist with each other on the same site (Trottier, 2012). Surveillance is often illustrated as both a benefit for the development of Western capitalism and the modern nation-state (Murakami et al., 2006). As the Iranian-Canadian author and blogger Hossein Derakhshan stated after being released from a six years incarceration in Evin prison: "Being watched is something we all eventually have to get used to and live with and, sadly, it has nothing to do with the country of our residence. Ironically enough, states that cooperate with Facebook and Twitter know much more about their citizens than those, like Iran, where the state has a tight grip on the Internet but does not have legal access to social media companies" (Derakhshan, 2015). Corporate and governmental actors alike—each for their very own reasons—develop, maintain and exploit complex infrastructures for collecting, storing, evaluating and putting to use huge amounts of data to ultimately construct an absolute information awareness.

As the Snowden revelations have shown, surveillance often takes place without consent or agreement. At the same time, fitting the notion of participatory surveillance, scholars have stressed that much of surveillance is voluntary. To circumvent legal obstacles, like the Fourth Amendment in the United States and the European Union Data Protection Regulation, the data-capture industry relies on so-called voluntary disclosure of personal data; written into the terms and conditions that users constantly agree to without reading the incomprehensible, small-type, multiple page-long lists of rules. People actively participate in corporate surveillance because it promises convenience and rewards (Andrejevic, 2007). Millions of people wish to have their purchases tracked—and even complain when credit or supermarket affinity card transactions are missed—to accumulate frequent-flyer miles, loyalty

discounts and other forms of "reward". People to a large degree accept the routine collection of their data for the convenience of paying for a meal by credit card, or paying for a toll with an electronic tag mounted on their car (Garfinkel, 2001). As Simson Garfinkel puts is: "It's a simple bargain, albeit a Faustian one" (2001, p. 5). Similarly, people willingly submit to government surveillance because it promises protection (Schneier, 2015). One informative case of continual voluntary self-surveillance is the quantified-self movement. While the earnest and geeky initiation of the "movement" by a group of technology evangelists was seeking better living through personalized control of data, commercial providers have increasingly entered the scene. The emphasis has therefore moved away from control over data towards the minutely quantified, intensively monitored, feedback-driven trajectories of self-improvement of health, diet, and fitness, as well as work habits, sex life, sleep patterns, and so on (Cohen, 2015/forthcoming). In 2014, Kolibree introduced a toothbrush that measures brushing patterns that transmit data to your smartphone to enable self-control as well as allow parents to monitor their children's brushing. Also in 2014, for example, Generali—a German holding company consisting of about 20 insurance companies—introduced a new rate that allows customers to use an application to track their behavior, which transmits data to the insurance company. In return, customers who have a "healthier" lifestyle according to the company's algorithmic evaluation receive special concessions.

Bringing the above-said together, it is reasonable to diagnose a strong tendency towards increased surveillance as well as the intersection of different forms and modes of surveillance. Surveillance—and its attendant apparatus, devices and systems—has become a central dispositif of our time (Bauman & Lyon, 2013; Gane et al., 2007). Today information flows and data monitoring on a mass scale produce a "surveillant assemblage" (Haggerty & Ericson, 2000, pp. 614-615) that predominately serves the interests of powerful entities, both private and public. Accordingly, contemporary tendencies complicate common conceptualizations of surveillance as discipline and control. Linking contemporary surveillance apparatuses with totalitarian political systems has become an oversimplified equation to make. "[T]he surveillance society is better thought of as the outcome of modern organizational practices, businesses, government and the military than as a covert conspiracy" (Murakami et al., 2006, p. 1). Considering the way things have developed over the past decades, it is reasonable to assume that the coming years will see governments and corporations expanding their already effective assemblages of surveillance. Yet, as will be argued in the third section of this article, this does not exclude the fact that other actors like civil society organizations counter-act current tendencies. Before I will explicate this aspect, I will outline why all this actually matters when we think of the existing correlations between MTI and the health of democratic constellations.

