Collaborative Chaos: Symbiotic Physical and Virtual Resistance to Pervasive Surveillance

GUILLAUME ROCHEFORT

Thesis submitted to the University of Ottawa in partial fulfillment of the requirements for the degree of Master of Arts in Communication

Department of Communication

Faculty of Arts

University of Ottawa

ABSTRACT

The scale of modern surveillance and the debate surrounding its nature have become expansively complex. Consequently, the field of communication and surveillance studies represent a critical area of scholarship with interwoven academic, policy and social implications. This thesis, a critical ideological study of modern surveillance founded upon an empirical study, draws on participant observation, militant ethnography and semi-structured interviews as research methods. From a participant insider perspective, it explores and interprets the experiences, meanings, and views of counter-surveillance actors targeted by surveillance based on participant observation and militant ethnography conducted during the 2017 Chaos Communication Congress in Leipzig and the 2019 Chaos Communication Camp in Mildenberg, Germany. Drawing on Jeffrey Juris' militant ethnography and **based on the participants' own experiences in resisting modern surveillance,** I focus on the lessons learned from those belonging to the third-wave of privacy activism. Through their personal experiences, this research reveals control strategies, lessons learned and views of privacy activists, hacktivists and civic-hackers on the state of modern surveillance. This thesis concludes that the current symbiotic nature of the state-corporate surveillance and disinformation nexus means any legislative solution to be unlikely.

ACKNOWLEDGEMENTS

To write a thesis is together a co-operative and solitary experience. For this reason, thanking those who have there for you along your journey becomes essential when reaching destination. Hence, I want to thank my thesis supervisor, Prof. Patrick McCurdy for his patience, guidance and invaluable input throughout this project. The same goes for Prof. Conway and Prof. Dubois, especially for their time and input during my research. To Prof. Amir Attaran, whose passion and dedication have become source of inspiration. Special thanks to Prof. Jeffrey Monaghan and the University of Carleton for the research grant, but more importantly to you Jeff for your encouragements and counsel at the beginning of the project.

I want to especially thank my father, Jean-Marc, for the eternal support and help throughout the entirety of my academic studies. To my brother, Fred, for his support and aid in times of need and being the best brother one could possibly hope to have. To my mother, Donate, an eternal source of inspiration, tenacity, and counsel in time of needs. To my friends Bryan, Jay, Peter, Darby and Julia; friendships which I have certainly too often neglected because of time and distance during this project. Thank you.

I would also like to thank the many activists who have helped make this project a reality. Special mentions to Nina, Joe, McFly and Pat for all your time and generosity along the way. Same goes for monkey, rof, kitt, tara and sylvian. Finally, I also wish to extend my special thanks to both Gabriella Coleman and Maureen Webb for their words of wisdom and encouragement.

CONTENTS

Chapter 1: Introduction

> *It is just when people are all engaged in snooping on themselves and one another that they become anaesthetized to the whole process [...] As information itself becomes the largest business in the world, data banks know more about individual people than the people do themselves. The more the data banks record about each one of us, the less we exist.*
>
> —Marshall McLuhan, 1970, p. 12

More than twenty years ago during rapid shifts within the information and communication technology (ICT) sectors, surveillance researcher Simon Garfinkel (2000a) warned against the Faustian bargain between privacy and modernity (2000a, p. 5). A false dilemma which in his view proposed that for technological modernity to be embraced, the sacrifice of privacy was necessary. A position wrongly presented as two mutually exclusive options, Garfinkel believed a well-informed populace backed by sound government regulations could embrace modern technology and rein-in the free-market's appetite for people's private information. Moreover, Garfinkel believed modernity could be achieved without the need to sacrifice individual and collective-based privacy in the same way that modernity could be embraced without the destruction of the environment.

Two decades later, the Faustian bargain as described by Garfinkel turned out to be and as predicted, a rip-off. For convenience, we have embraced technological modernity at the cost of collective and individual privacy rights without the benefit provided by informed consent. Indeed, the rapid changes witnessed in the ICT sectors have fundamentally altered how we socialize, consume entertainment and engage with public institutions (Couldry, 2012) through a process of mediatization. Defined as the consequence of media on the construction of sociocultural realities, this process has now become a contemporary feature of today's societies (Krotz, 2009) by taking hold unto our collective consciousness (Couldry & Hepp, 2013, p. 196). A process fuelled by the blurring

of the line separating state and corporate surveillance and at the cost of both collective and individual privacy rights. While not all changes influenced by mediatization are by themselves inherently negative, these transformations have nonetheless profoundly altered societies by turning, as predicted, the environment we live in into one big "electronic fishbowl" (Garfinkel, 2000b).

To the extent that we may all belong to the same electronic fishbowl, not everyone (in part due to their unique experiences) share the same insights on the matter. The meta-process attached to the mediatized world we live today means that those found within the nexus of tension between power and counter-power struggles also have unique perspectives worthy of analysis to understand and expand on current theories in the study of surveillance. For example, privacy activists, which include hacktivists and counter-surveillance actors, certainly have different perspectives to share worthy of analysis. As such in this thesis, I argue how the personal experiences of privacy activists with both surveillance and mediatized activism (Krotz, 2009; Mehrabov, 2016) can provide us with an exclusive look into the matter and perhaps help us better understand what the future may hold for the rest of us.

To paraphrase McLuhan (1968) who in the sixties commented on the growing and collective obliviousness of environments created by the technologies surrounding us, the proverbial fish does not know water until it is out of the fishbowl. Most of do indeed live in an opaque sea of surveillance[1], although it is possible to trace it. We know it is there because the engine which generates the surveillance systems resting behind the state were profoundly perturbed by the courageous actions of privacy activists, hacktivists, whistle-blowers, academics and the journalists covering them. Combined, the efforts of these counter-surveillance actors have helped the public trace the previously invisible dynamics of standing water. Like an ink marker dropped into the system, counter-

1 See: 30c3: Seeing The Secret State: Six Landscapes https://www.youtube.com/watch?v=e4woeUONee8

surveillance actors have enabled a better understanding of modern surveillance by allowing the public to trace the movements of the state-corporate partnerships behind modern surveillance.

Maybe in part due to its ubiquity, modern surveillance — despite its participatory and non-participatory nature — remains until now a powerful tool for control. While complex, these mechanisms can be better understood through the lens of “surveillance realism” (Dencik and Cable, 2017). This concept, defined as the feeling of powerlessness felt when individually confronted with the reality of pervasive surveillance (2017, p. 763-781), explains how we tend to rationalize its existence in a multitude of ways, either for “reward” (Garfinkel, 2000a), “convenience” (Andrejevic, 2007) and “protection” (Schneier, 2015). As a result, surveillance has in effect become an omnipresent and central aspect of our lives (Bauman & Lyon, 2013; Gane et al., 2007). So much so that ‘opting-out’ is now even more of a “wishful fantasy” (Brunton & Nissembaum, 2019).

Yet, due to the omnipresence of surveillance today, the sole act of researching surveillance is also for researchers harder to achieve (Widener, 2016). Not only because access to privacy activists and counter-surveillance actors with such experiences can be difficult to get (Widener, 2016), but also because doing so responsibly also requires an extra layer of competence related to security and privacy applications. This includes an awareness of best practices when it comes to information security for the researcher to ensure the privacy and anonymity of participants who sometimes may still be under active surveillance. Although those difficulties can complicate access to research, they can as I will argue throughout this thesis be alleviated using militant ethnography as a research method.

Thus, for this thesis, I have drawn on militant ethnography as the main research method to develop an ideological critique of modern surveillance going beyond

contemporary views found within the literature in surveillance studies. A research method developed by Jeffrey Juris (2007, 2008) during his research with anti-authoritarian movements, it is in the context of this study applied as a mechanism to better understand the meanings and experiences of counter-surveillance actors and privacy activists. I argue that using this method can help alleviate the methodological pitfalls and challenges associated with insider participant observation (Uldam and McCurdy, 2013). From the perspective of a participant-insider, this study thus focuses on the experiences of counter-surveillance actors as a case study to inform our academic and theoretical knowledge of modern surveillance. This research is thus supported by a two-year militant ethnographic study (See **Appendix 1 & 2**) involving on site research at hacker conferences and camps related to the Chaos Computer Club (CCC), Europe's largest gathering of hackers (Bennett, 2008).

More specifically, this research seeks to deepen our understanding of the perspectives, personal views and experiences of counter-surveillance actors from an insider and participant-observer perspective. It is supported by semi-structured interviews conducted with participants belonging to converging assemblies of the CCC. From the sharing of their experiences, I seek to discover the best practices, lessons learned and control strategies from the testimonies of counter-surveillance actors interviewed for this study. Moreover, through militant ethnography as the main method of research, I seek to offer a differing perspective on the nature of modern surveillance from what is found within the contemporary literature on surveillance. The analysis of these tensions, I believe, has the capacity to increase our understanding of counter-power resistance but also, about the nature of the symbiotic relationship between public and private surveillance.

By seeking to answer questions on counter-surveillance actors and their experiences, we can learn to better understand the phenomenon within the context of

liberal societies and the rise of networked authoritarianism within an increasingly mediatized world. While previous research focused on the societal importance of whistle-blowers and activists (Brevini et al., 2013), including the role of hackers and privacy activists in countering surveillance and promoting privacy (Kubitschko, 2015; Greenberg 2012; Newman, 2009), we still lack a more detailed understanding behind the meanings and lessons produced out of the experiences of counter-surveillance actors who have resisted surveillance. More specifically, from those actors belonging to the so-called third-wave of privacy activism, beginning with the rise of Anonymous in 2008.

Drawing on Jeffrey Juris' (2005b; 2007) method of militant ethnography as its main method of research, this research combines activism and academia while seeking to preserve academic standards of research. Contrary to other methods of research, militant ethnography primarily seeks to "help activists produce their own analyses and commentary on their space by producing politically relevant work to their movement" (Apoifis, 2017, p.2). Following this view, this thesis looks at the experiences of counter-surveillance actors from the perspective of an insider participant. While the means of repression by the state to suppress traditional counter-power movements are numerous and well documented (Kinsman, Buse & Steedman, 2000; Lubbers, 2012; Choudry, 2019), another area of research has yet to receive the attention it deserves. For instance, how control measures by the state are applied against much more splintered and seemingly leaderless internet-based movements threatening state-corporate surveillance partnerships.

Mainly, I seek to understand some of the best practices developed by hacktivists, privacy activists and other human rights defenders against targeted surveillance but also about its nature in light of their experiences. What control mechanisms can be learned from their experiences? What are their views about modern surveillance and how can we define it in light of increasing corporate and state powers?

1.1 Research Questions

As previously stated, this thesis is backed by qualitative semi-structured interviews taken from a two years ethnographic study. This includes interviews conducted with participants connected to the Chaos Computer Club, one of the oldest hacker organization in the world. This thesis will attempt to provide the necessary perspectives to help answer the following research questions:

- (RQ1) What are the experiences of counter-surveillance actors in resisting modern surveillance?
- (RQ2) What types of positive lessons and views regarding the state of modern surveillance can be gleaned from their experiences?
- (RQ3) How do their experiences diverge from or relate to known concepts within the literature within the fields of media and surveillance studies?

1.2 Thesis Outline

The following chapter proposes a theoretical framework which I believe will be helpful to analyze and understand modern surveillance. It does so through the juxtaposition of mainstream narratives framing the nature of modern surveillance against recent academic research within the fields of surveillance and communication studies. Firstly, the following chapter's seeks to fill a perceived gap between mainstream definitions of surveillance and recent academic studies touching on the relationship between modern surveillance, privacy and power. This framework will subsequently be supported by a two-parts literature reviews in which modern surveillance is defined a symbiotic relationship between governments and corporations (Ball & Snider, 2013; Trottier & Lyon, 2012). This will form the basis of the argument needed to conceptualize the societal consequences of surveillance based on a collective understanding of privacy as it relates to notions of power and counter-power (Nehf, 2003; Cohen, 2012). A two-parts review of the literature

will then serve as the foundations to understand the perspectives and experiences gathered from privacy activists during the ethnographic portion of this study. These perspectives accumulated during online and offline field-work with privacy activists and counter-surveillance actors will be analyzed in light of the theoretical position taken in the first half of this thesis.

Chapter 2: Theoretical Framework

The technology needed for them [The Right] to establish the total surveillance upon which to base their moral totalism is already available. Fear will increase the likelihood of that technology's use and the probability of right-wing forces being in power to use it. It is, therefore, in their interests to confine as many of us as they can to our cultural and geographic enclaves. Is this what we want?

-John Fiske, 1994, p. 253[2]

Privacy experts, whistleblowers and journalists have in recent years raised the alarm against the direction undertaken by liberal democracies with surveillance technologies. For many, time may have already run out to avoid the worst negative outcomes of surveillance against individual and collective privacy rights. While we cannot deny the repercussions behind the negative effects of surveillance on societies, a gap in understanding still exists regarding the nature and role of the state and corporations behind modern surveillance. Since the Snowden revelations, several publications have already and adeptly reviewed the current situation in the fight against surveillance from both a legal and social perspective (Gallagher, 2018; Green, 2019; Zaid, 2018). On this, Gallagher (2018) provides a constructed timeline of the legal and societal ramifications of the fight against surveillance, including the many hurdles facing privacy movements after the Snowden revelations in 2012.

One such challenge includes the perceived shift in public attitude toward surveillance and who bears responsibility for the threat posed by surveillance against privacy. For some observers, public scrutiny seemed to have moved away from the state and closer to corporate behaviours (Zaid, 2018). Named as possible causes for this shift are the scandals involving Facebook and the now defunct data-mining firm Cambridge Analytica (Popielec, 2019). For whistle-blower attorney Mark Zaid (2018), the shift in

2 See: https://henryjenkins.org/2010/06/john_fiske_now_and_the_future.html

scrutiny from government toward corporate behaviours can be seen especially in the public's growing interest in "corporate mishandling and misuse of personal data" (Zaid, 2018). However, the Snowden revelations did demonstrate tacit or implicit collaboration between technology corporations and intelligence agencies through the facilitation of surveillance of their own users for the state. A collaboration which for some became the central theme of the Snowden revelations. To quote Noam Chomsky:

> Snowden's great revelation was that there's no wall between Google and Amazon and the government. In fact, we now know Amazon is developing the cloud to keep all this information for the government, for the CIA, for the intelligence agencies.[3]

Ultimately, Snowden demonstrated how there was no such thing as a separation between corporate and state surveillance. More precisely because the surveillance of each build on and augment each-other and this within a state of "lawful illegality" (Austin, 2014). A careful examination of these relationships may allow us to synthesize the tensions between these shifts in perspective and consequently, allow us to better understand the nature of modern surveillance.

After the release of the Snowden (2019) memoirs, researcher Matthew Green (2019) — a cryptographer and professor at Johns Hopkins University — reviewed what he saw as the main lessons gleaned from the Snowden releases. This includes some of the most indiscriminate programs and technical concerns revealed by the whistle-blower then. As Green (2019) reminds us, the story behind the Snowden revelations can difficulty be told via a simple narrative. A fair amount of context is necessary to grasp its implications and as such, a simple telling of the "raw facts" or simple narrative can hardly do it justice. However, we can improve our understanding of the implications behind the revelations by looking at it from the perspective of a 'before and after' Snowden. While for Green (2019) proving shifts in attitude may not be a simple task, most would certainly agree that Snowden made the reality of state surveillance a more widely acceptable idea. In effect,

3 See: https://www.truthdig.com/articles/noam-chomsky-america-has-built-a-global-dystopia/

mass surveillance became a topic less confined to the realm of academia. As Green (2019) points out: “The idea that governments would conduct large-scale interception of our communications traffic was a point of view that relatively few “normal people” spent time thinking about and mostly confined to security mailing lists and X-Files scripts” (2019, p. 3).

For this reason, Green argues how Snowden’s main contribution has been how the whistle-blower allowed for surveillance concerns to gain ‘respectability’ by becoming part of the mainstream discussion. More specifically, to the point that even “the most paranoid observers were shocked by the sheer scale of what the NSA was actually doing out there” (2019, p. 3). Not as much because of the extent of the reach the agency enjoyed through its spying capabilities but more so because of its potential admittedly limited by a lack of virtual storage space. Such data-sensitive operations included the so-called “Optic Nerve” program in which the NSA and the United Kingdom’s Government Communications Headquarters (GCHQ) collected millions of images from Yahoo! Messenger’s chat streams. As well as the officially named MUSCULAR program, within which the NSA “tapped the internal leased lines used to connect Google and Yahoo datacenters” (Green, 2019). Together, these previously unknown surveillance operations revealed a reach beyond what previously known programs, for example such as PRISM, already allowed. Beyond the reach of these unknown programs, what alarmed some experts became the extent of the cooperation between the NSA and private corporations. For example, the manner by which corporations either did not have the choice to participate when not willingly complicit[4] in the implementation of mass surveillance programs against their customers (Shubber, 2013; Groll, 2016).

Indeed, perhaps the most important Snowden revelation referred to the extent of the state-corporate surveillance relationships, with the state enjoying exclusive access to

4 See: https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

tech companies' data (Ball, 2013). Ultimately, this vast surveillance apparatus seeks to "master the internet" (Senate of Canada, 2006) through "full spectrum dominance" (Munkholm, 2020) of military, economic, business and political activities within cyberspace.

2.1 Surveillance after Snowden

It helps to remember how researchers defined surveillance before and after the Snowden revelations (Bauman et al., 2014). Surveillance researcher David Lyon (2007) once defined surveillance as an external force, or the "focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction" (2007, p. 17). After the Snowden revelations and the Cambridge Analytica (Jamieson, 2018) scandals, Lyon's (2017) definition of surveillance expanded to include the internal and participatory dimension involved with modern surveillance. Including how people "comply with — willingly and wittingly, or not— negotiate, resist, engage with, and, in novel ways, even initiate and desire" (2017, p. 825). Indeed, participatory surveillance became a central focus for scholars after scandals involving the 2016 United States elections and private data by tech companies such as Facebook.