3. Privacy and Why It Matters for Democracy at Large

The surveillance strategies and practices discussed previously put into question our deeply rooted sense of privacy. According to critical voices, privacy and datafication simply appear to be incompatible (Lane et al., 2014). Again, it is vital to stress that "privacy-invasive technology does not exist in a vacuum" (Garfinkel, 2001, p. 6). Taking into account the shifting field of actors involved in surveillance, Lane and her colleagues emphasize that data on human beings today are "less often held by organizations with traditional knowledge about how to protect privacy" (Lane et al., 2014, p. xi). The lack of privacy can become life threatening, for example in the case of journalists working in non- or pseudo-democratic countries. More generally, the lack of privacy puts into question the health of democracy *per se*. Aggressive and wide-ranging forms of surveillance preemptively decimate the possibility of a "right to be let alone", as Gabriella Coleman (2014) has argued by referring back to Louis Warren and Samuel Brandeis' (1890) classical conception. Warren and Brandeis, who were among the first to consider the basis of privacy law, defined protection of the private realm as the foundation of (individual) freedom. "Privacy" is by all means a deeply contested phenomenon, as the discourse and concerns about privacy have varied over time and definitions strongly depend on varying interests and agendas. All the same, researchers agree that current and emerging technological developments in data processing pose serious challenges to societies as they destabilize the delicate balance between privacy, security, autonomy and democratic rights.

In this context, a helpful conception of privacy is the approach that privacy is the "claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others" (Westin, 1967, p. 7). Privacy, in other words, is something that every human being is in need of to some degree. To avoid misconception, it is important to note that privacy here is not understood as a reinforcement of liberal individualism, but as a phenomenon critical for societal arrangements as a whole. In other words, the question for the relevance of privacy is framed in social terms and conceptualized as an explicitly political issue. In this context, Julie Cohen's (2012) article on what privacy is for contributes a rich set of arguments to the discussion. As she puts it: "Privacy shelters dynamic, emergent subjectivity from the efforts of commercial and government actors to render individuals and communities fixed, transparent, and predictable. It protects the situated practices of boundary management through which the capacity for self-determination develops"

(Cohen, 2012, p. 1905). Accordingly, for Cohen, "freedom from surveillance, whether public or private, is foundational to the practice of informed and reflective citizenship. Privacy therefore is an indispensable structural feature of liberal democratic political systems" (Cohen, 2012, p. 1905). Conditions of diminished privacy seriously weaken practices of citizenship as "[p]rivacy isn't just about hiding things. It's about self-possession, autonomy, and integrity" (Garfinkel, 2001, p. 4). Seen from this perspective, privacy incursions not only harm individuals' capacity for democratic self-government, but also jeopardize the continuing vitality of political and intellectual culture at large (Cohen, 2012, p. 1906). Tim Berners-Lee, the inventor of the World Wide Web, recently stated that the extension of surveillance powers translate into a "destruction of human rights" (Katz, 2012). Ultimately, as Cohen remarks, "A society that permits the unchecked ascendancy of surveillance infrastructures cannot hope to remain a liberal democracy" (Cohen, 2012, p. 1912). In more practical terms, privacy plays important functions within democratic constellations by promoting, amongst other things, the freedom of association, shielding scholarship and science from unnecessary interference by government, permitting and protecting secret ballots, and by serving as a shield for those actors that operate to keep government accountable (Westin, 1967). All in all, the politics around privacy are critical for the constitution of democracy.

Let me now bring this conception of privacy into dialogue with the earlier-discussed elements concerning the pervasiveness of contemporary MTI that co-determines both people's practice of and the capacity for citizenship. A large portion of participatory MTI today aim to turn people into predictable citizen-consumers whose preferred modes of self determination play out along revenue-generating trajectories (Dean, 2009). Along with the spread of MTI, public and private regimes of surveillance have become an ordinary and mundane process that in many cases narrows critical citizenship and opportunity for it to flourish. "Imbuing our networked information technologies with a different politics will require both the vision to appreciate privacy's dynamism and the will to think creatively about preserving it" (Cohen, 2012, p. 1933). By implication, the widespread—if not even omnipresent—construction of systematic surveillance apparatuses fundamentally changes conceptions of what it means to be "visible" or "in public" (Haggerty & Ericson, 2006). This is particularly highlighted by scholars that explore the ways that exposure within surveillance assemblages affects both identity and resistance (Ball, 2009). Privacy prevents the absolute politicizing of life and protects the ability of actors to develop their identity as well as to voice their concerns freely across media environments.

In summary, the literature on surveillance leaves us with the convincing argument that the quantity and quality of monitoring have changed drastically over the past decades. One not only witnesses increasing surveillance and decreasing privacy, but also that current and emerging surveillance assemblages have fundamentally altered people's experience of and interactions with MTI. It is further reasonable to assume that the lack of privacy is harmful materially, psychologically, socially, and politically. After taking into account the arguments of the above-mentioned scholars, it becomes clear that discussing surveillance is also an examination about the health of democratic constellations. On a more theoretical level, one can distill that as surveillance merges into a corporate/government joint venture and shifts towards a participatory phenomenon, established conceptualizations of surveillance as discipline and control appear obsolete. So far, the array of actors that researchers and journalists alike have focused on are the state and the corporate sector as well as their consolidation (Ball & Snider, 2013; Beniger, 1986). Similarly, the worrying correlations between participatory media and surveillance have also gained considerable scholarly interest (Albrechtslund, 2008; Fuchs et al., 2012). Likewise, writings discussing the societal relevance of whistleblowing and activists' data leaks—both aspects that are connected to privacy—have emerged recently (Brevini et al., 2013). What has been much less noticed and investigated, however, is the role played by actors who counter surveillance.

This is all the more astonishing, considering the fact that due to all-encompassing surveillance, the question asking who is acting "against" surveillance is ever more pressing. In his seminal warning about the steady slide toward the surveillance society, Lyon (2001, pp. 131-135) has argued that sustaining privacy depends less on mechanisms devised and implemented by elites, and more on the extent to which resistance to surveillance practices are enacted through movements and organizations in civil society (see Bennett, 2008). To discuss exactly this issue is the aim of the following section. Throughout the third part of this article, I will therefore present findings from qualitative research that has been conducted on the Chaos Computer Club (CCC)—Europe's largest and one of the world's oldest hacker organizations—from 2011–2014. The data presented in this article is based on 40 face-to-face interviews, numerous participant observations at public gatherings, hackerspaces, hacker conventions and private get-togethers as well as on a media analysis that took into account self-mediation, practices, media coverage and different forms and styles of media access. I aim to make a convincing argument that the CCC counter-acts contemporary surveillance assemblages in two ways: first, by de-constructing existing technology and by supporting, building, maintaining and using alternative media technologies and infrastructures that enable more secure and anonymous communication; and second, by articulating their expertise related to contem-

porary MTI to a wide range of audiences, publics and actors. The hacker organization here stands representatively for a growing network of activists that feel ambivalent and uncomfortable towards the affordances of MTI to be used as a surveillance apparatus.

4. Counter-Acting Surveillance Assemblages

Since the year of its foundation in 1981, the CCC considers itself a non-governmental, non-partisan, and voluntary based organization that is involved in framing media technologies and infrastructures as political phenomena relevant to society at large. The hacker organization explicitly conceptualizes MTI as being embedded in complex power dynamics and act accordingly (Kubitschko, 2015a). After a brief identification stage, the collective registered as a nonprofit organization in 1984 and started to promote their political endeavor of advancing more secure communication and information infrastructures more explicitly. In addition, as a registered lobby group, the Club advocates for more transparency in government, communication as a human right, and free access to communication and information infrastructures for everyone. Colin Bennett (2008) has referred to these kinds of actors as privacy advocates that resist the spread of surveillance and in fact explicitly lists the Chaos Computer Club as a privacy advocacy organization. Ever since the late 1990s, the Club has seen an exponential rise of membership that today figures around 5500 members. To explicate the argument that the hacker organization is acting on indispensable structural features of contemporary democratic constellations, this article will focus on the Club's engagement since the early 2000s. Focusing on a specific time frame also allows us to concentrate on an episode when the three above-mentioned elements—popular online platforms, locative media and big data—were coming to life ever more prominently.