For Cambridge Analytica's whistle-blower Christopher Wylie, democracies have for a time been heading toward the "same direction as China" when it comes to surveillance and privacy: "just because it's not the state doesn't mean that there isn't harmful impacts that could come" (Stankiewicz, 2019). Similarly, human rights groups like Amnesty International (2019) also came out against corporate surveillance, arguing how pervasive surveillance technologies used by companies (such as Facebook and Google) today pose "an unprecedented danger to human rights" (Amnesty, 2019). Although I would agree with the premise, I believe drawing a distinction between corporate and state surveillance to be a moot point. Doing so does not help us to solve or even address the problem behind modern surveillance. As others before me have similarly stated (Kubitschko, 2015,

Doctorow 2020), the extent of the relationship between the state and corporations is such that it has become a symbiotic relationship. In return, this makes any attempt at differentiating between the two quasi meaningless:

> "[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" (Kubitschko, 2015, p. 83).

Surveillance practices committed by corporate and state entities ultimately augment each other, and as a result, the people become squeezed between the influence and power of corporations and the state. The state in this scenario becomes incapable of regulating the corporate sector finding itself in a compromised position. It is either unable or unwilling to enforce regulations which would normally protect the people. This result in corporations and the state having too much to lose in allowing comprehensive privacy regulations to happen, as doing so would cut off access to the power they both derive from the lack of robust privacy protections. Furthermore, enacting proper privacy protections to protect the weak would also mean cutting off the influx of vast quantity of data. Data which both the national security apparatus and the surveillance industrial complex depend on.

A relationship characterized by researchers as one resembling a 'symbiotic public-private surveillance partnership' (Kubitschko, 2015). To borrow a term from political economy, this partnership resembles a renewed form of regulatory-capture, although in this case with a twist. Regulatory-capture, a term originally coined by Nobel laureate and economist George Stigler (1971), describes a form of government failure in which the corruption of an authority or regulatory agency alter normal regulation mechanisms. In this case, these mechanisms become 'captured' or harnessed to serve the interests of a third party as opposed to the public (Bó, 2006). Traditionally, the term invoked issues of environmental governmental regulations within the oil industry (MacLean, 2016). Although

for surveillance theory, I propose that the term can have a useful potential to describe agencies and regulators who become prey to competing influence and interests originating from both within and without government.

In other words, state-corporate surveillance relationships become the product of a regulatory capture by diverging interests from within the state. In this case, the latter's goal takes prominence over the regulating agencies' original mandate to serve the public's interests. From this perspective, modern surveillance is not either related to the state or corporations exclusively, but is instead the product of the state acting as main benefactor and supposed arbitrator of surveillance. Democratic regulations to preserve privacy and protect people's rights cannot happen when the state itself is caught in such a compromised position.

When taking the entirety of observed cases during the Snowden revelations as examples, corporations either do not have the choice or sometimes willingly participate in the implementation of mass surveillance programs (Greenwald, 2014). Although some technology companies, as with Lavabit[5], have demonstrated a desire to resist unlawful government intrusion into their users' privacy, such examples are rare. This inverted regulatory capture means the relationship between states and corporations has become more than just mutually beneficial (Wood et al., 2006; Fuchs & Trottier, 2017). Consequently, the public finds itself unable to realistically defend themselves against state and corporate influences. This uneven can be exemplified in the way corporations wittingly write scripts for the NSA to increase and improve surveillance against their own users[6]. Because of this, drawing a difference between private and public surveillance have somewhat become a moot point. Especially when we consider the way by which data collected by corporations tend to ultimately end up into the hands of the state and this, outside of normal legal frameworks. Thus, when seen from this perspective, one could

5 See: https://www.wired.com/2016/03/lavabit-apple-fbi/
6 See: https://foreignpolicy.com/2016/10/04/how-american-companies-enable-nsa-surveillance/

argue that corporate surveillance is effectively another form of state surveillance. A point made clearer when looking at mainstream debates which followed the Snowden revelations about the nature of modern surveillance.

Earlier, I have argued how concerns about surveillance have shifted away from the role of the state and toward the role of corporate surveillance, especially after the 2016 elections in the United States. As a consequence, some have attempted to separate corporate and government surveillance by putting the blame solely on corporations for the loss of privacy in the western world. One of the problems with this narrative is in its avoidance to mention the role of the state within this symbiotic partnership. Sometimes, the focus on corporation when theorizing surveillance is to differentiate contemporary capitalism to previous forms of capitalism in the past (Kulwin, 2019). Such is the case, for example, with Zuboff's (2015) surveillance capitalism. Here, I advance how this view may prevent us from understanding the nature of contemporary surveillance and power in general but also, how such power is distributed. Just as we did not define surveillance during the reign of the Stasis in Germany based on its economic system, for example by calling it "Surveillance Socialism". Hence, I argue how there is no reason why we should be making an exception for surveillance when it affects liberal democracies based on a capitalist system. Regardless of the economic system in which it operates, surveillance has historically always remained both a tool for power and a control mechanism for the establishment.

In her book, Zuboff (2019) points out how we are today living in an era of surveillance capitalism, one which is strongly pushing us toward new markets within the context of new technologies. No longer should we be repeating the adage "if it is free, you are the product", as this according to Zuboff no longer applies. Instead, Zuboff (2019) underlines rather bluntly how today's 'users' of modern technology are no longer the mere

‘product’ but instead, the ‘abandoned carcass’ derived from “the surplus that is ripped from your life” (Zuboff, 2019). This process, previously advanced in Zuboff’s (2015) other work, is designed to create capital out of the behavioural data surplus it appropriates from the people themselves. A process, which she argues, is not without reminding us of the way capitalism evolved from the industrial age to modern day. This is best exemplified, as Zuboff argues, in the way capitalism previously developed other forms of commodities formerly existing outside the market dynamic, such as the commodification of work into labour.

Most importantly, Zuboff advances how the difference today lies in the manner by which surveillance capitalism exacerbates an already growing asymmetry of power. A “division of learning” between those privy to such information and those who are not (Kofinas, 2019). This asymmetry of knowledge and the power derived from it, as she claims during an interview, is what makes the accumulation of data so valuable today (Kofinas, 2019). However, my view is that while accurately describing a process, this theory is to me reductionist in its analysis of power, especially when considering the symbiotic relationship between state and corporations concerning surveillance.

For Cory Doctorow (2020), the symbiotic relationship at play is thus also a mean of strategic feasibility. As the researcher explains: “the only really affordable and tractable way to conduct mass surveillance on the scale practiced by modern states — both “free” and autocratic states — is to suborn commercial services” (Doctorow, 2020). Indeed, modern surveillance not only suborn commercial services but also its own regulative apparatus. As the state finds itself in a conflict of interests in which it becomes both a regulator and a profiteer of mass surveillance:

> Without Palantir, Amazon, Google, and other major tech contractors, U.S. cops would not be able to spy on Black people, ICE would not be able to manage the caging of children at the U.S. border, and state welfare systems would not be able to purge their rolls by dressing up cruelty as empiricism and claiming that poor and vulnerable people

> are ineligible for assistance. At least some of the states' unwillingness to take meaningful action to curb surveillance should be attributed to this symbiotic relationship. There is no mass state surveillance without mass commercial surveillance. (Doctorow, 2020)

Comparably, in an earlier critique of Zuboff's book, Evgeny Morozov (2019) underlines some conceptual concerns he sees in Zuboff's work. Mostly, in the way the concept in his view lacks "an account of how anonymous power under capitalism operates" (2019, p. 20). To get around this gap, as Morozov (2019) explains, Zuboff attempts to contrast the "instrumentarian power" of surveillance capitalism with those of the "totalitarian power" of dictatorships. Power whom she argues operates with violence and coercion, unlike the former who she writes operates through "means of behavioural modification" (2019, p. 22). While the latter may be true to some extent, we must remember how violence can take difference forms which differ from traditional brutish and physical violence (Fanon, 1960; Zizek, 2008; Antoine 2020). To draw from concepts on violence established within the field of post-colonial research (Antoine, 2020), violence (aside from its more brutish form) can manifest through objective or systematic means.

As Antoine (2020) argues, "what distinguishes violence from non-violence is not always clear" (2020, p. 27). For this reason, researchers must remember to look "beyond the brute and more visible sense of the term" (2020, p. 27). This ambiguity surrounding the expression, as he argues, is what allows for objective or systemic violence to be used by power in a symbolic or systemic fashion. In return, this makes this form of violence more difficult to pinpoint. In this case, surveillance — even when done under the guise of behavioural modification — could be seen a form of violence, herein defined as systemic or objective as argued by Zizek (2008). While not itself defined in Zizek's book, surveillance in this case can be defined as 'systemic' violence, for example as we consider the way that it discriminates based upon race or social class. Furthermore, it also 'objective', in the manner by which surveillance systems also derive their power from

unequal political and economical realities. Within the context of post-colonialism, Antoine (2020) remarks how objective forms of violence can also become harder to discern over-time. The reason given by Antoine (2020) is that its opacity typically stems from “systems and institutions working exactly as they should” (2020, p. 27).

The view I presented early in this chapter to define modern surveillance included both a symbiotic definition and dimension emphasizing the state-corporate symbiotic relationship with mass surveillance. In my view, Zuboff’s concept of surveillance capitalism fails to do so by overly focusing on the corporate side of the issue. Ultimately, drawing a distinction between corporate and state surveillance becomes a moot point once we consider that all corporate surveillance is, ultimately, a form of government surveillance. Surveillance stemming from data collected and enabled by state-corporate partnerships existing outside both public and legislative scrutiny, as the Snowden revelations revealed.

2.3 The Golem

Although the relevance of the nation-state in a globalized world can be said to be declining, the state still possesses monopoly over violence within its borders. As such, it can organize such power against other dissenting groups deemed a threat to its survival. For this reason, looking into activist resistance against the surveillance state, as noted by Choudry (2019), can help academics understand more clearly the nature of modern surveillance. For example, by looking at how modern surveillance remains to this day a tool for social control, for example by “[nipping] dissent in the bud as far as possible” (2019, p. 29).

Firstly and as Radha D’Souza (2019) asserts, it helps to look more deeply at the origins of the surveillance state — with the United States representing its archetypal example — in liberal democracies. This can be done when examining the way those states have over time become governed. In this case, under a model in which “military, security

and surveillance are organized around principles of national security" (2019, p. 30). Doing so he argues allows us to better understand the forces driving such a model of governance. Briefly and as the author states, modern surveillance came as a result of the considerable advancements and inventions achieved in the field of cybernetics after the end of the Second World War. Defined as "the science of command and control of any system, human and non-human, using communication sciences" (2019, p. 32), cybernetics fathered the Information Communication Technologies (ICTs) sector.

More concretely, the technologies behind the data-driven feedback loops connecting machines to humans and humans to machines using a set of desired patterns. For D'Souza (2019), this historical process echoes what the father of cybernetics Norbert Wiener (1948) himself envisioned after the advent of new technologies developed during and after the World War Two. Weiner himself feared that the same technologies used to defeat fascism could one day turn inward to help satisfy the state's addiction to "gadgets of surveillance" even during peace time (D'Souza, 2019, p. 35).

Predictably, after the end of the Second World War, ICTs and algorithms in general grew exponentially and this alongside the rapid increase in emerging networks around the western world. An increase which has led to the overall convergence of media technologies we know today but also, toward our private and collective vulnerability to surveillance systems. As a result, as D'Souza recalls, the "blurred boundaries between public and private power with media corporations, the federal state, foreign relations and the security and intelligence apparatus" (2019, p. 43) expanded. This has led to what D'Souza symbolically refers to as 'The Golem'. More precisely, The Golem as the symbolic intermediary between Hobbes' Leviathan and The People, embodies what I previously defined in this thesis as the symbiotic relationship between state and corporate surveillance.

In Hobbesian terms, the Golem as D'Souza defines it represents "a robotic automatic that shields the Leviathan and transforms the minuscule men and women in the body politic into minuscule subjects" (2019, p. 33). In a sense, the Golem acts as a proxy for the Leviathan. It enables the latter to project its power without suffering from direct political repercussions. It does so by shielding the Leviathan from any association against what may otherwise unnecessarily "unravel the body-politic" (2019, p. 33). Through this lens, the panoptic abilities of communication technologies enabled via 'surveillance capitalism' becomes the symbolic Golem. This allows the Leviathan to remain unattainable while appearing to fulfill its obligations under the social contract by shovelling culpability unto the Golem or in this case, corporations.

Firstly, It is important to understand theoretically why the focus on either corporate or state surveillance individually can be detrimental to our analysis of surveillance. For Christian Fuchs (2015), many surveillance concepts focusing on either corporations or the state can appear to be incomplete by providing only a partial view of the phenomenon and its societal origins. As Fuchs (2010) notes, many concepts in the field of surveillance studies have for a long time attempted to model or explain surveillance and its origins. They have done so however often by failing to ascertain the extent by which the state and corporations have forever acted as the "central actors" behind the rise of the current post-modern surveillance complex (2010, p. 120; citing Gandy, 1993, p. 95; Ogura 2006, p. 272). In his view, it would be difficult to ignore how much the goals of the two have become increasingly intertwined.

Secondly for Fuchs (2015), besides erring toward relativism, many concepts found in the field of surveillance studies lack a proper definition of power. This includes concepts such as 'surveillance assemblages' (Haggerty and Ericson, 2000), in which decentralized systems of surveillance help create 'data doubles' out of diverse data flows; and

‘participatory surveillance’ (Albrechtslund, 2008) or the mutual surveillance exercised through shared-practices on social media platforms whom he argues “downplay the actual repressive power of capitalism and the state” (2015, p. 7). On this, Fuchs (2015) argues how critical researchers looking to avoid similar pitfalls should first trace the origins of today’s public-private surveillance complex by observing the relationship between institutions and technology corporations. The latter which he argues have for a long time worked jointly to implement “totalitarian surveillance systems” (2015, p. 8). Following in on these footsteps, the following chapters will focus on the role of counter-surveillance actors in unveiling relationships between state-corporate surveillance.

2.3 Networked authoritarianism and collective notions of control

Participatory forms of surveillance (Albrechtslund, 2008) or community-based monitoring of other individuals, have become increasingly popular in today’s hyper mediated world. To be clear, participatory surveillance is not always inherently and morally wrong. Sometimes, such as with health surveillance during a pandemic, participatory surveillance can be key to prevent unnecessary deaths using the power of community-based monitoring to prevent the further spread of disease. In other cases, the term is also used to describe an actual phenomenon which we have all become acquainted to thanks to our social media habits. However by itself, participatory surveillance only address the surfacing symptoms of the disease. Such practices, the act of willingly engaging in surveillance are also embedded within a system of surveillance apparatuses. They ought to be understood through the lens of a broader context of societal control. It would be wrong to deny how part of the cultural normalization of surveillance and the capitalization of private data may be done voluntarily. However, there is a parallel to be drawn with what researchers looking into the recent rise of authoritarianism and surveillance in western liberal states have discovered (Hintz & Milan, 2018; Glasius, 2018; Glasius and

Michaelsen, 2018). More precisely, the unintended (or not) consequences of the mechanisms of the modern state and of the surveillance-industrial complex we now find ourselves in (Choudry, 2019).

Drawing on Hintz and Milan's (2018) findings on the origins of authoritarian practices in liberal democracies, we must first look at this inherent tension through an integrated perspective. This includes "both the top-down and the bottom up dimensions" (2018, p. 3944), which brings us closer to an understanding regarding the sharp increase in surveillance practices witnessed across liberal democracies. The latter which is forcing us, according to the authors' view, into a downward spiral helping to erode people's trust in institutions. As a result, this threatens their ability to properly engage in an "informed exercise of civic rights" (2018, p. 3948-3951). Following in the same direction in an essay titled *What authoritarianism is… and is not: A practice perspective,* Marlies Glasius *(2018)* believes such trends in surveillance, populism, xenophobia and nativism must be understood through a broader context. This view necessitates to distinguish between 'authoritarian' and 'illiberal' practices as they happen within a democratic and transnational context surrounding democratic accountability in general (2018, p. 517).

Both set of practices, drawing on Schatzki (2005), should be understood as a set of "doings and sayings organized by a pool of understandings, a set of rules part of an organizational and social context" (Schatzki, 2005, p. 61; as cited by Glasisus, 2018, p. 524). While such set of practices may sometimes be unknown, unearthing them can help bring more accountability to those issues. One such example of an unaccountable authoritarian practice under this model, as notes Glasius (2008), would be the previously *known-unknown* mass surveillance programs conducted by the NSA (2018, p. 524).

To further our understanding of the legitimacy crisis and what may be fuelling it we may look at recent research within the field of surveillance studies. For this, researchers

have categorized a set of anti-democratic processes or practices creeping into the everyday life of liberal democracy policing (Glasius and Michaelsen, 2018). Such processes or “patterned actions that are embedded in particular organized contexts” are under this model separated between ‘illiberal’ and ‘authoritarian’ practices. Distinguished by their respective “type of harm” and “political consequences” (2018, p. 3797), illiberal practices infringe upon “the autonomy and dignity” of an individual. In contrast, authoritarian practices instead seek to short-circuit democratic accountability (2018, p. 3797-3799). Moreover, the researchers classify those threats into three distinctive categories: arbitrary surveillance, secrecy and disinformation and freedom of expression (2018, p. 3796).

In describing their digital topology, Glasius and Michaelsen (2018) stresses how acts violating the freedom of expression of individuals, which include the act of political policing, ought to be embedded within other similar attempts seeking to undermine people’s autonomy and dignity (2018, p. 3804-3806). Under this model, practices defined as both authoritarian and illiberal, contribute to the sabotage of democratic accountability by nullifying what Couldry (2014) calls “voice”, or the ability for people to be heard. Glasius and Michaelsen (2018) thus provide examples of such practices by referring to targeted and persistent surveillance against activists and journalists (2018, p. 3805). As Glasius (2018) notes, the sharp increase witnessed in the last decade in all three categories of threats have helped further decrease public accountability and transparency toward democratic institutions. Often times, it has done so by hindering people’s access to information, including their freedom to communicate (2018, p. 527).