To start with, the CCC, of course, does what one might primarily expect from a hacker organization: hacking. Yet, it is worth emphasizing that hacking can take many different forms. In the context of the research presented here, hacking is understood as critical, creative, reflective and subversive use of technology that allows creating new meanings. This kind of engagement goes back to the early days of the CCC and has intensified over the past decade. One of the recent example is the CCC's so-called Federal Trojan hack in 2011. By disclosing governmental surveillance software that was used (unconstitutionally) by German police forces, the Club initiated a heated political debate about the entanglements of technological developments and state surveillance in Germany. This was two years before the issue of surveillance gained global currency owing to Snowden's revelations about the US National Security Agency (see Möller & Mollen, 2014). Here it is helpful to note that the notion of "data protection", which is derived from the German Datenschutz, entered the vocabulary of European experts in the 1960s and 1970s at about the same time as the notion of informational or data privacy arose. Germany, in other words, can generally be considered a surveillance aware nation. The notion of Informationsselbstbestimmung (informational self-determination), for example, has constitutional status in Germany. This example shows that hacktivism, as hackers' political engagement is generally entitled (see Jordan & Taylor, 2004), does indeed include digital direct action (Coleman, 2014). Hacking in the case of the Federal Trojan means acting as a watchdog of governmental agencies by uncovering surveillance tactics and practices. By deconstructing the abstractness of a given technology—surveillance software in this case—the CCC materializes its formerly unrecognized political quality.

Another principal set of hacker practices to counter-act surveillance assemblages is the CCC's financial, social and technical support of infrastructural projects that establish alternative information and communication environments. That is to say, the CCC aims to contribute to create (more or less) uncontrolled spaces where the regulation of the state and the interests of corporations cannot intrude. Developing anonymous communication spaces for citizens has been a project deeply embedded in hacker cultures for some time. The reasons and ideologies of so-called crypto-warriors, for example, differ, but they align in the desire and development of tools that might ensure to enhance privacy (see Greenberg, 2012). In practice, this means that besides critically engaging with technological artifacts the CCC puts a lot of effort into building, supporting and maintaining alternative infrastructures that enable more secure and anonymous ways of communicating outside the realm of data-hungry, profit-oriented assemblages. During the 2008 Beijing Olympics, for example, the Club provided a manual and matching tools enabling journalists and other interested users to circumvent online censorship and surveillance by allowing people free access to information and communication. At the time of research, the hacker organization was operating five Tor servers and was running one of the most used XMPP servers in the world. The Onion Router (Tor) is an overlay network that has its roots David Chaum's (1981) notion of mix networks and is best considered a privacy enhancing technology. More concretely, it is a client software that enhances online anonymity by directing internet traffic through a volunteer network of special-purpose servers scattered around the globe. The Extensible Messaging and Presence Protocol (XMPP), formerly known as Jabber, is an open technology that includes applications like instant messaging, multi-party chat, voice and video calls. "The right to privacy includes the right to anonymity. The only way to protect this right is to exercise it" (Garfinkel, 2001, p. 172). The two systems are designed to protect people's anonymity while browsing

the internet and to conceal information from unwanted listeners. The design of Tor and XMPP makes it difficult—and potentially even impossible—for governments to seize the content or to eavesdrop on the interactions. It is important to mention that Tor and XMPP might be considered alternative MTIs, but this does not necessarily imply that they are autonomous in an absolute sense, as they still depend on the commercial internet backbone like cables and internet exchange points. At the same time, these are initiatives that constitute serious alternatives to existing profit-driven online services highlighting that cryptography can be a powerful tool for controlling the unwanted spread of personalized information. The Club's aim is to set limits on surveillance assemblages by making anonymous access as the standard mode of operation across the network's architecture.

Tor is amongst others widely used by journalists and human rights activists who feel the need to conceal their identity due to the drastic penalties that their publications might imply in their home country. Similarly, most aspects of whistleblowing today would be unimaginable without anonymizing services. Encryption is an effective way of avoiding feeding surveillance assemblages with data. Some cryptography enthusiasts go as far as arguing that the technology is a silver bullet for achieving universal privacy, solving virtually all of the problems posed by contemporary surveillance assemblages. Tim May explains in his manifesto, which he read at the first cypherpunk founding meeting in 1992 in Silicon Valley, and later posted to the group's electronic mailing list: "Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner" (May, 1992). According to May, "crypto anarchy" would, among other things, "alter completely the nature of government regulation,…the ability to keep information secret, and will even alter the nature of trust and reputation" (May, 1992). Yet, it is important to note that cryptography does not necessarily protect privacy, but also protects information (Garfinkel, 2001). What cryptography does in the first place is to guarantee the confidentiality of a given transmission, which is why it is widely used in online banking and other confidential transactions today. Nonetheless, when it comes to people's day-to-day communication and interactions across media environments, encryption is far from being a mass phenomenon. It requires the use of specific services and precautions on the side of the users to avoid accidentally disclosing their true identity. So, this article is not trying to argue that cryptography is the single best or only tool to counter surveillance. All the same, creating, supporting and maintaining alternative infrastructures that enable more secure and private communication means to establish conditions under which ideas can be expressed, exchanged and circulated in new ways. The examples of Tor and XMPP also underline the notion that hacking is best conceptualized as critical, creative, reflective and subversive use of technology that allows creating new meanings. In other words, the hacker organization's practices related to technology demonstrate a constructive way of countering surveillance. By doing this, the CCC is part of a global network of activists that enable a large variety of people to act with and through more secure MTI.

To expand on this line of thought, it is also interesting to note that CCC's engagement in relation to encryption and anonymizing services is double-sided. On the one hand, members use alternative technologies and infrastructures for inward-oriented communication. Since many activities—like the above-mentioned Federal Trojan hack—need to be coordinated and take place "in secrecy", the Club cannot rely on commercial platforms or other readily accessible services. From this perspective, privacy is fundamental for the Club to practice their political activities. On the other hand, the CCC brings its idea of free and secure communication to life through developing, supporting and maintaining the mentioned alternatives for the larger public. Tor and XMPP enable people to exercise anonymity and to handle data flows about themselves. Surveillance might indeed be "structurally asymmetrical" (Andrejevic & Gates, 2014, p. 192) as it is generally available only to actors with access to and control over data collection, data analysis, and database management. All the same, as the case of the CCC underlines, there are efforts to consciously and purposefully advance the cause of privacy protection. Accordingly, by acting on digital self-determination and the right to informational privacy the hacker organization is co-determining the balance of privacy, security, autonomy and democratic rights. The Club acts on creating what Warren and Brandeis (1890) called a "right of privacy" and—in many ways echoing the belief of the two Boston lawyers—refuses to believe that privacy has to die for technology to flourish. As a side effect, so to say, the case study presented in this article shows the human face of technology as it explicitly demonstrates that not machines but individual and collective human actors establish and maintain particular technologies. While the over-whelming majority of contemporary media environments is set up to gather, collect and manage big data, the CCC supports, builds, maintains and uses alternative media technologies and infrastructures that are set up to respect privacy and to honor autonomy. The initiatives that Club members originate and encourage are "interstitial spaces within information processing practices" (Cohen, 2012, p. 1931) that provide "breathing room for personal boundary management" (Cohen, 2012, p. 1932) outside the realm of routine surveillance. Acting on surveillance assemblages therefore is based on critical, creative, reflective and subversive engagements with technology

that allow creating new meanings.