Once again and in both their studies on everyday acts of authoritarianism in the digital age, Hintz and Milan (2018; 2019) also underline the importance of the concept of voice by Couldry (2014). In this case, its usefulness as a model can be found in its ability

to go beyond a single-state context when studying surveillance. In other words, by helping to account for the organizational and contextual state-corporate authoritarian partnerships from which these practices become normalized (2017, p. 3944, citing Glasius, 2018 p. 517-525). From this perspective, the symbiotic state-corporate surveillance complex I mentioned earlier not only becomes an existential threat to citizens' agency but also to the democratic process. A process which contributes to the erosion of the state's legitimacy for the governed.

According to Couldry (2019), we are today witnessing the emerging order of data colonialism. Looking into what researchers in the field of post-colonial surveillance practices have found on the relationship between surveillance and legitimacy crises may help us understand better these inherent tensions. According to Morse (2019), who has done extensive research on post-colonial surveillance, legitimacy crises as described above further tend to develop into a vicious circle by acting as a driving force behind an even bigger increase in surveillance powers, especially following a rebuke: "as those with power fear a loss of control over the stolen resources on which that power is founded" (2019, p. 199). Looking back at the Snowden revelations, some might argue that this is what exactly happened. For many, little was done to curb the intelligence agencies' illegal surveillance activities while the surveillance powers of the state itself have only increased.

Consequently, researchers have sought to better understand the relationships between the surveilled subjects, looking more deeply at what possible lessons can be gleaned from the individual experiences of those confronted with pervasive surveillance. In recent years, several studies have injected a renewed importance on the value of the surveilled subject's relation with surveillance. This includes looking deeper at the meanings applied to their experiences as well as the negative consequences associated to the practice itself (Choudry, 2019; Woods, 2019; Saulnier, 2017; Mehrabov 2016, 2017;

Lubbers, 2015). Following in the same direction, professor Murikami Woods (2017; 2019), Canada's Research Chair in Surveillance Studies, believes there is a need for a "systematic political theory of the way by which authority and surveillance relates" (2017, p. 357). Paraphrasing Giddens (1985), Murikami Woods (2017) believes this is even more important as "state surveillance itself is a marker for a drift to a totalitarian state" (2017, p. 357). This also warrants a closer examination to better understand its inherent international and trans-national dimensions. Dimensions in Woods' (2017) view "integral to the phenomenon" (2017, p. 358). Consequently, Woods (2017) suggests how the study of modern surveillance should ideally include both national and international perspectives. More specifically, it also needs to focus on the relationships between "democracy, authoritarianism, colonialism, capitalism and surveillance" (2017, p. 358).

Within social movement research, professor Aziz Choudry's (2019) research on learning about the surveillance from repression also follows in the same steps. For example, Choudry (2019) notes how "today's struggles against the surveillance and criminalisation of dissent must confront the state and capitalist power relations which organize these practices" (2019, p. 17). In this case, Choudry's (2019) proposition to surveillance researchers is to look at activists and their experiences of repression as a starting point to understand the nature of modern surveillance. This can be done by carefully observing "which social forces are more likely to challenge these practices successfully" and focusing on "who is more likely to be the most affected by the problem" (2019, p. 58).

In this case, to get a clearer picture of the issue of modern surveillance, one should proceed with a careful examination of the tactics used against activists based on their testimonies. Ideally, doing do could serve as a stepping stone toward a better understanding to the way by which social control, through surveillance, is exercised among

liberal democratic societies. This according to Choudry (2019) is perhaps best illustrated when examining previous social struggles against the surveillance state. A subject which for Choudry (2019) has for a long time remained an important yet overlooked field of research (2019, p. 3-5).

Furthermore, research on the subject for Choudry (2019) should ideally begin with an investigation of targets of surveillance and their experiences of abuses. Mainly, to augment knowledge production and the sharing of best practices among activists (2019, p. 17). By drawing on the work of George Smith (2006), Choudry (2019) stresses how such experiences, as difficult as they may have been for those affected, provide us with an opportunity to “explore the social organization of power as it is revealed through moments of political confrontation (...) as the state’s repressive structures are lid bare when we come up against them” (Smith, 2006; as cited in: Choudry, 2019, p. 5-6).

For Duncan (2019), offering an alternate understanding of the various techniques of social control and their effects should also begin with a re-conceptualization of privacy as a collective issue. Specifically, by going beyond classical and individualized notions of the concept. As Duncan (2019) notes, classical and individualistic notions of privacy contribute to increasing surveillance realism among the population. Surveillance realism, defined as the condition in which people resign themselves to ubiquitous surveillance using different form of rationalizations (Dencik & Cable, 2017). One example may be the popular argument where someone declares having ‘nothing to hide’ and therefore ‘nothing to fear’ from surveillance (Ball et al., 2009, p. 353). To conclude, Duncan (2019) by drawing on Solove (2007; 2011) argues how such rationalizations often originate from a limited understanding of privacy. They do so as they tend to overlook the importance of both privacy’s individual and collective qualities. To quote Edward Snowden: “arguing that you don't care about the right to privacy because you have nothing to hide is no different from

saying you don't care about free speech because you have nothing to say." (Snowden, 2013).

2.4 Conclusion

To summarize this chapter, we have looked at the symbiotic relationship between corporate and state surveillance and discussed its relationship with modern surveillance. Throughout the chapter, I argued how the symbiotic surveillance relationship between state and corporations (Trottier & Lyon, 2012; Ball & Snider, 2013; Doctorow, 2020) means all corporate surveillance is ultimately a form of government surveillance. As Doctorow (2020) suggests in *How to Destroy Surveillance Capitalism*[7]*,* today's surveillance landscape would not exist in the way that it does now without the symbiotic state-corporate surveillance relationships. As such, any regulatory or legal limits imposed on these relationships by the state would consequently hinder its own surveillance capabilities. A phenomenon which I explained using the borrowed concept of inverted regulatory capture. This predicament, I argued, puts the citizenry as well as the fourth estate in a disadvantageous position, pitted against the combined power of state-corporate entities.

In the next chapter and based on Fuchs' (2011) negative approach to surveillance, I define the concept of surveillance from a negative perspective. More precisely and as Choudry (2019) recalls, I define modern surveillance as a tool for control, one still used today to "nip dissent in the bud as far as possible" (2019, p. 29). To situate this thesis within the literature and drawing on Mehrabov (2015), the following chapter will also discuss common subject of inquiries between the fields of communication and surveillance studies. **Chapter 3** will conclude with a review of the literature for the concept of privacy about both its individual and collective dimensions.

7 Doctorow's new book came out at the end of my thesis and after I had already developed similar points. The fact that we share similar arguments is a coincidence.

Chapter 3: Literature Review Part: 1/2

Information is power. But like all power, there are those who want to keep it for themselves.

— Aaron Swartz, 2008.

Although there seems to be a consensus on the severity of the problem surrounding modern surveillance today, there exist many disagreements about its conceptual nature. Should we treat surveillance purely as a negative or technology-neutral concept? What is surveillance's relationship to power and counter power? How best to prevent and counter surveillance's consequences on privacy from an individual and collective standpoint? Is a re-contextualization of privacy considering our renewed understanding of the effects of surveillance in order? More importantly, what do people at the forefront of the fight against surveillance have learned themselves sometimes targeted because of their activism?

To recall, this study on surveillance and counter-surveillance actors aims to further our knowledge of the multilayered nature of contemporary surveillance. It seeks to investigate surveillance as it is experienced by people from a communication perspective. To help in this matter, I have drawn on Fuchs' (2011) *How Can Surveillance Be Defined?* to define the term:

> "a specific kind of information gathering, storage, processing, assessment, and use that involves potential or actual harm, coercion, violence, asymmetric power relations, control, manipulation, domination, disciplinary power. It is instrumental and a means for trying to derive and accumulate benefits for certain groups or individuals at the expense of other groups or individuals." (2011, p. 127-128).

Throughout this chapter, I will provide an overview of the two most common perspectives when it comes to the study of surveillance: neutral and negative. This includes an analysis of their respective theoretical strengths and weaknesses in the context of this study. According to Fuchs (2011), critical and social theory can help surveillance researchers in their approach to the subject of surveillance by avoiding common pitfalls of research. Inspired by an overtly negative approach to surveillance as proposed by Fuchs (2011), I

seek to avoid its normalization without simultaneously withholding the critical potential behind proper academic research.

3.1 Negative Approach to Surveillance

To begin, the field of surveillance studies is according to Fuchs (2011) divided into three schools of thoughts. All three perspectives (positive, neutral and negative) also sharing different definition of the concept of surveillance. This includes also their own set of characteristics, claims and commonalities toward the notion of surveillance. These particularities should be considered, as the approach researchers may choose from the onset of research will also influence how they study the concept. To exemplify this notion, Fuchs (2011) points to the way neutral definitions of surveillance have in the past approached the subject ontologically. Meaning, together as both a universal phenomenon and a tool part of the "fundamental mechanisms" and "authoritative resource" at the state's disposal for the organization of society (Giddens, 1984, p. 181).

According to Fuchs (2011), unlike negative approaches to surveillance, neutral definitions do not perceive surveillance as an inherently positive or negative notion, nor do they draw a distinction between information gathering and surveillance (2011, p. 125). To provide an example, Fuchs cites Turin Monahan's (2011) definition of surveillance as an example of a neutral contextualization and cultural specificity against the often repeated claim of universality by neutral approaches. For example, Monahan's definition of surveillance as a cultural practice "embedded within, brought about by, and generative of social practices in specific contexts" (Monahan, 2011, p. 496).

For Levina (2017), neutral definitions should come with a warning, as they tend to fail to capture the intrinsic relationships between the state, citizens and surveillance, including the way people internalize the latter as part of their everyday lives (2017, p. 530). Based on her experience living in the Soviet Union, Levina's (2017) article points to the

recent rise of surveillance and authoritarianism seen among democratic liberal societies (Haggerty and Samatas, 2010). Echoing Fuchs (2011), this argument proposes that failing to distinguish between information gathering and surveillance can lead researchers to miss the power dynamics at play. Dynamics often "bound up with coercion, domination, and (direct or indirect; physical, symbolic structural or ideological) violence" (2011, p. 126).

In Fuchs' (2011) view, negative approaches to the conceptualization of surveillance tend to define data collection as done for the sake of "control and discipline of behaviour" (2011, p. 122). A practice often exercised by different societal competitive interests causing psychological, structural or physical violence. As opposed to neutral and positive definitions, negative definitions do not view surveillance as a universal concept nor as a technologically neutral tool. Rather, according to Fuchs (2011), negative approaches to surveillance have historically characterized the practice as a uniquely negative and pernicious concept serving the sole purpose of domination over others (2011, p. 124). Moreover, negative definitions perceive surveillance as a notion anathema to democratic societies and more precisely, "the notion of a participatory, co-operative, sustainable information society" (2011, p. 126).

Taking a definitive and transparent and ideological negative approach toward the study of surveillance provides researchers with certain advantages. More importantly for this study, one of such advantage to the negative approach lies in its "method of negation" which can serve as a cry against "everything that mutilates mankind and impedes its free development" (Fuchs, 2011, p. 114; as cited in Horkheimer, 1947, p. 126). Ideally and as Fuchs (2008) previously stressed, a negative approach should be complemented with a concrete comparison of its ontological opposite. Doing so can help open the door for an argument to be made against the false claim of its universality. For example, this could be an organization which demonstrates solidarity and cooperation between different

ideologies without the domination of one group over another.

3.2 Surveillance and Communication Studies

In recent years, scholars have warned against the growing fragmentation and sometimes, decreasing interdisciplinary dialogue within the field of communication research (Fuchs, 2018). It is argued that a lack of interrelation between disciplines can prevent us from the benefits of the theoretical and methodological strengths each discipline can offer, consequently affecting the quality of academic research. As a silver lining, for surveillance researcher Mehrabov (2015), this fragmented reality has provided some with an opportunity to look at the effects of surveillance from a different point of view. For instance, by looking more closely at surveillance as a phenomenon and the effects it has on society and human beings from a communication perspective.

In *Exploring Terra Incognita*, surveillance studies researcher Mehrabov (2015) maps the theoretical delimitation and strengths of the surveillance studies discipline from a communication studies perspective. Following his literature review, the author notes two main shifts behind a wider range of research in recent years. The first difference refers to how researchers have recently begun to look more closely at the causes and effects of surveillance beyond the visual act of monitoring only. While the first shift suggests a departure from traditional theories and concepts, the second shows a new tendency to diversify the range of subjects and topics researched across different fields in general.

More closely, these shifts in the surveillance studies discipline have marked a crucial departure from more traditional definitions and explanations of surveillance to the analysis of a broader range of processes and power dynamics at play. This is so because, according to Mehrabov (2015), research in surveillance has in the last decade or so tended to move away from more abstract theories and concepts toward arguably more discernible issues. For example, the relationship between surveillance and the surveilled

subject, including on “the work of being watched” (2015, p 123). For Mehrabov (2015), emergent researchers should be paying special attention to the “power dynamics” involving the different actors and processes involved. By doing so, they may better depict a more detailed picture of modern surveillance (2015, p. 123). Following Christensen and Janson (2011), Mehrabov (2015) stresses the importance to observe such processes from a “broader context of social control, of social exclusion and closure”, allowing for a better understanding for “the complex forms of surveillance that they lead into” (2011, p. 232; p. 123). Drawing on Fernandez and Huey’s (2009), Mehrabov (2015) argues how the study of surveillance and therefore resistance to it should ultimately aim to be “situational, contextual, and historically specific” (2009, p. 199-200).

This is especially relevant as Mehrabov (2016) argues in the context of state and corporate surveillance, where resistance to the seamless merger of the two powers in semi-authoritarian states has been put at a serious disadvantage. Rather than directly censor dissent, as notes Mehrabov (2016, p. 500), networked authoritarianism seeks to “compete with it, making an example out of online dissenters to affirm the futility of activism to a disillusioned public (Pearce and Kendzior, 2012, p. 284). More importantly and with surveillance now forming the core of our mediatized environment, the “intertwining of surveillance, conducted for political purposes by state, with surveillance, conducted for economic purposes by private companies [...] forms a new sort of opponent” (2016, p. 507). This opponent is particularly difficult to deal with, as it simultaneously resists old and new “weapons” while also “[thriving] on them” (Hardt and Negri, 2000, p. 138; as cited in Mehrabov, 2016, p. 507).

3.3 Privacy: a collective and individual value based on consent

Researchers have in recent years called for a re-contextualization of privacy away from classical conceptions and closer to collective minded interpretations to protect

against the negative consequences of modern surveillance (Choudry, 2019). In the book, professor Aziz Choudry underlines how a re-contextualization of privacy would allow better protection for subaltern groups against the social and commercial implications behind surveillance. More specifically and paraphrasing Fuchs (2011), Choudry (2019) believes a renewed interpretation of privacy must ideally empower the collective privacy rights of non-elite members of society to resist “surveillance by dominant groups, push back against the tendencies of these groups to hide their abuses, and strengthen the abilities of subaltern groups for collective action” (as cited in 2019, p. 59).

To better understand this notion, we must look at the historical development of the concept of privacy in liberal societies to understand its close ties to concepts of personal autonomy and consent. Today when discussing privacy and identity, we often tend to refer to privacy in the context of the data produced by the technology we use, such as one’s texts, emails or photos. However, the problem with this particular view of privacy is that it frames the value of privacy based on an individual perspective, preventing us from appreciating privacy’s value as a collective notion. The issue with statements framing privacy in individual terms lies with how they tend to limit our understanding of privacy itself. As Garfinkel (2000a) underlined before, the word privacy can sometimes fail to convey the “really big picture” and how it is not “just about hiding things” but also, “self-possession, autonomy and integrity” (2000a, p. 12). These concepts are fundamentally closely related to notions of collective freedom and cannot go without one another. As such, the risk posed by surveillance against privacy is not only individual but also collective.

However, what does privacy as a collective value really means? To recall, the previous chapter on surveillance demonstrated how unchecked and expanding surveillance powers threaten the erosion of privacy and personal autonomy. Concepts

which are essential to the notion of democratic self-governance. Within the privacy literature, we find several well-established researchers who have already highlighted the value of privacy in the context of democratic societies (Cohen, 2012; Nissembaum, 2009; Rossler, 2018, Solove; 2011; Westin 1967). As well, on the dangers faced by privacy against the rapid technological advances and growing capacity for corporate and state surveillance (Garfinkel, 2001; Rosenberg 1969; Whitaker & Whitaker 2000).

In discussing the importance of data from a colonial perspective during a lecture titled *The Emerging Social Order of Data Colonialism: Why Critical Social Theory Still Matters!,* professor Nick Couldry (2019) describes how surveillance today amounts to an invasion of the private realm. An invasion which "interferes with the space of the self, the very basis of freedom...what Hegel called the 'freedom to be with oneself', by self, without external interference" (2019, 39:00). As a Hegelian conception of autonomy and personal freedom, this perspective closely relates to our modern and individualized conception of privacy as originally developed in the legal writings of Samuel D. Warren and Louis Brandeis' (1890). For Bennett (2010), these authors were among the first to expand privacy's classical conception in legal terms to include notions of personal behaviour, decision-making and information; a concept more commonly known as "the right to be let alone" (2010, p. 3).

Decades later the social and political ramifications of privacy and the 'right to be let alone' were further developed in Alan Westin's (1967) influential work on surveillance titled Privacy and Freedom (1968). In the book, the professor draws a distinction by defining privacy as the consent by individuals and groups. Consent to control and "determine for themselves when, how and to what extent information about them is communicated to others" (1967, p. 7). According to one reviewer (Bland, 1968), Westin differentiated himself from his contemporaries by avoiding limiting his scope of research solely to the physical

aspect of surveillance (1968, p. 2). For Bland (1968), Westin included in his research different forms of data and psychological surveillance. As such, Westin juxtaposed the threat posed by unregulated surveillance against privacy's societal value and overall importance for democratic societies (1968, p. 6). Since for Westin (1967), privacy in its four basic states (solitude, intimacy, anonymity and reserve) provides individuals and groups with the necessary means for authentic organizational autonomy. An independence in the form of self-identity development helped by protected means of communication (1967, p. 34-44).