Taken together what has been outlined so far, the Club's modes of engagement with MTI can be considered largely technical; which is to say that they require a high level of expertise (skills, knowledge and experience) related to technology *per se* (Kubitschko, 2015b). The hackers' contestation of surveillance assemblages, however, goes beyond "activism gone electronic" (Jordan & Taylor, 2004, p. 1), since CCC members also articulate their expertise related to contemporary MTI to a wide range of audiences, publics and actors. They do so by means of public gatherings, self-mediation, coverage by mainstream media outlets as well as by interacting with institutional politics. Ever since the early 1980s the CCC has organized public gatherings like the annual Chaos Communication Congress, which today attracts more than 6000 visitors. Self-mediation practices include running individual websites and personal blogs, creating radio shows and podcasts, as well as posting their views on popular online platform accounts. At the same time, mainstream media not only increasingly cover the Club's activities but also grant individual members—in particular the organization's spokespersons—access to their outlets. Articulating their expertise across media environments not only gives the CCC a voice that is heard by a large number of people, it also enables the hackers to raise awareness and spread knowledge related to surveillance and other related issues where politics and technology collide. This facet of articulation is particularly important because being able to act on a given issue first of all preconditions that one is aware of the existence and relevance of the issue at hand. Spreading awareness and knowledge, in other words, is a precondition to enable other people's engagement. In addition to interacting with different audiences and publics, the hackers also carry their standpoint to the realm of traditional centers of power through advising senior politicians, legislators and the constitutional court in Germany. At the same time, articulation also includes legal measures. In 2014, together with the International League of Human Rights, the CCC filed criminal complaints against the German Government for its violation of the right to privacy and obstruction of justice by bearing and cooperating with the electronic surveillance of German citizens by foreign secret services. As matters stand, the court proceeding is still taking place. No matter what the actual outcome will be, the complaint raised the public's attention towards governmental surveillance practices. In fact, making their voice heard in the domain of institutionalized politics and gaining recognition of mainstream media outlets are two dynamics that perpetuate each other in interesting ways.

In the case of the CCC, acting on the notion of privacy does not only refer to doing "stuff" with technology but also the ability to actively deal with both the functions and effects of technology. Put in more concrete terms, the Club is counter-acting surveillance assemblages through direct digital action—de-constructing existing technology and supporting, building, maintaining and using alternative media technologies and infrastructures—as well as publicly thematizing and problematizing the issue. By merging technically oriented operations and discursive activities, the hacker organization brings forward a twofold strategy: On the one hand, the hackers open up the possibility for people to use privacy enhancing technology, and on the other hand, the CCC spreads awareness and knowledge related to surveillance and privacy. Instead of exclusively relying on cryptography and the science of secret communication, the Club practices a form of activism that acknowledges the relevance of counter-acting surveillance assemblages on different layers. Accordingly, in addition to co-creating interstitial spaces for personal boundary management within information and communication landscapes (Cohen, 2012), the hacker organization also takes part in shaping discursive spaces that establish exchanges of knowledge, flows of information and new levels of awareness. Taken together, this demonstrates that the CCC's interventions in the domains of technology can therefore be conceptualized as interventions in social and political domains.

5. Conclusions

Following the quasi-omnipresent spread of media technologies and infrastructures, surveillance has turned into a mundane practice enacted by a wide range of entities. The approach taken in this article is not to discuss surveillance *per se*, but instead to examine how one of the world's largest (and Europe's oldest) hacker organizations is countering contemporary surveillance assemblages. To do so, I have first illuminated the correlations between online platforms, locative media and big data—three elements that have lastingly influenced the way people experience surveillance and the way surveillance is practiced. Subsequently, the article has explicated the growing intersection of governmental and private-sector efforts related to surveillance. Taking these expanding assemblages of surveillance (see Haggerty & Ericson, 2000) as a starting point of discussion, the line of argumentation followed Cohen's concept that "freedom from surveillance, whether public or private, is foundational to the practice of informed and reflective citizenship" (Cohen, 2012, p. 1905). By presenting qualitative research on the Chaos Computer Club, the article illustrates the ways in which the hacker organization is acting on "an indispensable structural feature of liberal democratic political systems" (Cohen, 2012, p. 1905). More concretely, it has made clear that counter-acting surveillance assemblages and establishing new regimes of privacy is taking place through bringing together direct digital action and different forms of articulation. That is

to say, the Club deconstructs existing technology as well as supports, builds, maintains and uses alternative media technologies and infrastructures. At the same time, CCC members also spread knowledge and create awareness towards issues related to surveillance and privacy by articulating their "technical" expertise to a wide range of audiences, publics and actors. Accordingly, it is argued that hacker organizations like the CCC provide an exemplary case study for highlighting the efforts of civil society organizations to counter-act contemporary surveillance assemblages that infiltrate people's everyday-life. Following the reasoning that privacy is critical for democratic citizenship to flourish, the Club's engagement can be considered a contribution to the formation of indispensable structural features of contemporary democratic constellations.