As others have argued (Dawes, 2014; Koch and Henke, 2017), the social dimension of privacy becomes the more relevant considering Habermas's sociological inquiries, diving into the public sphere and its transformations. This especially when considered as a tool to help understand privacy's role in the maintenance of legitimate democratic self-governance. According to Koch and Henke (2017), privacy ought to ideally be perceived as representing a realm helping to shield the private sphere against interference from the system, or what Habermas called the state and the economy. It does so by encapsulating a "place of self-determination [...] interrelated with the public but distinct from it" (2017, p. 6). Drawing on Kellner's (2014) analysis of the necessary conditions for authentic democratic governance, Koch and Henke (2017) also highlights the difference between privacy and anonymity. The authors demonstrate how privacy when residing within a symbolic and collective realm must be shielded against unduly intervention to what Habermas (1974; 1991) called "aggressive political and economical instrumentalization" (2017, p. 5-10).

In conjuncture with Cohen's (2012) argument, the concept of privacy in democratic societies is essential to the development and "continuing vitality of political and intellectual culture at large" (2012, p. 1906). Without the free flow of information and ideas to which

surveillance is incompatible with, “a society that permits the unchecked ascendancy of surveillance infrastructures cannot hope to remain a liberal democracy” (2012, p. 1912). In return, privacy as a realm must therefore be defended against the inherent non-neutrality of technology, according to Garfinkel (2001). For him, this is so because technological advances have in the past often proved to be tendentiously dehumanizing, tendentiously allowing for “greater control of nondeterministic processes, whether they're a person's selection of breakfast cereal or the election of a political candidate.” (2001, p. 320). Hence, to ignore the danger posed by technology against privacy or believing technology to be inherently neutral is according to Garfinkel (2001) a mistake. Especially so once we consider how much more complicated and expensive it is to “construct services that protect people’s privacy than to destroy it” (2001, p. 323). Although technology may protect people’s privacy to an extent, the ultimate solution to the threat posed by growing surveillance powers may ultimately be of a political rather than of a technological nature. Even though for Garfinkel (2001) the state could be said to be the worst privacy violator of our time, it is in his view “all the more reason to pursue a legislative solution” (2001, p. 325). However, this claimed solution also poses its fair share of problems.

With public and private power increasingly merging their capacities, the cooperation between states and corporations in the development of surveillance systems also means that the line between public and private sectors have ‘blurred in the name of commerce’ (Tue, 2019). As a result, we have observed to the normalization of corporate-state surveillance itself. Many such examples of the intimate cooperation between the state and corporations observed over the years have shown the extent of the alarming rise in public-private power. Amazon’s doorbell camera company Ring, for example, is one such mechanism which was successfully embedded into governmental surveillance networks in the United States (Gustavo, 2019; Greene, 2020). More recently in 2020, protests in the

United States against police brutality and racism in light of the murder of George Floyd have renewed calls for more scrutiny over networked surveillance. This has included the role of law enforcement, technology companies and the state in the creation of new forms of networked authoritarianism[8].

As one federal judge explains in the New York Times (Orenstein, 2018), a similar failure by lawmakers to protect privacy and "to keep pace with the times" also affects how the judiciary deals with surveillance. Unintended consequence or not, prosecutors have often abused their surveillance powers by counting on the judges' lack of technological understanding of the technologies they face. This is due in part because of the rapid advance in surveillance and investigations technologies forcing judges to play 'catch up' with law enforcement's investigative methods because of a lack of proper government regulations (Kari, 2017). Consequently, requests to use investigation technologies have become one-sided against the surveilled subject who often will remain unaware of such privacy violations.

In conclusion, surveillance affects privacy multi-laterally, on an individual but also collective level. Taking inspiration from Westin's innovative and multi-lateral approach to studying surveillance, we ought to also study privacy by looking at the issues through a different lens. One which ideally should include both individual and collective dimensions surrounding the concept of privacy.

Chapter 4: Literature Review Part: 2/2

"Hacker": A hacker is someone who enjoys playful cleverness — not necessarily with computers.

— Richard Stallman[9]

8 See: Atlas of Surveillance, Documenting Police Tech in Our Communities, EFF, 2020. https://atlasofsurveillance.org/

9 Taken from: https://stallman.org/articles/on-hacking.html

In a guidebook dedicated to newly graduate researchers, Hart (2002) recalls the key elements required to develop and unleash one's imaginative approach in social sciences. Drawing on the works of the late social scientist C. W. Mills, Hart (2002) traces the lineages of his method back to those of Marx, Weber, Mannheim and Durkheim. According to Luciano (2011), Hart's imaginative approach requires the researcher to early in the developmental stage of research delve into the literature by playfully engaging with the ideas and views encountered. As one reviewer suggests (Luciano, 2011), researchers must confront the views discovered with an open mind "regardless of how or where they originated…or who proposed them" (2011, p. 30). For Luciano (2011), Hart's playful approach is especially helpful to help one connect the dots between different kind of research studies encountered during the concoction of a literature review. For playfulness allows one the ability to better detect the interplay between theories. Especially during the methodological examination of a particular subject by allowing to, according to Luciano (2011), "think about, manage and play with ideas" (2011, p. 23).

Similarly, playfulness as an approach and method closely resembles the mentality and methodology behind those of hackers as they confront challenges and obstacles during their activities. Indeed, anthropologist Gabriella Coleman dedicated an entire book on hacker humour titled *Coding freedom: the ethics and aesthetics of hacking* (2012). Developing her thesis further In *Weapons of the Geek (2017),* Coleman expands on the factors motivating hackers and geeks to act politically through a careful examination of the methods and tactics employed during previously acted upon causes with humour, a common characteristic and tool within their arsenal. Coleman's research also stresses the diversity and complexity of the political dimensions behind hacktivists actions, which typically involve various forms of "levity and play into their activities" (2017, p. 93). A dimension often observed during her research on Anonymous (Coleman, 2013).

As Coleman (2017) later observed, hackers and hacktivists demonstrate an aptitude to work across ideological lines as well as the ability to build autonomous communities and infrastructures. Playfulness and humour become a lens through which they can decipher the world. Such a perspective allows hackers to “approach solutions not only with technical know-how and ability but also with some degree of agility, guile and even disrespect” (2017, p. 92). This agility, or “oscillation between craft and craftiness, of respect for tradition and its wanton disregard” (2017, p. 92) is not different from what academic researchers sometimes face. While researchers stand ‘on the shoulders of giants’, the advancement of knowledge depends on them challenging obsolete traditions and conventions to move their discipline forward.

When compared to other trades, what makes the nature of hackers unique for Coleman is the way their performance often permeates their craft. For instance, during hacker conferences and camps, where a sense of solidarity comes in display. For example, this sense comes alive through their arts and crafts, or what Coleman (2010) calls the hacker ‘lifeworld’. The hacker lifeworld, according to Coleman, became part of an important aspect of the hacker culture and mindset. As opposed to representing a mere extension of their online world as Coleman (2010) writes, hacker conferences and by extension hacker camps serve to re-enforce the links developed online. It does so by tightening and opening nodes between the old and the new, leading to concrete experiences going beyond the time spent at the events.

According to John Postill (2014; 2018), the convergence of hackers, geeks and makers — whom he calls ‘freedom technologists’ (2014, p. 2) and ‘techno-pol nerds’ (2018, p. 2) — recalls the works of Chadwick’s (2016) ‘hybrid media system’, Kubitschko’s (2015) ‘interlocking arrangements’ and Hussain’s (2014) ‘political technologists’. According to Postill (2018), they represent the output of what Strauss (1978) once called the ‘social

world' emanating out of real-life consequences (2018, p. 17). As such, this 'social world' also includes sub worlds (Strauss, 1978) or spaces of political actions sharing their own set of particularities (Postill, 2018, p. 56). On such space of interest for this research is the Chaos Computer Club. As one of the oldest organization of hackers in the world, it annually since the 1980s holds the Chaos Communication Congress, a popular hacker conference held in Germany.

The Club's history is said to be, according to Postill (2018), divided into three distinct phases or waves. The first, beginning with the founding of the Chaos Computer Club officially in 1983 as well as the early 1980s' "Hacker Crackdown" (Sterling, 1992). The second, following Barlow's Internet Declaration of Independence and the 90s Crypto wars in the early 1990s and the third phase, culminating with the rise of Anonymous and Wikileaks (2008 – 2016). For Postill (2018) and since the 1980s, the success of the so-called freedom technologists traces back to their distinct ability to interject themselves as new mediators. For example, between "old and new media actors, technologies and practices" (2018, p. 182) while simultaneously acting upon them.

Another important common denominator between them could be said to be their staunch anti-authoritarianism (Coleman, 2016 & Postill, 2018). A stance, according to Coleman (2011), often mixed with "a profound skepticism toward institutions and other forms of entrenched power" (Coleman, 2011, p. 93), a position exacerbated by a long and detailed history. More specifically of law-enforcement crackdowns and criminalisation against their activities since the early 80s and 90s (Sterling, 1992). Although some hacktivists are known to be antagonistic toward law enforcement, this does not necessarily mean they are uninterested by the nuances of the law. As Coleman (2016) stresses, while a good deal of them may share a negative stance toward law enforcement: "they nevertheless display enormous interest in and facility with legal principles and statutes"

(2016, p. 97). This dedication demonstrates in them an ability for self-preservation which often comes into play through their mutual "commitment to their existence as an entity" (2016, p.98). This self-awareness, reminds Coleman, ties in with what Christopher M. Kelty (2008) defined as a 'recursive public'. When writing on the particularities and cultural significance of the free software movement, Kelty (2008) defines a recursive public as:

> … vitally concerned with the material and practical maintenance and modification of the technical, legal, practical, and conceptual means of its existence as a public; it is a collective independent of other forms of constituted power and is capable of speaking to existing forms of power through the production of actually existing alternatives. (2008, p. 254)

Comparatively, John Postill (2018) argues how hacktivists and civic-hackers best symbolize a recursive public as they have, for many times, spoken to existing forms of power through the creation of strategic 'action-fields' existing between "the fundamental units of collective action in society" (Postill, 2018, citing Fligstein & McAdam 2011, p. 3). To be clear, action-fields in this context refers to cooperation between social actors which is both created and maintained (2011, p. 7). Much like convergence spaces, action-fields can include camps and congresses, as they also bring new partnerships between people and various networks together (2018, p. 43). Drawing on Fuchs' (2009) review of Castells' book *Communication Power*, this counter-power resides within a "transformative capacity" (Giddens, 1985) or ability to alter events by social relationships "operating in and through human action" (Giddens, 1981, p. 49f). For the Chaos Computer Club (CCC), we find power defined not by its capacity of coercion but instead based on its degree of cooperation between participants[10].

Following this view, Postill (2018) stresses how hacktivists, civic-hackers and data-activists belonging to the third wave also share distinct particularities which sometimes

10 See also: Fuchs (2008) p. 31-34 and 40-58.

defy sociological classification (2018, p. 64). One such particularity can be found in their multi-disciplinary expertise ranging from computer, law, art, media, politics, which often translates into a common ideological position for anti-authoritarianism (2018, p. 50). For example, by demanding ‘privacy for the weak, transparency for the powerful’ (de Zwart, 2016). A notion which supports the idea that “only by opening the black box of government to inspection by ordinary citizens that a truly democratic system can be built.” (de Zwart, 2018, p. 58). Moreover, for Postill (2018), hackers and hacktivists have over time become “important historical agents” (2018, p. 12) who demonstrate a firm ability to produce existing alternatives to power while maintaining a capacity for self-survival (2018, p. 18).

Despite some clear divergence in perspectives and political ideologies, Gabriella Coleman (2018) writes how they are in general unbound “to a singular political sentiment or even format” (2018, p. 100). Generally, they “avoid defining (and thus policing) the broadly defined ideologies that all their participants must share” (2018, p. 99). This view has allowed over time for the emergence of so-called ‘Free Spaces’ intersecting between these communities, often taking the form of hacker conferences, hacker camps and hackerspaces. As a result, for Coleman (2017), these activities have over time grown into real-life lifeworld spaces in which hackers, geeks and artists alike demonstrate their own particular style of self-organization. This in return gives them an independence existing outside mainstream societal and institutional values. One example is the annual Chaos Communication Congress in Leipzig, Germany, a conference attended each year by ten of thousands of participants from all over the world (CCC, 2017).

2.2 Learning from counter-surveillance actors

Acknowledging the reality behind the plurality of hacker movements and cultures matters will influence the methodological approach taken by the researcher before and during fieldwork. For Sebastian Kubitschko (2017), researchers delving into hacker and

hacktivist movements ought to adapt their methodological procedure early in the development of their theoretical framework. This is done first by “fleshing out specificity” (2017, p. 187) to narrow down the scope of the qualitative research. A good point of departure according to Kubitschko would be to focus on a particular organization, movement, or group. This allows for better detection of the specific patterns and conclusions relevant to the particular phenomenon investigated (2017, p. 188). Hence, for this thesis, I have drawn heavily on Kubitschko’s research on the interlocking arrangements (2015) and communicative construction (2018) of hacker cultures as models to help build my own research model and framework. More specifically, by fleshing out the specificity of my project. Rather than focusing on the Club, I decided to investigate one of its sub worlds.

In *Coding Democracy*, Maureen Webb (2020) describes the early stages of the ‘Hacker Crackdown 3.0’ era beginning with the 2008 election of Barack Obama in the United States. In the book, Webb (2020) contextualizes the third wave of hacker crackdowns against the growing converging interests of both the state and corporations with surveillance technologies during the Obama administration (2020, p. 171; p. 259). More precisely, the book examines the growing opposition against what she sees as the growing relationship between the state and corporations, who she argues faced “harshly repressing” (2020, p. 260) methods.

This can be observed, as she points out, in the Obama’s administration response to hacktivists and freedom of information activists taking a stance against the rise of corporate and state control over the internet. Citing journalist David Sirota’s description of the Obama administration’s prosecution of Aaron Swartz (Knappenberger, 2014). The activist was one of the first to raise the alarm against state-corporate relationships involving surveillance[11]. Tragically, Swartz later committed suicide awaiting trial while the

11 See Swartz’ Interview: ‘TrapWired to Spy: 'Private corps do US govt's dirty work'

target of intensive surveillance by federal agents, shortly after Swartz allegedly released hundreds of thousands of paid-access only scholarly articles for free to the public[12]. In the book, Webb (2020) paints a portrayal of the repressive methods which the Obama administration engaged in. Methods which she argues aimed to be taken as a message against what authorities saw as a clear political threat coming from the freedom of information communities (2020, p. 271):

> The prosecution of Aaron Swartz in my opinion was about sending a particular, laser-like message to a group of people that the Obama Administration sees as politically threatening, and that is, essentially, the hacker, the information and the democracy activist community. And the message that the Obama Administration wanted to send to that particular community was in my estimation, 'We know you have the ability to make trouble for the Establishment, so we are going to try to make an example out of Aaron Swartz, to scare as many of you as possible into not making that trouble. -David Sirota (Knappenberger, 2014)

Looking at the repercussions against many of the participants of one of such freedom of information community, in this case Anonymous, Webb sees a direct link between the rise of authoritarianism and corporate surveillance. This within the context of the rising severity of actions directed against those resisting state-corporate surveillance. The rise of Anonymous along with the state's responses provide many examples of the heavy-handedness approach[13] taken against hacktivists and digital privacy activists.

For the sake of this research, it helps to see the rise of Anonymous from a historical standpoint by considering its place in the fight against surveillance over the decades. Seeing the movement as belonging to a third wave of counter-surveillance actors who, due in part to the success of their campaigns, became the target of increasingly punitive actions by the state. To better understand this view, one must look at the multitude of crackdowns and overall aggressive state interventions in the last decades or so against digital privacy activists. According to Gabriella Coleman (2017), this can be observed more acutely when looking at the period beginning from the late 80s to early 90s. Many of the

12 See archive on Cryptome.org: https://cryptome.org/aaron-swartz-series.htm
13 For a timeline of arrest and raids against Anonymous participants, see: https://web.archive.org/web/20130406162836/http://wiki.par-anoia.net/wiki/Main_Page

state-sponsored interventions against digital privacy activists and hackers she argues have over time become increasingly more extreme, especially so in the last decade. As Coleman (2017) underlines, some of these tactics employed against hacktivists and privacy activists reached an “unprecedented calibre” fuelled by “marshalling geographically extensive state forces” (2017, p. 97).

Much of the heavy-handed responses followed with serious legal repercussions for many participants, including lengthy prison time and fines. One of the most severe examples being the one of Jeremy Hammond, who is today serving a prison sentence in the United States (Hammond, 2019). Other targeted state actions against hacktivists have gone beyond law usual enforcement methods and the courts. Sometimes, actions against hacktivists have involved special units from intelligence agencies, for example The Joint Threat Research Intelligence Group (JTRIG) in the United-Kingdom. In one particular case, the unit sought to manipulate public opinion by discrediting and disrupting hacktivists online using sock-puppet accounts (Al-Bassam, 2017). Other state-sponsored actions against counter-surveillance actors, for example, those combined by the Centre of Investigative Journalism, have also involved many illegal investigation techniques in which authorities sought to hinder group activities. Investigations which oftentimes happened using extra-judicial and unconventional means normally reserved for terror investigations (CIJ, 2020). As Barrett Brown, a journalist who in 2011 helped expose a public-private partnership between HGBary, Palantir and the Chamber of Commerce to spy on web users puts it: “the US and other states have no intention of allowing populations to conduct their affairs without scrutiny”[14].

Responding to this escalation notes Coleman (2017, p. 92), many of these cases have received a high degree of sympathetic media attention[15]. A degree of attention which

14 See: A sinister cyber-surveillance scheme exposed, Barrett Brown, 2011: https://www.theguardian.com/commentisfree/cifamerica/2011/jun/22/hacking-anonymous

15 See also: Thorsen, Sreedharan & Allan, 2013.

helped bring forth a certain popularity toward hackers finding themselves portrayed prominently in popular TV shows in the form of modern revolutionary heroes (2017, p. 97). A new-found popularity which, as Coleman explains, had a direct result on hacker communities. This can be observed first-hand when looking at the growing overall attendance at hacker conferences and camps. For instance, with the Chaos Computer Congress in Germany (Coleman, 2017, p. 94). Congresses and camps offer a space for hackers to engage with and celebrate their lifeworlds, but they also provide a necessary community aspect in support of those caught in the frontlines. Consequently, activists who in some case became unfairly the target of heavy-handed state actions. As such, during camps and congresses, one can observe assembly-led initiatives such as the *#FreeAnons*[16] and *#MailtoJail*[17] campaigns. Initiatives taking place in both the virtual and physical worlds. Thus, the playfulness attitude, anti-authoritarian roots and trust-based relationship shared by the CCC could also explain why the organization became a safe refuge for hacktivists and their supporters.

2.3 Chaos Computer Club: a constellation of counter-surveillance actors

The Chaos Computer Club is Europe's largest rassemblement of hackers (Bennett, 2008). Founded in the spring of 1981 in the city of Hamburg, Germany, the group today counts thousands of members and has become the most influential hacker community in Europe (Bennett, 2008, p. 52). Each year since its original inception in 1984, the Club holds the Chaos Communication Congress. In 2018, more than 17,000 computer enthusiasts, activists, artists, and hackers from around the world attended the sold-out conference[18]. Still today, the self-organized conference promotes as guidelines to the public the ideals of its co-founders Klaus Schleisiek and Wau Holland. Namely, the right to

16 See: https://www.anonymous-france.eu/ccc-project-for-imprisoned-anons.html
17 See: https://twitter.com/scotconsulate/status/1165228940925050881 and https://twitter.com/AnonymousVideo/status/1133736168892375040
18 See: https://www.dw.com/en/chaos-computer-clubs-wondrous-nerd-festival/a-41944928

privacy, freedom of information and decentralized self-organization[19]. Due to technical issues related to a fire and an increase in attendance, the Chaos Congress has since 2017 moved to a larger location in Leipzig, Germany[20]. A testament to the Club's growing popularity and influence within Germany's civil society on issues related to technology and privacy since its founding in the early 80s.

Therefore, I propose looking into the philosophical underpinnings of the group from its origins, starting with one of its two co-founders, the late Wau Holland. Following this short description, I will review the current academic literature on the CCC, including a short discussion regarding the assemblies forming the core of its constellation.

Going back as far as the early 1980s, Wau Holland envisioned a space in which people could "mobilize chaos and humour as well as ethics" (Denker, 2014, p. 171). What he defined as positive chaos could be energized, he thought into concrete challenges against society's more rigid structures. Avid reader of the Frankfurt School philosophers, more especially Adorno and Horkheimer, Holland strongly believed in the power of humour and positive chaos as a counter-cultural force for change[21]. Rather than throwing bombs to try to instigate change as he once stated in a 1988 newspaper interview, Wau believed it more strategic and "more effective to find the absurdities and make people laugh" (Schares, 1988).

As Denker (2014) notes in *Hacking Europe,* Holland sought to include early in the Club's inception concepts of counter-power resistance and sousveillance tactics. These strategies, underlines Denker (2014), ranged from counter-control to inverse panopticism tactics (2014, p. 171)[22]. In Denker's (2014) own words: "Holland's political agenda

19 Interview with Klauss, accessible on Web Archive as it is no longer reachable in its original form: https://web.archive.org/web/20190917164111/http://politicalcritique.org:80/world/eu/2019/chaos-computer-club-how-did-computer-freaks-in-germany-come-together

20 See: https://www.ccc.de/en/updates/2017/34C3-in-leipzig

21 As cited in Denker's footnotes on p. 170, who himself cites Kulla (2003).

22 Denker (2014) cites the biography of the late co-founder Wu Holland. See: Kulla, D. (2003). *Der Phrasenprüfer: Szenen aus dem Leben von Wau Holland; Mitbegründer des Chaos-Computer-Clubs* (Vol. 241). Pieper and the Grüne Kraft. p. 16.

occupied a space between computer technology's democratization and popularization and its somewhat anarchistic appropriation" (2014, p. 170). For Holland, "positive chaos" and "playfulness" should be celebrated as the Club's core principles. Indeed, for the co-founder, positive manifestations of chaos mattered and needed to be reflected within the organizational structure of the club as well. Hence, the computer security activist described the organization as self-organized and akin to a "galactic association without any fixed structure" (2014, p. 172). Most importantly, this galactic association would come out strongly to support the free flow of information and privacy against "the brave new world in the year of big brotherhood" (2014, p. 172-173)[23].

While Wau Holland strongly supported the free flow of information, he did not appear to be an absolutist by any means. For instance, Holland once stressed the importance for hackers to handle the data and secrets they amass ethically and with care. Failing to do as much, he once argued, can too often and easily lead one into a vulnerable position in which the hacker become the "plaything of intelligence agencies" (Wau-Pengo debate, 1989)[24]. To support his views, Wau cited the Hacker Ethic, a set of originally six guidelines and principles first published in Levy's (1984) book *Hackers: Heroes of the Computer Revolution*[25]:

- Access to computers — and anything which might teach you something about the way the world really works — should be unlimited and total. Always yield to the Hands-On Imperative!
- All information should be free.
- Mistrust authority — promote decentralization.
- Hackers should be judged by their acting, not bogus criteria such as degrees, age, race, or

23 Wu Holland's quotes taken here belong to issues of *Datenschleuder*, from which Denker himself cites. Some quotes can be accessed on http://ds.ccc.de and http://media.ccc.de — as well as the Club's local archives.

24 See re-enactment of the Wau-Pengo debate (1989) accessible on: http://www.wau-holland-stiftung.de/en/news/2015/02/re-enactment-of-the-wau-pengo-debate-1989-at-the-31C3/

25 This version of the Hacker Ethic includes two last points later added by the CCC following the incident with Pengo. See: https://www.ccc.de/en/hackerethics

position.

- You can create art and beauty on a computer.
- Computers can change your life for the better.
- Don't litter other people's data.
- Make public data available, protect private data.

While hackers are known to break rules, Wau certainly understood how they would also unlikely follow a set of iron laws, even if those rules happened to be “their own” (1989, p. 25). While Wau agreed that everyone enjoyed personal freedom and thus were free to follow the rules or not, they must remember that such freedoms also came with their own consequences. Hence, Wau heavily stressed the importance of following one’s ethical standards as a safety mechanism against losing one’s independence and becoming the intelligence agencies’ “plaything” (1989, p. 26).

After the fall of the Berlin Wall, the CCC became one of the few groups fighting for privacy against new surveillance measures in Germany (Bendrath et al., 2009, p. 12). For Bendrath (2009), the privacy movements’ success reflects both their openness and decentralized nature, “making it easy for anyone to participate” (2009, p. 16). As the authors themselves note (2009, p. 15), the efforts of the German privacy movements in the 1980s and 1990s flourished into a counter-political movement late into the 2000s. One of its major contribution had been re-insertion of privacy as a topic in mainstream debates (2009, p. 17). Many counter-strategies employed by members of the CCC in the last two decades have reflected the playfulness and humour Wau supported, including positive chaos as a strategy to challenge the rigidity of systems. This of course in the hope of helping expose what he saw as the wrong uses of technology by technology (Denker, 2014).

For example, in 2008 and to prove a point, members of the group uncovered

vulnerabilities in Germany's electronic voting system by hacking voting machines into playing chess (Webb, 2020, p. 277); during the 2008 Olympics, CCC members helped circumvent China's Great Firewall by distributing "freedom sticks" with the Tor browser included to athletes and journalists[26]; the same year, they took the fingerprints of the German Minister of the Interior from a cup and published them online to warn against the weakness of bio-metric identification methods[27] (Krasmann & S Kühne, 2014 p. 6); something which they did again after the release of Apple's Touch ID feature in 2013 using fingerprints taken from photos of the Defence Minister's own hands[28]; in 2011, the group uncovered surveillance malware technology used by the German police. Surveillance malware previously exposed in 2018 by WikiLeaks during the so-called *Staatstrojaner affair*[29] *(Hudig, 2012).* As Webb (2020) notes, since the days of the 1984 Bildschirmtext hack[30], members and supporters of the CCC have demonstrated both a willingness and an ability "to disobey the law in the spirit of peaceful, nondestructive civil disobedience" (2020, p. 278). They have done so, more importantly, while remaining faithful to Wau Holland's ethos of positive chaos.

Many of these exploits have prompted researchers within the field of communication and information research to examine more carefully the role played by loosely networked collectives. For example, collectives such as the CCC in their role to counter surveillance assemblages (Bennett, 2008; Denker, 2014; Kubitschko, 2015, 2018; Wagenknecht & Korn, 2016). This includes how groups like the CCC have helped counter-act pro-surveillance tendencies using alternative media technologies and infrastructures.

26 See: The Register (2008) https://www.theregister.com/2008/08/07/torbrowser_olympics/ and Wired (2008) https://www.wired.com/2008/08/usb-dongle-brea/ and CCC (2008) https://www.ccc.de/en/updates/2008/chinesewall

27 Krasmann & S Kühne themselves cite Die Datenschleuder, a magazine published by the Chaos Computer Club, edition 92 p. 56-57, available on https://ds.ccc.de/download.html — they also note that the technique was not new, and had been previously demonstrated at another CCC event in 2005.

28 See: Guardian (2014) https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands

29 See: Wikipedia's section on the Staatstrojaner affair: https://en.wikipedia.org/wiki/Chaos_Computer_Club#Staatstrojaner_affair

30 See: Hafner & Markoff, 1995, p. 158.

Researchers Kubitschko (2015), drawing on Cohen (2012), has for example touched on the importance of “interstitial spaces within information processing practices” (Cohen, 2012, p. 1931) in the context of the fight against surveillance. Space itself becomes crucial in this case, as it allows the Club to counter-act “contemporary assemblages of surveillance” (2015, p. 82) in two distinct ways. As Kubitschko (2015) points out, through their “subversive engagements with technology” (2015, p. 84), they in effect exercised what Warren and Brandeis (1890) called their “right of privacy” by “shaping discursive spaces that establish exchanges of knowledge” (2015, p. 85). This includes for example the self-organizing of hackers camps and congress which allows in return for “flows of information and new levels of awareness” to emerge (2015, p. 84). The creation of both digital and physical spaces concludes Kubitschko (2015) is what allows in return the Club to go beyond digital style activism.

Beyond space as a process to create new meanings, the organizational and communicative aspects of the CCC helped it earn trust and legitimacy among hackers communities. As argued by Kubitschko (2018), the organization employs ‘discursive construction’ (Fairgust and Putnam, 2014) of ‘organized sense making’ (Weick et al., 2005) together influenced by internal and external aspects (2018, p. 84). From an organizational perspective, the Club thus benefits from a vast array of supporters coming from all walks of lives often encouraged to speak out and cooperate with other civil actors. As such, the Club’s “multi-layered media ensemble” (2018, p. 92) enables the organization’s collective voice to be heard across different political landscapes. This situation is in part helped by the inherent interlocking arrangements found “between hacking and the communicative figuration within the Club” (2018, p. 93). This “spiral of legitimation” (2018, p. 95) fuelled by hacking and communication strategies allows the Club to secure legitimacy as a trusted civil society organization from an internal and

external viewpoint.

Wau's vision of a "galactic association without any fixed structure" is alive and well within the hundreds of assemblies or decentralized organizations attached to the CCC. During a camp or congress, hundreds of assemblies will settle in along with its respective members into their designated area. These sub-spaces become where people are invited to participate in various activities, such as workshops, lectures, debates, and so on. To use Routledge's notion of *convergence space* (2003), those assemblies help to "articulate collective visions" (2003, p. 345) without the need for a "single organization or ideology being in a position of domination" (2003, p. 345). Despite convergence spaces often becoming spaces of 'contested social relations' (Sharp et. Al 2000) as argues Routledge (2003, p. 346), the CCC has over time provided a stable framework enabling its members to cooperate based on a set of universalist positions reaching across spaces (Harvey, 1996).

Figure 1: Image tweeted during the Chaos Communication Camp, 2019.

Chapter 5: Methodology & Research Design

For Silverman (2013), himself drawing on Specker (2003) and Murcott (1997), the methodology section of a thesis offers the researcher with an opportunity. In this case, to be transparent by presenting “an honest account of the conduct of the research” (2013, p. 657, table 20.2). We attain transparency through this process by demonstrating a general openness towards one's strategy, goals and research design. This is first achieved by providing an understanding of the strengths and weaknesses behind each method adopted. For a qualitative study such as this one, what is generally expected out of the methodology chapter can be summarized in four concrete steps:

1. Provide an account of how the research was conducted.
2. Explain your research design and strategies.
3. Describe the techniques and methods employed.
4. Justify your decisions. (Silverman, 2015, p. 658)

Before we begin, I will explain the justifications behind the decision for a mixed-methods design approach for this thesis. This includes the choice of Jeffrey Juris’ (2007) militant ethnography, participant observation and semi-structured interviews as research methods.

For Cameron (2009), the origins of mixed-methods design can be traced back to the philosophy of pragmatism in the early 19th century. Although more recently, to post-positivist influences (2009, p. 140-141). Drawing on Morse (2016), I argue that the practical and exploratory nature behind the mixed-methods research design can help researchers better understand different aspects of a particular phenomenon. For example, by supplementing their primary and initial method of research with an albeit lesser, secondary component (Morse, 2016, p. 14). Although, as Morse warns, it can be “easier to mess things up” (2016, p. 77). However, this process can be eased when both the core and the supplementary components of the chosen methods belong to the same paradigm.

Even though as Morse (2016) argues, some researchers “do not consider combining two methods from the same paradigm as mixed methods” (2016, p. 15), mixed-methods research design can still involve a core qualitative component fuelled by an inductive and theoretical drive. When done sequentially, the first method can be appended by a second supplementary method. For example, as pointed by Morse (2016), when doing ethnography and semi-structured interviews subsequently (2016, p. 85-92).

5.1 Militant ethnography

Militant ethnographers have sometimes used two sets of qualitative methods, such as in-depth interviews supplemented by participant observation, to complement or expand on the analysis of their initial findings[31]. For David Silverman (2016), the *in situ* ethnographer must remember to always follow principles of openness and flexibility in the design of a successful qualitative research (2016, p. 11). Flexibility and openness are together necessary principles helping to ease the immersion process part of any ethnographic study. In return, doing this can help build the necessary parallels between the researcher and its subjects, allowing for a reflexive process of attitude learning to emerge (2016, p. 15).

In this case, reflexivity for Silverman (2016) refers to Garfinkel's (1967) notion of “the ways in which our portrayals of social realities simultaneously describe and constitute the realities” (2016, p. 36). For these portrayals to be solidified, researchers often turn toward a research design involving a mixed method process of qualitative inquiry to help deepen the analysis of their research findings. According to Silverman (2016), this decision can emerge when new and unexpected factors emerge during and after fieldwork (2016, p. 38)[32].

The goal of militant ethnography follows in the footsteps of McIntyre’s 2004 ‘useful

31 See: Juris, 2007; Juris, 2008; Apoifis, 2017.
32 See: Merry, 1990; Conley & O'Barr, 1990.

solution' (2004, p. 19) for the production of "politically applicable work" (2008, p. 8) by and for social movements. As Juris (2007) himself explains in his research on the *Movement for Global Resistance in Barcelona*, "from within movement, for movements" (2007, p. 5) means converting the collective knowledge gained from research into a "fluid and accessible" medium applicable to both activists and others (2007, p. 165). Following this logic, this study thus seeks to generate and then collect a sample of the accumulated experiences to ensure proper knowledge retention within a collective intelligence (Lévy, 1993).

For this, Jeffrey Juris' (2007) method of militant ethnography thus becomes a pragmatic approach to ethnographic research. In other words and as technique, it is based on a reflective framework to qualitative inquiry where the researcher purposely walks the line separating academic research and activism (2007, p. 165). As Juris and Khasnabish (2013) argued in *Insurgent Encounters*, the reality behind modern transnational activism and today's interconnected world of communication technology calls for new research methods and design better adapted to situations researchers must face (2013, p. 22). For example, by offering an engaging and interactive approach between the researcher and its subjects. More concretely, militant ethnography seeks to produce via the collaborative efforts of both the researcher and participants emergent knowledge useful to activists while adhering to academic standards of research[33].

According to Apoifis (2016), the philosophical roots underpinning Jeffrey Juris' (2007) militant ethnography trace back "as far back as Karl Marx's Workers' Inquiry (1880)" (2017, p. 3). As well, it follows into the footsteps of Nancy-Scheper Hughes' (1995) "politically and morally engaged" ethnography and Charles Hale's (2006) "activist anthropology" (2017, p. 4). Thus and drawing on established ethnographic methods, militant ethnographers enjoy a multitude of techniques developed by qualitative

33 See: Juris, 2007, p. 164-165; Gordon, 2008; Russell, 2014; Apoifis, 2017, p. 3.

researchers to help them critically engage with their subjects. This many sided approach as recalls Apoifis (2016) is not without recalling Snow & Trom's (2002) "multilayered and nuanced" research design. The latter in which a core approach is simultaneously supported by a plurality of tested methods (2002, p. 150). These instruments or tools can range from, according to Apoifis (2016):

> "...text, discourse and media analysis (Juris, 2007: 169; Russell, 2014: 3); in depth interviews and timely written field-notes (Juris, 2008: 5); respondent validation techniques (Russell, 2014: 5); processes of reflexivity (Juris and Khasnabish, 2013: 3); and rigorous ethical and con-sensual fieldwork practice (Apoifis, 2016, in press)." (2017, p. 4)

What differentiates militant ethnographers from their contemporaries is how they deliberately step on the line separating activism and academia to produce reflexive knowledge relevant to the movement under study. For Apoifis (2016), militant ethnographers "support their particular blend of activist and academic research" (2017, p. 4) with established methods to produce concrete findings for social movements "from within social movements" (Apoifis, 2017, p. 4-5). Despite its solid philosophical grounds, Apoifis (2016) underlines how militant ethnography remains vulnerable to criticism of bias and subjectivity "potentially stifling the poignancy of research findings" (2017, p. 4).