Acknowledgments

The author would like to thank the highly valuable feedback provided by the reviewers of this article. The research presented in this article was made possible by a scholarship from Goldsmiths' Media and Communication Department and the University of Bremen's Creative Unit "Communicative Figurations" (funded within the frame of the Excellence Initiative by the German Federal and State Governments). I would also like to thank Corey Schultz at the University of Southampton for improving the readability of this article.

Conflict of Interests

The author declares no conflict of interests.

References

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*, *13*(3).

Andrejevic, M. (2007). *iSpy: Surveillance and power in the interactive era*. Lawrence: University Press of Kansas.

Andrejevic, M., & Gates, K. (2014). Big data surveillance: Introduction. *Surveillance & Society*, *12*(2), 185-196.

Ball, K. (2009). Exposure: Exploring the subject of surveillance. *Information, Communication & Society*, *12*(5), 639-657.

Ball, K., & Snider, L. (2013). *The surveillance-industrial complex: A political economy of surveillance*. New York: Routledge.

Barnard-Wills, D. (2012). *Surveillance and identity: Discourse, subjectivity and the state*. Aldershot: Ashgate.

Bauman, Z., & Lyon, D. (2013). *Liquid surveillance*. Cambridge: Polity.

Beer, D. (2009). Power through the algorithm? Participatory web cultures and the technological unconscious. *New Media & Society*, *11*(6), 985-1002.

Beniger, J. (1986). *The control revolution: Technological and economic origins of the information society*. Cambridge: Harvard University Press.

Bennett, C. (2008). *The privacy advocates: Resisting the spread of surveillance*. Cambridge: MIT Press.

Beyer, J., & McKelvey, F. (2015). You are not welcome among us: Pirates and the State. *International Journal of Communication*, *9*, 890-908.

Brevini, B., Hintz, A., & McCurdy, P. (2013). *Beyond WikiLeaks: Implications for the future of communications, journalism and society*. London: Palgrave Macmillan.

Bucher, T. (2012). Want to be on the top? Algorithmic power and the threat of invisibility on Facebook. *New Media & Society*, *14*(7), 1164-1180.

Chaum, D. L. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, *24*(2), 84-88.

Cohen, J. (2012). What privacy is for. *Harvard Law Review*, *126*(7), 1904-1933.

Cohen, J. (2015/forthcoming). The surveillance-innovation complex: The irony of the participatory turn. In D. Barney, G. Coleman, C. Ross, J. Sterne, & T. Tembeck (Eds.), *The participatory condition*. Minneapolis: University of Minnesota Press.

Coleman, G. (2014). *Hacker, hoaxer, whistleblower, spy: The many faces of anonymous*. London: Verso.

Couldry, N. (2012). *Media, society, world: Social theory and digital media practice*. Cambridge: Polity.

Couldry, N., & Turow, J. (2014). Advertising, big data and the clearance of the public realm. *International Journal of Communication*, *8*, 1710-1726.

Dean, J. (2009). *Democracy and other neoliberal fantasies: Communicative capitalism and left politics*. Durham: Duke University Press.

Derakhshan, H. (2015, July 14). The web we have to save. *Medium*. Retrieved from https://medium.com/matter/the-web-we-have-to-save-2eb1fe15a426

Fuchs, C., Boersma, K., & Albrechtslund, A. (2012). *Internet and surveillance: The challenges of web 2.0 and social media*. London: Routledge.

Gane, N., Venn, C., & Hand, M. (2007). Ubiquitous surveillance: Interview with Katherine Hayles. *Theory, Culture & Society*, *24*(7–8), 349-358.

Garfinkel, S. (2001). *Database nation: The death of privacy in the 21st century*. Cambridge, MA: O'Reilly.

Gillespie, T. (2010). The politics of "platforms". *New Media & Society*, *12*(3), 347-364.

Gomez, J. (2004). Dumbing down democracy: Trends in internet regulation, surveillance and control in Asia. *Pacific Journalism Review*, *10*(2), 130-150.

Graham, S. (2004). *The cybercities reader*. London: Routledge.

Greenberg, A. (2012). *This machine kills secrets: How WikiLeakers, Cyberphunks, and Hacktivists aim to free the world's information*. New York: Dutton Adult.