To discuss these issues, militant ethnographers confront these issues head on by deliberately stepping on the line separating activism and academia as they seek to provide an unfiltered representation of activists' views. To be openly working with activists, reminds Apoifis (2017, p. 3), should not automatically raise issues of political partiality against the ethnographer. Instead, by taking this deliberate stance, the militant ethnographer purposely seeks to negate the concept of objectivity. In other words, what Bertie Russel (2014) defined as the "disavowal of positivist knowledge and the construction of situated partisan knowledge(s)" (2014, p. 1) within a particular time and space. This deliberate approach reflects the way by which, for Apoifis (2016), "contemporary activists procure

relevant knowledge as insiders producing politically applicable work" (2017, p. 3). For this thesis, I have taken the role of the activist-scholar as a mechanism to more easily convert reflexively created movement-information into knowledge accessible to the academy. More importantly, knowledge which remains relevant to the activists under study. According to militant ethnographers Maribel Casas-Cortès and Sebastian Cobarrubias (2007, p. 14), when done under this optic, "research becomes a political tool to intervene in the processes that are moving us towards a neo-liberal world" — or worst.

5.2 Participant observation

When properly applied, the previously mentioned empirical tools can help militant ethnographers uncover relevant and representative knowledge from the activists' own point of view. Participant observation can be useful in this case to help researchers triangulate information and subsequently enrich its context[34]. Although to achieve, some requirements must be carefully followed. What these requirements entail for the researcher is to remain in constant awareness of their roles and position as activist-scholar. This is done when recalling their subjectivity and how it may influence during research their interpretative processes (Uldam and McCurdy 2013). According to McCurdy (2009), the benefits associated with insider participant observation has to do with its potential as a research method. For example, its capacity to reward us with a wealth of information otherwise not available (2009, p. 148)[35].

While many of the pros and cons regarding participant observation are already well documented[36], for Uldam and McCurdy (2013) several grey zones remain. Most particularly in the study of social movements (2013, p. 943). As the authors contend, such grey zones reflect the interplay between insider/outsider and overt/covert dimensions which observers may face as they engage in the different positions during fieldwork.

34 See: Burawoy, 1991a; Jorgensen, 1989; Litcherman, 2002.
35 See: Jorgensen, 1989; Plows, 1998; Roseneil, 1995.
36 See: Atkinson and Hammersley 1993; Snow et al. 1986.

According to their literature review of the key debates between insider and outsider positions, these dimensional dissimilarities can be managed. Especially if countered by a reflexive and critical approach regarding one's work during fieldwork (2013, p. 945). Helped by a strong ethical guideline, proximity can help increase accountability for both a researcher's subjects and readers. By doing so, a researcher's proximity toward his subject becomes an asset. This, of course, as long as such proximity supports "a reflexive awareness and constant questioning of one's position" (2013, p. 945).

To more easily connect the ethical and interpretative implications related to the study of social movements, McCurdy and Uldam (2014) have proposed a reflexive framework in the form of a quadrant. A methodological aid I found useful when presented with similar challenges during this research. The framework, built on top of two ethnographic research experiences (2014, p. 41), can help researchers introduce and familiarize themselves with the ethical and methodological ramifications surrounding insider/outsider and overt/covert roles. This before, during and after field-work (2014, p. 52).

5.3 Semi-structured interviews

To delve deeper into people's experiences, militant ethnographers and researchers can exploit different tools and methods, including qualitative semi-structured interviews, to find answers to their research questions. Qualitative inductive research for Flick (2009) is concerned with "analyzing concrete cases in their temporal and local particularity and starting from people's experience and activities in their local contexts" (2009, p. 21). According to Alsaawi (2014), many of the practical and ethical challenges associated with interviews can be countered. For example, according to Kallio (2016), if triangulated with other tested methods and by remaining in constant awareness of their methodological limitations (2016, p. 155). As Kallio (2016) notes, semi-structured interviews can be an

effective tool for researchers looking to increase reciprocity with their subjects during the interview process. Semi-structured interviews can enable more lee-way in the structure of the interview. For instance, by allowing necessary “space for participants' individual verbal expressions” to emerge (2016, p. 2955). For Denzin (2001), qualitative researchers can use interviews not necessarily as a data collection method. They can use interviews also as a “vehicle for producing performance texts and performance ethnographies about self and society” (2001, p. 24, as cited in Alsaawi, 2014). They do so according to Kvale (1996) because they can help pinpoint central themes in the life-world of the interviewees (1996, p. 100).

For the sake of this critical ideological study of surveillance, I have opted for semi-structured interviews to supplement the militant ethnographic portion of my research. In this case, to delve deeper into the experiences of activists who faced repressive surveillance. As Alsaawi (2014) stresses, the open-ended format of the semi-structured interview process allows for better flexibility and space when seeking to elaborate on particular themes during interviews (2014, p. 151). However and due to its interpretative nature, the process of interviewing is not inherently neutral. Ultimately, the researcher produces written narratives out of oral stories first told within a process which in itself influenced by uneven power dynamics between the interviewee and interviewer (Kvale, 1996, p. 126). While remaining aware of these limitations, it is possible to combine different research techniques to help alleviate some of its downsides (Bauer & Gaskell, 2000, pp. 336-350).

To better accommodate the need of my interview participants, I made sure to respond to their preferences for the conduct of the interview. For example, if done either in person or online. When online, I conducted interviews using encrypted communication applications to protect the privacy of each participant. Before and after my first fieldwork

visit to Congress in December 2017, I worked on refining my interview guide following Kallio's (2016) recommendations. Such as, how the trustworthiness of semi-structured interviews depends on the rigorousness of the data collection procedure during the research phase. A factor which can have a significant influence on the results (2016, p. 2955)[37]. Therefore, to ensure proper data collection, I followed the authors' own framework for the elaboration of my interview guide beginning with the identification of interview prerequisites (2016, p. 2959).

Following in these steps, I designed my interview guide[38] to better reflect the main topics and themes enumerated in the first half of this study (Taylor, 2005). The interview guide quickly became an introduction mechanism before each interview. This allowed for example participants to know beforehand the themes to be discussed. Before every interview, I made sure to share the interview guide with all participants. This allowed for them to familiarize themselves beforehand with the topics and themes discussed during the interview (Gill et al., 2008). This often proved to be a successful strategy, helping to break the ice before the actual interview even began. Over time, my interview guide evolved "based on the actual research interview experiences" (2016, p. 2962)[39].

5.4 Ethics

Proper attention to ethical procedures must be given before, during and after the completion of a research project. This is especially true for research involving human participants, particularly those judged to belong to a vulnerable group. This of course includes those unfairly surveilled by the state. For these reasons, argues Silverman (2013), researchers ought to view ethics as one of the key components underpinning the proper conduct of academic research (2013, p. 318). Hence, I have taken proper care to follow best practices suggested by my supervisor and security experts, while carefully

37 See: Kitto et al., 2008; Gibbs et al., 2007.
38 To consult the interview guide, see: Appendix 3.
39 See: Taylor, 2005; Holloway & Wheeler, 2010.

following the University of Ottawa's ethics guidelines[40]. For this, I have taken great care to ensure the security of all communications with my study participants, including the storage of research data to the best of my abilities. For example, I have enforced the exclusive use of encrypted communication software when communicating with my participants while keeping sensitive information on an encrypted hard drive at all time.

I received ethics clearance to interview participants for this thesis on May 22nd, 2018, although my first visit to the Chaos Communication Congress in December 2017 was performed under the supervision of Prof. Jeffrey Monaghan from Carleton University, who also contributed a research grant to cover transportation costs[41]. To protect as much as possible the identity of each interviewee, my supervisor and I decided to limit the amount of identifiable information from each of the participant. For example, by not requesting a physical signature on the consent form. Instead, before each interview, I e-mailed the consent form to allow participants to familiarize themselves with their rights and how the interview would proceed. Before each interview began, I asked participants if they had read the consent form, and if they agreed to it. A decision made to avoid collecting signatures or names, and thus, lessen the privacy risks involved with data collection. The consent form also explained participants how their personal data would be handled and destroyed upon the completion of the thesis. Before each interview, I also forwarded to every participant along with the consent conform the interview guide containing all the questions and themes for the interview.

During observational field work, I introduced myself as a researcher, but also explained the meaning behind my particular method of research, while at the same time explaining my background as a privacy activist. At the conferences attended, I made sure to make people aware of my presence and of me taking notes. I did not take recordings or

40 See: The University of Ottawa's ethics guidelines: https://research.uottawa.ca/ethics/guidelines

41 The consent form can be viewed in Appendix 4.

photos, instead I used what the participants themselves published on social media and other platforms. In conjuncture with my supervisor, we decided to protect the identity of those who have participated in this study by keeping the names and origins of each participant strictly confidential. Using the word ‘Participant’ followed by a number, I have also limited the biographical description of each to a minimum.

5.5 Triangulation and data analysis

Now, I would like to note how the following chapter on the research findings is situated beyond the conventional positivists-constructionists quandary in the social sciences. In other words, wherein researchers debate the possibility in reaching truth ‘out there’. For Silverman (2016), this position advances that while research cannot provide us with an exact representation of the specific social world, we as researchers examine. However, qualitative research can nonetheless provide us with “the meanings people attribute to their experiences and social worlds” (2016, p. 126). For this reason, this research does not aim to represent the view of every participant belonging to the Chaos Computer Club. Rather, this study focuses instead on one of its many sub-worlds.

It is important to recall how the meanings social researchers derive out of the experiences they get from interviews conducted can increase our knowledge of the many social worlds surrounding us. Researchers can derive such information from the social worlds they research through in-depth interviewing and the analysis of the collected narratives (Harding, 1987; Latour, 1993; Silverman, 2016). For Van Maannen (2011), it is through the activity of fieldwork that ethnographers manage to tell the story or what he calls ‘the tale’. Through fieldwork, ethnographers manage to reach an “understanding of others, close or distant” (2011, p. 1). This understanding is, of course, distilled from the researcher’s interaction with their research subjects and within their own environment. However, ethnographers can nonetheless share to the best of their ability what they see

as a “truthful account of the social world being studied” (2011, p. 2). Most importantly, when the time comes for these findings and accounts to be converted into a credible written report, its final representation remains a conscious choice by the researcher.

According to Van Maannen (2001), ethnographers must aim to “represent the culture, not the fieldwork itself” (2011, p. 4). By avoiding too much “distortion” (2011, p. 16) in the transmission of the message, they seek to communicate a meaningful experience of their work and findings back to their readers. As such, it is an exercise bound to be interpretative to an extent. Like Van Maannen’s (2011) proposition, I believe the way we go about how we tell the tale matters, even more importantly so for militant ethnography, as the tale becomes another medium to share the meanings, views and experiences developed during fieldwork. As Cunliffe (2010) reminds us, this process of reflexivity is what binds ethnography as a method together. It does so according to Cunliffe (2010) by “understanding and unsettling the constructed, fictional, and ideological nature of selves, “realities” and texts” (2010, p. 231). In the end, to do ethnography can be as much a process regarding the ‘other’ as much as it can be a process of the ‘self’. Hence, it matters deeply how we think of the interactions with the subject of our study. In this case, how we also go about writing the texts we write about them (2010, p. 226).

Therefore, and the sake of transparency, I believe I must first write a few words about my own standpoint as an activist-scholar. This before delving into the next chapter and into the core of the thesis’ ethnographic work. It would be false to say that this project started at the beginning of my graduate studies. While the final idea for the thesis certainly germinated during my graduate program, this study is also the culmination of more than 12 years of participation as both activist and apprentice researcher with different communities. As one member of the CCC once said: “you kind of stumbled upon this world randomly” while I was also trying to find my own niche within academia. This is because

early at the beginning of my undergraduate political science degree, my interests already focused on emergent counter-power groups who used the internet as a tool for change.

The difference between now and then is the theory and methodology background I have accumulated over the years and during my studies. While pursuing my own path, the field of ethnography also went through a phase of transformation (Juris and Khasnabish, 2013, p. 1-39). In the last two decades, ethnography as a discipline has become much less authoritative, involving more interpreters as opposed to a single producer of knowledge.

While greatly influenced by my past, I tried to the best of my abilities to remain careful to make this thesis about the ideas presented rather than myself. Despite this, some may disregard the ideas presented in this thesis outright in part due to the apparent bias involved. However, as Juris (2007) once argued, militant ethnography differs from other more classical methods of research as it seeks to 'overcome the divide between research and practice' (Juris, 2007, p. 165). It does so by jumping straight into the flow of social practice. As Juris (2007) argued, the act of becoming 'active practitioners' allow us to gain better analysis based on "practical, embodied understanding" (2007, p. 166).

5.6 Limitations and conclusion

This thesis has several limitations imposed by the methods employed, the size of the interviewee sample but also, my own position as an activist-scholar. This includes known limitations involved with semi-structured interviews and the interviewer-interviewee dynamics (Kvale, 1996, p. 126). Moreover, also how this thesis is, of course, constrained by time, budget and experience. As such, it does not claim to be a representative overview of surveillance, hackers or privacy activists in general. Nonetheless, while there exists no "unmediated version" (Hollway and Jefferson, 2000, p. 151) of how we as individuals understand the world. Despite this, researchers can still infer useful conclusions from the

data they get by theorizing on the meanings, knowledge, and concepts “underpinning the data” (Ryan, 2006, p. 100).

Chapter 6: Findings and Discussion

“Suddenly to realize that one is sitting, damned, among the other damned—it is a most disquieting experience; so disquieting that most of us react to it by immediately plunging more deeply into our particular damnation in the hope, generally realized, that we may be able, at least for a time, to stifle our revolutionary knowledge.”

— Aldous Huxley, 1941, p. 30

This critical ideological study of modern surveillance is founded upon an empirical study, using as its main methods of research participant observation, militant ethnography and semi-structured interviews. From a participant insider perspective, it explores and interprets the experiences, meanings and views of counter-surveillance actors targeted by surveillance. It is supported by participant observation and militant ethnography conducted

in Germany between 2017 and 2019, respectively during the Chaos Communication Congress in Leipzig and the Chaos Communication Camp in Brandenburg[42]. Drawing on the principles behind militant ethnography, I focus on the lessons learned based on the participants' own experiences. In this case and as described in **Chapter 4**, counter-surveillance actors belonging to the third-wave of privacy activism (Postill, 2018). In total, 8 interviews were conducted. For this chapter, I have thus opted for a narrative intertwined with analysis to relay the findings of this study. The goal here is to simultaneously reflect upon the concepts presented in the first half of this thesis in light of discoveries made in the field.

As a research study which coherence stems from both my position as a researcher and of member of the community I am researching, demonstrating a degree of reflexivity is essential to achieve academic trustworthiness[43]. This implies an ability to inquire about my role as an instrument of research but also to question the potential implications of the research findings versus my own standpoint (or role) as activist-scholar. A position which admittedly can be both a blessing and a curse (Merrigan et al., 2012, p. 97). A blessing because, according to Frey (1994), this can allow one to more easily portray the views of an under-researched group. A curse because, taking such a dual position makes it harder to differentiate between my own views and those of my study participants. To avoid such pitfalls, I have questioned my own representations and interpretations during the research process. Similarly, I must stress the interpretative nature of this research. This study is innately interpretative and based upon my ethnographic observations. One primary criterion guiding such research is and as mentioned by others, the opportunity to learn

42 See **Appendix 3** for the full schedule.

43 In *Reading and writing as method: In search of trustworthy texts*, p. 59, Schwartz-Shea and Yanow (2009) state: "researchers writing for readers across epistemic boundaries might write more scientifically persuasive manuscripts if they recognized that reader-reviewers are likely to be asking, implicitly if not explicitly, 'What makes this ethnographic account trustworthy?' (See also Clifford, 1998)". In the text, they describe 6 necessary criteria, which are themselves connected to 8 categories of persuasive elements (Yanow, 2009). These 6 criteria are: thick description, researcher reflexivity, data triangulation, data audit, negative case analysis and member-checking.

(Frey, 1994; Stake, 1998).

Moreover and drawing on Schwartz-Shea and Yanow (2009), the ontological and epistemological presuppositions underpinning the interpretative methodological perspective come with a warning. In part because it considers 'objectivity' or "the ability of the researcher to stand outside of the subject of study", as something which is unattainable and "not conceptually possible" (2009, p. 65)[44]. From this perspective, it is more desirable and realistic to aim for transparency by being explicit about one's role, initial access and standpoint as researcher. Doing so they argue can help ethnographers produce more trustworthy and less deceiving research outcomes. Before outlining the main study findings, let us recall the three research questions driving this ideological study on surveillance (as originally stated in **Chapter 1)**:

• (**RQ1**) What are the experiences of counter-surveillance actors in resisting modern surveillance?

• (**RQ2**) What lessons and views regarding the state of modern surveillance can be gleaned from their experiences?

• (**RQ3**) How do their experiences diverge from or relate to known concepts found in the literature within the fields of media and surveillance studies?

6.1 Summary of Findings

These findings provide an overview to be presented more in-depth through the following narrative-analysis and in light of the literature previously reviewed in **Chapter 2, 3** and **4:**

• From their experiences resisting the symbiotic nature of contemporary surveillance, participants tend not to draw a clear distinction between state and corporate surveillance, often seeing the two as interchangeable.

44 Also see: Bernstein, 1983; Hawkesworth, 2006 and Yanow, 2006.

• Control mechanisms elaborated by participants when targeted with surveillance touch on strategies dealing with the media, encryption applications and how to reverse isolation through internationally-based solidarity and organization.

• Likewise to offering a space for the celebration of a shared ‘life-world’ as proposed by anthropologist Gabriella Coleman, Congresses and Camps also provide a space where decentralized resistance against surveillance in support of those targeted is possible through the sharing of a collective sense of contextual commonality.