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

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

Hepp, A. (2012). *Cultures of mediatization*. Cambridge: Polity.

Hjorth, L. (2013). Relocating the mobile: A case study of locative media in Seoul, South Korea. *Convergence*, *19*(2), 1-13.

Howard, P. (2015). *Pax Technica: How the Internet of things may set us free or lock us up*. New Haven: Yale University Press.

Jordan, T., & Taylor, P. (2004). *Hacktivism and cyberwars: Rebels with a cause?* New York: Routledge.

Katz, I. (2012, April 17). Tim Berners-Lee urges government to stop the snooping bill. *The Guardian*. Retrieved from theguardian.com/technology/2012/apr/17/tim-berners-lee-monitoring-internet

Koskela, H. (2000). "The gaze without eyes": Video-surveillance and the changing nature of urban space. *Progress in Human Geography*, *24*(2), 243-265.

Kubitschko, S. (2015a). Hacking politics: Civic struggles to politicize technologies. In E. Gordon & P. Mihailidis (Eds.), *The civic media reader*. Cambridge: MIT Press.

Kubitschko, S. (2015b). Hackers' media practices: Demonstrating and articulating expertise as interlocking arrangements. *Convergence*, *21*(3), 388-402.

Lane, J., Stodden, V., Bender, S., & Nissenbaum, H. (2014). Editors' introduction. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, big data, and the public good: Frameworks for engagement* (pp. ix–xvi). Cambridge: Cambridge University Press.

Lauer, J. (2011). Surveillance history and the history of new media: An evidential paradigm. *New Media & Society*, *14*(4), 566-582.

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Philadelphia: Open University.

May, T. (1992, November 22). The crypto anarchist manifesto [Electronic mailing list message]. Retrieved from http://www.activism.net/cypherpunk/crypto-anarchy.html

Möller, J., & Mollen, A. (2014). *The NSA in the German quality press*. Paper presented at Multi-method-designs in Transnational and Transcultural Comparative Research Workshop, Bremen.

Monahan, T. (2006). *Surveillance and security: Technological politics and power in everyday life*. New York: Routledge.

Murakami, D., Ball, K., Lyon, D., Raab, C., Graham, S., & Norris, C. (2006). *A report on the surveillance society. Report for the UK Information Commissioner's Office.* Wilmslow: Surveillance Studies Network.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Cambridge: Harvard University Press.

Rosenberg, J. (1969). *The death of privacy*. New York: Random House.

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. New York: W.W. Norton.

Schwartz, R., & Halegoua, G. (2014). The spatial self: Location-based identity performance on social media. *New Media & Society*, online first.

Temperton, J. (2015, July 15). No U-turn: David Cameron still wants to break encryption. *Wired*. Retrieved from http://www.wired.co.uk/news/archive/2015-2007/2015/cameron-ban-encryption-u-turn

Trottier, D. (2012). *Social media as surveillance: Rethinking visibility in a converging world*. Aldershot: Ashgate.

Tufekci, Z. (2014). Engineering the public: Big data, surveillance and computational politics. *First Monday*, *19*(7).

Uldam, J. (2014). Corporate management of visibility and the fantasy of the post-political: Social media and surveillance. *New Media & Society*, online first.

Van Dijck, J. (2013). *The culture of connectivity: A critical history of social media*. Oxford: Oxford University Press.

Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193-220.

Westin, A. (1967). *Privacy and freedom*. New York: Atheneum.

Whitaker, R. (1999). *The end of privacy: How total surveillance is becoming a reality*. New York: The New Press.

Zuboff, S. (1988). *In the age of the smart machine: The future of work and power*. New York: Basic Books.

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

About the Author

Dr. Sebastian Kubitschko

Sebastian Kubitschko is a post-doctoral researcher at the Centre for Media, Communication and Information Research (ZeMKI), University of Bremen, where he is a member of the interdisciplinary Communicative Figurations network. His research focus is on how hacker organizations gain legitimacy and the ways they politicize contemporary technology. Sebastian holds a PhD from Goldsmiths, University of London, and is the European Editor of Arena Magazine. Together with Anne Kaun he is currently editing a volume on emerging methods in media and communication research.