6.2 First stop: Chaos Communication Congress — Leipzig, Germany.

The reasoning behind my decision to pick the Chaos Congress as the first stop for this ethnographic and ideological critique of surveillance relates to my own experience as a privacy activist but also, my own reading of the literature as presented in the previous chapters. Because this thesis uses a negative approach to define surveillance (Fuchs, 2011), we have seen previously how its critique should also be complemented with a concrete example of its ontological opposite. As Fuchs (2011) reminds us, this can be an organization in which solidarity and cooperation between different ideologies is possible without domination of one group over another. Symbolizing a strategic ‘action-field’ (Postill, 2018) or ‘free-space’ (Coleman, 2018). Thus, the Chaos Congress and Camp bring together different networks within a collective space where such a kind of cooperation is both created and maintained. As we will see, assemblies, like many hackers communities, are free spaces not because “they are open to everyone” as Coleman (2018, p. 94) explains. Instead, they are open in the sense that they independently exist outside the influence of institutional norms and values.

In my case, I knew that Congress had become for many of us involved in the third wave of privacy activism a natural refuge for those involved with these communities.

Although when I first visited Congress in 2013, the conference happened in Hamburg, Germany. However, as of 2017, the Club decided to move the location to Leipzig due to growing attendance numbers and renovations following a fire which rendered the former location unusable. For this reason, the 2017 iteration of the Chaos Communication Congress found a new and bigger home in Leipzig, Germany[45]. With the hindsight, the decision made sense as the new and massive conference centre allowed the Club to welcome more than 15 000 visitors coming from different parts of the world[46][47].

Of note, the Chaos Communication Congress as organized by the CCC would not be possible without the hundreds of volunteers or 'Angels' donating their own time to run and maintain the event. Their devotion allows in return for the experience to be fully enjoyed by the rest of us. This includes the massive physical and digital infrastructure surrounding it, including emergency CERT teams ready to intervene as well as technical teams responding to the needs and demands of thousands of hackers. This joint effort underlines the gargantuan cooperative effort needed behind such an event to even be possible. It also and at the same time demonstrates how it exists free of state and corporate monetary influence. Refusing sponsorships, the Club manage to remain independent by relying on merchandise, donations and tickets sell. This demonstrates what Coleman (2017) calls the ability of hackers to demonstrate their own particular style of self-organization outside and independently of mainstream societal and institutional values. Similarly, to what Postill (2018) refers to as a "firm ability to produce existing alternatives to power while maintaining a capacity for self-survival" (2018, p. 18).

One of the many ways in which people attending Congress can get involved, besides donating their time to be become Angel or attend lectures, is to participate with the hundreds of assemblies[48] or sub-worlds present at Chaos Congress. Akin to decentralized

45 See: https://www.ccc.de/en/updates/2017/34C3-in-leipzig
46 See: https://www.lvz.de/Leipzig/Lokales/Hackerkongress-in-Leipzig-endet-mit-Besucherrekord
47 See: https://www.lvz.de/Leipzig/Lokales/Chaos-Computer-Club-trifft-sich-in-Leipzig-Hackerkongress-will-nach-vorne-schauen
48 See: complete list of participating assemblies at the 2017 Chaos Congress:

sub-action-fields, assemblies share different particularities depending on the interests and commonalities of their respective participants. They can be not only spaces where geeks, hackers and makers' cultures converge but also where cooperation and part of the Club's transformative capacity (Giddens, 1985) is both created and maintained. One such assembly, known as Milliways, was already familiar coming from my first visit to Congress back in 2013 during the year of the Snowden revelations. The name, itself, a reference to the restaurant found at the end of the Universe in Douglas Adam's *Hitchhiker's Guide to the Galaxy.* During camps, the Milliways assembly provides free meals to hungry hackers and free (as in free speech) beer during Congresses. For many reasons, Milliways has become an action-field found amongst the convergence cultures living inside camps.

Much well less known however and more important to this thesis, is that Milliways also became over time a platform and refuge for activists, hackers and geeks. The assembly contributes to the amplification of the voices of those targeted by states or corporations for their activism. The assembly for example hosts the Mail to Jail campaign in which Camp and Congress attendees are invited to sit down at the booth and write letters and tweets of encouragement to hackers and activists undergoing legal troubles. Moreover, financial donations are available for the FreeAnons campaign to support the legal costs of hacktivists. These campaigns while providing support help to ensure that activists do not feel socially isolated when targeted by state actions.

This collaborative aspect I believe reflects the same pattern of positive chaos and collaboration which the Club's founders themselves, as discussed in Chapter 4, once hoped to see emerge. Due to already knowing some people present there, I believed that Milliways would be ideal as a mean to "flesh out specificity" (Kubitschko, 2017, p. 187) of my subject. By narrowing down my research subject, this would in return allow for an easier detection of the underlining patterns and conclusions relevant to this research. On

https://events.ccc.de/congress/2017/wiki/index.php/Static:Assemblies

my first day, I met with a Milliways organizer who happily introduced me to long-term CCC participants who then proceeded to take me along for the rest of the conference to meet and talk with different assemblies.

As a civic-hacker organization, the CCC together brings a much-needed expertise to help “deconstruct the abstractness of a given technology” (Kubitschko, 2015) and consequently shorten the public-expert gap within society. However, the same interlocking arrangements described by Kubitschko which form its expertise also serve to educate and deconstruct the abstractness of today’s power relations related to surveillance and privacy. In other words, the expertise of its members during Congress serve to also shorten the gap between public and experts in fields that could be considered less technical. This can be seen for example in the lectures, workshops and events happening during Congress. Activities which touch on contemporary social and political issues in ways that differ from more mainstream sources.

Two lectures were particularly relevant and inspiring for this thesis. The first from former Lulzsec member Mustafa Al-Bassam, titled “Uncovering British spies’ web of sockpuppet social media personas”[49]. The lecture explicitly exposed how intelligence units who normally target terrorists were instead manipulating social media to turn public opinion against privacy hacktivists. Supported by previously released Snowden documents[50], Mustafa traced back a web of sock-puppets accounts belonging to the Joint Threat Research Intelligence Group (JTRIG), a unit within Britain’s intelligence agencies tasked with targeting, infiltrating and discrediting activists using “online techniques to make something happen in the real or cyber world”[51]. Mustafa’s work uncovered another dimension of modern surveillance. In this case, as opposed to seeking to prevent

49 See: https://media.ccc.de/v/34c3-9233-uncovering_british_spies_web_of_sockpuppet_social_media_personas

50 See: Snowden Docs Show UK Spies Attacked Anonymous, Hackers (NBC News) https://www.nbcnews.com/feature/edward-snowden-interview/exclusive-snowden-docs-show-uk-spies-attacked-anonymous-hackers-n21361

51 See: JTRIG tools and techniques (PDF) https://www.eff.org/files/2014/07/14/jtrigall.pdf

something from further happening, surveillance here sought to initiate actions against the surveilled to alter public opinion.

In contrast with my research, which focuses on actions directed against counter-surveillance actors in the real-world to prevent something from further happening online. For example, by targeting those in charge of communication, organizational infrastructure and platforms run by activists for their research. Besides system administrators, this also includes community moderators, researchers and activists behind popular social media accounts. This matters, in light of Mehrabov's (2016) suggestion for a need for more activists run platforms as opposed to corporate-run social media platforms.

While activists have increasingly leaned toward this view, those activists run platforms are also fragile. In part because those running them do not enjoy the same financial and legal defence mechanisms when the state comes knocking compared to other organizations. The implications for a potential and fourth generational wave of privacy activists mean that they must ensure to consider the potential survivability of the platforms they control before even launching them. Besides the security aspect, this includes social, political, legal realities such as where the platforms are hosted and ran from.

The second lecture related to my field of research touched on social cooling, or how our awareness of the surveillance data-driven economy is leading to conformity on a mass scale. It allowed me to better understand the relationship between mass and targeted forms of surveillance and their effects on the individual. As defined in Chapter 3 using a negative approach (Fuchs, 2011), surveillance (outside a heath context) is detrimental to human beings as it ultimately seeks to isolate and control. Asking "What does it mean to be free in a world where surveillance is the dominant business model?" Schep's lecture[52] directly touched on the long-term intended and unintended consequences of big data

52 See: Social Cooling - big data's unintended side effect - How the reputation economy is creating data-driven conformity. https://media.ccc.de/v/34c3-8797-social_cooling_-_big_data_s_unintended_side_effect

surveillance from both an individual and societal level.

Much like panoptic surveillance on a theoretical level is argued to isolate and provoke self-censorship and other self-regulation mechanism (Bentham & Božovič, 1995; Galič et. Al, 2017), the reputation economy brought forward using surveillance as a dominant business model also leads to conformity through “self-censorship and risk aversion”, behaviours which then become “the new normal”[53]. From a militant ethnographer standpoint, this picked my interest as I wondered: what are the lessons to be gleaned from those who their personal experience with surveillance however much extreme did not in their case lead them into isolation or conformity?

On Day 2, my guides and I had a discussion about my research and whether if I would like to talk to discuss my story and research on their live radio show. Considering my research asked participants to open about their own personal experience with targeted surveillance, my friends believed I should be transparent about my experience and personal story. As the interview was livestreamed during Congress, this also gave me an opportunity to detail the rationale behind my methodology as well as the goal behind this study. We thus spent an hour going through the details of my research, what I wanted to achieve with it and how I came about with the idea. Looking back, I realize this was the right move, as the literature itself demand that the ethnographer be transparent with its subjects to initiate a more trusting relationship.

As the interview went on, listeners asked question via Internet Relay Chat (IRC). An opportunity which gave me the chance to explain the reasoning behind my methodology, in this case militant ethnography, and how it differed from mainstream academia. This I felt was well-received, especially after I explained the specific goal of the activist-scholar: to help the community it studies retain and share amongst themselves the knowledge accumulated over the years. I believe the message was well-received despite the general

53 See also: https://www.socialcooling.com/

skepticism toward academia felt by activists in general. As I was told many times, my personal experience as an activist but also the method chosen were key factors behind why I was even listened to by the community to begin with.

On the third day, after re-working my interview guide in light of my recent experiences, I had the chance to do my first sit-down interview with a study participant. Participant 1 was introduced through someone at Congress whom we both knew and trusted, which helped break the ice and initiate the conversation. After explaining the topic and the reasoning behind the project, Participant 1 decided to participate under the condition that no recording could take place. An eventuality we had already discussed along with my supervisor that someone would be against recording the interview for privacy reasons. Considering the topic of surveillance and that participants would prefer a certain degree of protection to share their personal experience, my supervisor and I decided that the interview could be recorded taking notes only. Admittedly, I understood Participant 1's worries right away, seeing myself tell the same reasoning as an activist to a researcher years prior.

On the final day before heading to Berlin to celebrate the new year, I took a picture with other Congress participants as a show of support for Lauri Love. Love is an activist from England who then faced extradition to the United States for hacking charges following his alleged participation with Anonymous' related operations. To our pleasure and months later after his lawyer appealed the extradition, a judge ruled in Lauri's favour[54] with the charges against later dropped by the United States government[55]. On my return, I spent the next year (2018) deepening my literature review and improving my interview guide based on my experience at Congress. As well, I took the time to follow up on potential interview contacts referred to myself following my visit to congress, interviews conducted by phone.

54 See: https://www.bbc.co.uk/news/uk-england-42946540
55 See: https://www.bbc.com/news/uk-england-suffolk-43119355

Yet, an apprentice in the art of interviewing, I found the experience much more difficult than conducting the interviews in person, unlike what I first thought originally. It differs not only because of the lack of presence and visual of the other person, but also because encrypted communication can make for the recording and transcription of interviews more complicated than usual. There is also the irony of asking a surveillance victim to do an interview while using an encrypted communication application to ensure their privacy while demanding a recording of the conversation for the sake of transcription.

During the year following my first field-work at Congress, I also met with Maureen Webb (2020), the author of *Coding Democracy*, whose research looks into how hackers have helped disrupt the rise of surveillance and authoritarianism. Both of our research coincided in multiple ways, as mine focused on the experiences with targeted surveillance of privacy activists and hackers fighting the rise of western-based authoritarianism and surveillance within liberal democracies. They were also linked because, interestingly, both of our research led us to the same place although at different times. While Maureen began her research in 2015 in Berlin at the Chaos Communication Camp (where she interviewed participants and members of the Club), mine began two years later in 2017 at the Chaos Communication Congress. With the hindsight, it does seem logical to find targets of surveillance in places where those fighting against the rise of authoritarianism and surveillance assemble. My hypothesis, while already confirmed by my personal experience as an activist, had also been independently confirmed by another researcher. This of course marked a definite turning point in my research.

My idea to return to Germany and visit the camp in 2019 came from two CCC members. Those were the same friends who took me along during Congress, helping me introduce myself and my research to assemblies part of Congress in 2017. While my first visit to Congress as a scholar-activist helped break the ice and familiarize myself with the

two hats I was now wearing. Thus, the Camp provided an opportunity for me to find the rest of the interviewees I needed and show my commitment. During the time between Congress and the Camp, I also spent many hours lurking the various IRC channels and platforms used by members of #Milliways and other assemblies. This turned out to be helpful. Because of the way the Camp is set up, tickets are sold through a voucher system; meaning one person who buys a ticket can vouch for another and so on. My continuing presence during down-times helped me to obtain a voucher in time before tickets were ultimately sold out. The way the CCC works is that those tickets are first distributed to assemblies who then share them amongst their participants. This in return ensures an open but trust-based system where tickets are prioritized to members belonging to the constellation of communities attached to the Club. While this process might seem chaotic at first, in my experience it works. Although fieldwork can happen during a set time, for militant-based ethnography, to maintain involvement during and between down-times can be helpful, especially when new opportunities of research arise.

6.3 Telling the Tale — Second stop: Chaos Communication Camp, Brandenburg, Germany.

After having introduced how access has been established through my standpoint as an activist-scholar, this section will dive into the rest of the interviews, including my second visit to Germany at the Chaos Communication Camp. The most detailed description I have found portraying the Chaos Communication Camp and the experience one may feel attending was sent to me by a friend. The blog titled “Surreal Realism” or “Surrealer Realismus” in its original German[56], adeptly describes the surrealism felt when roaming through the Camp’s immense emplacement. The feeling that one is experiencing a “camp simulation” or as the author puts it, “a museum from the future exhibiting what once was”. In this case, decentralized clubs working toward common goals. Amongst the various

56 See: Surrealer Realismus: https://www.kambor-wiesenberg.de/surrealer-realismus/

assemblies can be found near the middle of the camp the iconic CCC rocket ship often surrounded at night by smoke, laser lights and revellers dancing to nearby music. As one long-timer Camp participant explained, the rocket ship will symbolically reactivate and transport the aliens — in other words those attending the camp — back to their planet once it is over. Because for many, the experience is much like stepping out of the matrix for a few days, only to painfully come back to reality when it ends.

The Camp, similarly, to how Coleman (2009) describes hacker conferences, is also the celebration of a shared and unique life-world. One which provides the necessary context to contextualize resistance against surveillance through the debates surrounding it. In many ways, this helps generate support for those targeted as a result of their actions. However, this can sometimes bring out tensions amongst participants depending on the world-views one bring from the outside. At my arrival in the Camp, I already knew where to go based on the messages I received from the two friends who I did the interview with during Congress. As I later discovered, if you do not have a place to settle your tent or have an assembly you know who can welcome you, Milliways will welcome you. I thus decided to pitch my tent at Milliways not far from the tent-kitchen they had installed to prepare meals to feed hungry hackers during the entirety of the Camp. My two friends, who back during Congress served me as guide, again generously proposed to help me with my thesis and introduce my project to people they believed would be interested to participate. Hence, I cannot overstate how without their help my research project would have likely not been possible.

Going back to Chapter 2 and Mehrabov's (2016) research on the failures of mediatized activism in Azerbaijan and Turkey, we learned how activists should tend toward a new model of practice. For example, by reconsidering their relationship with for-profit and state-surveillance owned social media platforms when seeking to organize.

Ideally, this model would aim to develop new relationships and connect the rest of society "in concert with the activists of different social movements" (2016, p. 511). When walking through Congress and Camp, I thought of this model reminding myself of Coleman's (2017) explanation of how hackers "avoid defining (and thus policing) the broadly defined ideologies that all their participants must share" (2017, p. 99). They achieve through pragmatic cooperation and wilful political action between radical and less radical ideologies.

To achieve longstanding and sustainable community-based collectives where activists can feel safe to exchange and participate requires the necessary infrastructure to help maintain such an environment but also trust. With time, such trust can be earned enabling for a space to emerge in which cooperation between its members and the public is possible. The Club today can be said to enjoy such a space thanks to the combined effort and work hours of a multitude of volunteers who ensures an event like the Chaos Congress happens smoothly. For Congress as well as the camps, the infrastructure required is of course not only physical but also virtual, allowing for talks and lectures to be uploaded and translated in various languages unto the Club's online media platforms ensuring a discussion with those watching from afar. For these reasons I believe both an online and offline dimension is essential for activists-run platforms to survive, as each dimension re-enforce each others. Because there is a need for more online activist-run platforms may also be directly related to the nature of modern surveillance today as the line between government and corporate surveillance becomes blurred.

6.4 Interview findings and analysis

The interview questions[57] centred around the research questions and themes reviewed in the first half of this thesis. This includes issues dealing with isolation and

57 Available in **Appendix 4 (**p. 123).

privacy, their views on the media and surveillance, the need for activist-run platforms. Moreover, I also asked in their view how participants defined modern surveillance. Participants interviewed have gone through difficult experiences, sometimes involving lengthy prison sentences and fines, as well as years of constant surveillance for whom sometimes still continues to this day. These interviews thus offer a glimpse into the views of counter-surveillance actors but also the meanings they have attributed to their experiences.

Theme 1: Control mechanisms

I strongly suspected how pertinent to my research my first interview with Participant 1 might turn out after hearing about Participant's 1 experiences. Later, near the end of the research, I realized it was an early and fairly representative outcome of what to expect for the remaining interviews. Especially on the recurring themes touching on isolation induced by surveillance, control mechanisms against the negative consequence associated with surveillance as well as on the role of the media and the press. For Participant 1, knowing how to remain in control is perhaps the most important point to remember when targeted by surveillance. Police may engage in different tactics to prolong the incertitude one feels by expanding the time-frame between surveillance, arrest and charges. Each stages, Participant 1 explained, bring forth sentiments of incertitude authorities may exploit to sabotage your own legal case.

Tactics can include "waiting it out" as strategy to delay court actions, as authorities may use the press to sabotage your own moral by letting you know they "control" the narrative (Participant 1 interview, 2017). Giving the Malwaretech situation as an example[58], Participant 1 explains the purpose behind this strategy as waiting for you to commit a mistake while you are stalked by the press or agents. As Participant 1 said, while the police cannot directly leak information about you, the press and more often than not,

58 See: https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/

tabloids can and will. In Participant's 1 claims, information gained by the police can be leaked to the press, who in effect end up acting as proxy for law enforcement to circumvent investigating protocols and privacy laws.

This press/law enforcement tandem, he says, is often used against activists to impose social isolation. Because of this, having a strong awareness of your rights can go a long way in maintain control. For this, Participant 1 repeats, finding actual expert counsel and independent journalists you can trust become tools at your disposition to maintain your balance. Because of the rush to publish and editor pressure, most mainstream journalists he claims cannot be trusted to protect you as their sources. They often make mistakes, misrepresent what you say or sometimes will outright cooperate with law enforcement. For others, like Participant 3, how you go about selecting journalists you talk to also matters as not all journalists or news organizations may be worth your time and trust. In other words, one must investigate the investigative journalist first. For Participant 3 and others, this means looking at both the reputation of the individual journalist and the news organization for which they work for:

> "It all depends on the reputation of the journalist interviewing me. Because if they are really new I am much more careful due to them lacking experience. If they are not new and have experience, I always check their background and where they're coming from (vice, wired, motherboard). For example, I would never in my life give an interview to Russia Today or Sputnik, but if someone from Motherboard, Wired or Vice came to talk to me, I'd be much more inclined to talk considering how their reputation precedes them" (Participant 3 interview, 2019)

For Participant 1, a good deal of advice given to activists are often wrong. This is because he claims not all lawyers or even experts have the best intentions in mind: "Most advice we give to activists are garbage" (Participant 1 interview, 2017) he says, as he makes a reference to the often-repeated catchphrase in the privacy community to "Use signal, use Tor"[59][60]. As Participant 1 explained, exclusively using encryption applications

59 See: https://medium.com/@amstanley/i-asked-my-friends-to-use-signal-use-tor-and-this-is-what-happened-7df616166ef9

60 See also: https://dev.to/ondrejs/effective-communication-security--beyond-use-signal-use-tor-55hk

can sometimes contribute to the isolation instigated by targeted surveillance. As one feels surveilled, a tendency to double-down by exclusively using security applications, such as encrypted messaging apps, can emerge. The problem rests in how applications such as Signal often function within a so-called silo environment. Meaning, if the other person does not have the same application installed on their device the encryption feature will not be possible. This influences communication, as activists trying to protect themselves from targeted surveillance may further self-isolate if their friends or family also do not use the application.

For Participant 1, readiness and preparation for any eventualities matters. As Participant 1 explains, much of the uncertainty caused by surveillance or the potential of surveillance may come from different directions. For example, such as living under “the constant fear of having your door kicked in” (Participant 1 interview, 2017). This can happen, as he claims, in the early morning hours or sometimes, by having agents dump folders of blank papers on you — for example when inside an interrogation room — to insinuate they know more about you than they actually do. In other instances, police may also attempt to mess with your sense of time. Because of this, having the right people to turn to who can provide you with the much-needed help and counsel you require can be essential.

Another control strategy for Participant 1 refers to carrying pre-prepared statements whenever outside or at home in the likelihood that the situation presents itself with either the police or the press. As Participant 1 says, it helps to be surrounded by people who have previously went through similar experiences. Giving the CCC as an example, this can help you keep both feet on the ground. While The Press/Law Enforcement synergy mentioned earlier can be used against you to create social pressure on yourself, your friends and your family, you may sometimes get some positive press. However, anything

negative the press can find about you will be made to appear ten times worse, stresses Participant 1.

As Participant 1 explained, the goal of those conducting the surveillance is of course to isolate you. Something which you must, as Participant 1 repeatedly tells me, combat at all cost, stressing “don’t get backed up in a corner” (Participant 1 interview, 2017). While authorities may try to make the sole act of being around you a risk, for example by having your friends get “randomly searched” (Participant 1 interview, 2017). Therefore, one must remember to avoid at all cost falling into another vicious circle of self-isolation. The risk is to end up (falsely) thinking you have nothing to lose. As Participant 1 reminds me, many of those targeted by surveillance cannot whist-hand the pressure and often go into different coping mechanisms, some of which less healthy than others. Nonetheless, it helps to know beforehand ways to overcome those eventualities. One needs a feeling of hope, something you can hold on to for the future, concludes Participant 1.

Theme 2: State-corporate surveillance relationships

For Participant 3, despite the amount of information unveiled by the Snowden revelations, most people have remained ignorant of the consequences of these revelations for the future of liberal democracies. In the participant’s view, people tend to keep on using the same applications and services that do not protect their privacy as before, mostly because alternatives are often too inconvenient for them to use:

> “They tend to go from statements such as having nothing to hide because it makes life easier as well. They think if they start using something else, that they might also miss out on things...for them, it is often too much effort to introduce something new in their life, as most just want to keep the old ways as long as they can keep living their lives and not get in trouble. The only way this situation might change is if they get personally in trouble at some point and have to alter their own habits to protect themselves.” (Participant 3 interview, 2019)

For Participant 3, besides the manner by which the media reported on the actual

revelations, how the media curated those revelations also became problematic. In Participant 3's view, this may also explain why the Snowden revelations did not have as much a positive impact on the behaviour of individuals. As Participant 3 explains, because the revelations didn't expose any actual victims of surveillance, this meant that for many people it also became harder to understand how it affected them personally. To quote Participant 3: "if there had been decent proof of victims of surveillance maybe people would think twice before doing something" (Participant 3 interview, 2019).

A third theme of this thesis, as discussed in **Chapter 3** on privacy, pertained to the inherent non-neutrality of surveillance technologies as suggested by Garfinkel (2001) and Cohen (2012). This includes the consequences of the non-neutrality of surveillance technologies versus the ability of the citizenry to defend itself against the combined powers of public and private entities. This includes the social and political implications these non-neutral technologies have on the survival of liberal democracies. As argued before (Garfinkel, 2001), privacy ought to be defended against the inherent non-neutrality of technology. Especially when considering how such advances, he claims, have in the past almost exclusively been used to manipulate and control nondeterministic processes (2001, p. 320). As Garfinkel argued, taking the position that technology is neutral can be a gamble we take at own peril, as doing so can have grave consequences for the informed consent of the citizenry. A position made clearer when examining answers from some study participants on the nature of surveillance technologies today. However, contrary to what Garfinkel (2001) proposed (2001, p. 525), participants tend to not believe that a legislative solution to be possible.

As succinctly explained to me by Participant 2, surveillance and propaganda technologies developed by the U.S. government or sometimes for the US government by private companies. For example, instances such as with the United States Central

Command (CENTCOM) in 2011[61]. The issue lies in how these technologies tend to inevitably fall into the hands of "the worst people in the world" (Interview with Participant 2, 2019)[62]. Even as the U.S. government claims these technologies won't be used against their own citizens, these "well-crafted means of disinformation, of deceiving the public" (Participant 2 interview, 2019) tend to inevitably fall into the hands of private companies. Unaccountable to the public, these private companies then sell those technologies for a price to dictatorships abroad[63]. As Participant 2 explains:

> "these are technologies that simply cannot be used for what we would call good. They cannot be used to improve informed consent. Unlike a gun, which can be used for any number of different things, including liberating countries from dictatorships, it is something that is only meant to deceive and confuse. And once those things get out, which they have and start developing further, they never go away. They're out there, it's software." (Interview with Participant 2, 2019).

This predicament affects the ability of both the press and the people to resist. The latter which simply can no longer "defend themselves" (Interview with Participant 2, 2019) against state-corporate surveillance partnerships. The synergy at play behind surveillance and targeted disinformation technologies means even in the unlikelihood of all three branches of the United States government taking a stand against. Simply put, there is no putting the toothpaste back in the tube. As Participant 2 explains during the interview:

> "You've got several hundred companies out there in the US alone, out of a couple thousands contracting firms, who have pretty impressive capabilities, who have already sold them abroad, and the genie is not going back in the bottle." (Interview with Participant 2, 2019)

When asked on this issue, participants understand how private and state surveillance, including disinformation, often tend to overlap as they simultaneously depend on one another to work. For instance, one could argue Cambridge Analytica would have had a much harder time sowing confusion without the data accumulated from the

61 See: Revealed: US spy operation that manipulates social media https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks

62 See: https://www.eff.org/deeplinks/2020/10/latin-american-governments-must-commit-surveillance-transparency

63 See: German Made State Malware Company FinFisher Raided https://netzpolitik.org/2020/our-criminal-complaint-german-state-malware-company-finfisher-raided/

surveillance Facebook generated from their users. Surveillance which, as the Snowden revelations showed as discussed in previous chapters, is imposed by state-sponsored surveillance programs such as Prism to which agencies like the NSA heavily benefits from. As intelligence agencies impose strict surveillance systems to companies, those have in return recuperated the cost of these surveillance infrastructures by selling user data to the highest bidder. In this case, government imposed regulations which would protect privacy becomes an impossibility considering the state's conflict of interest, being together a regulator and main beneficiary of said surveillance. A situation which I referred to in the first half of this thesis as inverted regulatory capture. As opposed to coming from the outside such as in the case with regular regulatory capture, as with the oil industry and environmental regulations, the regulatory capture in this case happens from within. This conflict of interests means that a legislative solution to the problem of surveillance and disinformation remains unlikely.

As Julian Assange once explained[64], the economics of both surveillance and disinformation have become another weapon in the arsenal — along with bombs, guns and cops — to enforce control over the population. Hence, as propaganda expert Dr. Emma Briant said in an opinion piece published in the Organized Crime and Corruption Reporting Project: "Governments are failing us,"[65]. A failure happening while Cambridge Analytica spin-offs and data firms like Palantir who are both enabled by data gained from mass surveillance, "continue to provide training, or engage directly, in tactics to influence the behaviour of citizens" and this without any kind of accountability[66].

Thus, the relationship between disinformation and surveillance becomes two-fold. First, knowing what is going on as a result of mass surveillance allows disinformation to

64 See: https://twitter.com/wikileaks/status/1136963035703185408

65 See: Governments Have Failed to Learn from the Cambridge Analytica Scandal https://www.occrp.org/en/37-ccblog/ccblog/13225-governments-have-failed-to-learn-from-the-cambridge-analytica-scandal

66 See: Forged letter warning about wolves on the loose part of Canadian Forces propaganda campaign that went awry https://ottawacitizen.com/news/national/defence-watch/forged-letter-warning-about-wolves-on-the-loose-part-of-canadian-forces-propaganda-campaign-that-went-awry

become a more effective tool for control. As a result, the negation of privacy by illegal mass surveillance makes democratic societies vulnerable to manipulation on a grand scale. In the view of Participant 2, we now witness a powerful ability to confuse actual events (including the understanding of said events) or even sometimes to manufacture events in blunt ways through unsophisticated means. To quote the study participant, this surveillance-disinformation relationship “makes it that much harder for the citizenry [and journalists] to understand or get a good sense of what’s going on” (Participant 2 interview, 2019). In return, this confusion also makes it harder for either the press or people to differentiate between true and false. A knowledge disparity and credulity gap emerges due to a lack of contextual information. Together, the people and the press then lack the ability or the competence to speculate about what is technology and politically possible. For example, by failing to grasp the repercussions behind the enormous sum of money invested to both research and test the kind of technology available today within surveillance and disinformation industries. Unfortunately, as another participant perhaps cynically explained during a public discussion on IRC, “people are often gullible in the wrong places and skeptical in the wrong places” (IRC discussion, 2019).

The confusion instigated by surveillance and disinformation in return makes it even harder for most people to understand the severity of the issue in question. This is because those supposed to cover these injustices often fail to grasp their severeness on both a short and long-term basis. This confusion inevitably influences how news are reported and analyzed. For example, in the way such news are received and interpreted by the people. This failure to comprehend can be attributed in part to an incomprehension regarding such issues by those who report them. For instance, participant 2 cites the example of Thomas Friedman from the New York Times. Friedman who, during the Snowden revelation[67] cited the creator of The Wire in an editorial in which the author show skepticism toward the

67 See: Blowing a Whistle, Thomas Friedman, 2013. https://www.nytimes.com/2013/06/12/opinion/friedman-blowing-a-whistle.html

dangers imposed by surveillance. As Participant 2 notes, both these people ought not to care about surveillance as they together share a perspective stemming from a privileged position. In this case, the former being a Pulitzer prize winner working for the New York Times and the latter, the creator of a popular TV show.

Theme 3: Collective privacy

Similarly, Participant 2 believes most have legitimate reasons not to worry about targeted forms of surveillance. This is not to say that one should not be concerned about surveillance on a personal level, but that they are not concerned for the wrong reasons. What should concern them, Participant 2 explains, is surveillance perpetrated against those making important discoveries, what he calls “the pentagon papers style of people” (Participant 2 interview, 2019). This, of course, refers to Daniel Ellsberg, an analyst previously charged under the Espionage Act of 1917 for leaking a top-secret Pentagon study about U.S. involvement in the Vietnam War. Those are the ones as Participant 2 claims which surveillance seeks to primarily isolate and thus, censor. In other words, those who “take risks to move things forward or keep things from getting worse” (Participant 2 interview, 2019) and consequently help citizens to retain informed consent. For Participant 3, this also includes hacktivists, as “they have the will, the power but also the knowledge to make a change”, including the capacity to “disrupt normal life if necessary” (Participant 3 interview, 2019). These abilities may not always be technical, but also political. To provide an example, Participant 3 gave the case of Iceland which arguably became the only country to jail any bankers after the 2008 Great Recession. As Participant 3 explained, this particularity can be attributed to the unique influence of the Pirate Party, who then had many of its members in influential position within the government. When asked why in their view governments dread hacktivists and counter-surveillance actors, Participant 3 explains:

> "I think governments are afraid of hacktivists in general because they have the knowledge and power to make a change or to disrupt life for something better in the future. Government powers want to prevent that because they want to try to keep everything from changing. Of course, they also want a descent life, but they want to achieve this by keeping the old ways and through means which are not always humane or descent, like surveillance or through harassing hacktivists who want change. As long as this doesn't change, hacktivists will be hunted." (Participant 3 interview, 2019)

Consequently, as one participant said during a discussion on a public chat with other activists, privacy's value is not about "what you've got to hide" but instead, about "what you might create and do with other people" (Discussion, IRC, 2019). A position which helps to make Solove's (2011) position, who posited that even if you got nothing to hide, privacy remains valuable on a collective level, a bit clearer. Since not everyone can defend themselves, as others like Solovjovs (2019) have argued, individual privacy if consent based also serves to safeguard the collective by providing herd immunity to the group at large[68].

This factor, of what you may create or do with other people, ties in with what Cohen (2012) called the "continuing vitality of political and intellectual culture at large" (2012, p. 1906). More precisely, the value of privacy becomes clearer when understood on both an individual and collective level and as an essential factor to the good functioning of democracy. While most need not worry about targeted surveillance, they gain in safeguarding privacy for those who take risks, the so-called "pentagon papers" style of people. The activists, researchers, whistle-blowers, and independent journalists working to ensure public institutions and corporations remain accountable. An important point considering the inability of the state and legislative bodies to rein in the surveillance and disinformation industry. In the view of Participant 2, the only way this tendency can reverse itself (if it can) depend on if private companies and state actors caught doing illegal surveillance and disinformation receive the same treatment that activists, who once

68 See: BalCCon2k19 — Solovjovs, Kirils — NOTH1NG T0 HID3 https://www.youtube.com/watch?v=Af3R5X4JPzg

exposed the surveillance-disinformation industry, have received by the U.S. government:

> "When they are caught they have to be punished essentially, just as the government comes after us and try to make an example of us by putting us a hundred years in prison, these people... it has to be viewed as seriously as state views espionage. Because it is treason against everyone, it is treason against democracy, it is treason against informed consent to do these things." (Participant 2 interview, 2019)

Companies and state actors responsible for surveillance and disinformation are rarely if ever held accountable for their actions the same way activists, journalists and hacktivists are when caught exposing state and surveillance industries. To make this view clearer, one may look at the case of Peter Thiel's data-mining company Palantir, whom activists from Anonymous exposed in 2011 in a series of counter-surveillance operations against HBGary[69], the U.S. Chamber of Commerce and Palantir (the latter which includes as backers the CIA's venture arm, In-Q-Tel)[70]. Through leaked documents, the operation by the counter-surveillance actors demonstrated how data-mining companies such as Palantir helped target activists with harassment, intimidation and plans to use information on journalists' children as leverage. In response, the company's representatives then went into full denial by blaming the stratagem on a rogue employee. When further documents got exposed, the company became forced to admit how their plans to spy on journalists and activists had not, contrary to their previous statements, been the work of a single rogue employee but instead, the work of the company's chief lawyer.

As Participant 2 remembers, by that time the press such as the New York Times had already moved on the another news cycle. When the company resurfaced in the news after the Cambridge Analytica (CA) scandal, Palantir resurfaced in the news. This time, in a plot to help CA siphon the information on more than 50 million Facebook users and U.S. citizens[71]. An operation winch ended contributing to the election of Donald Trump. Once

69 See: HBGary Federal hacked and exposed by Anonymous https://nakedsecurity.sophos.com/2011/02/07/hbgary-federal-hacked-and-exposed-by-anonymous/

70 See: How Peter Thiel's Palantir Helped the NSA Spy on the Whole World https://theintercept.com/2017/02/22/how-peter-thiels-palantir-helped-the-nsa-spy-on-the-whole-world/

71 See: https://techcrunch.com/2018/03/27/facebook-data-misuse-scandal-affects-substantially-more-than-50m-claims-wylie/

again this time, accountability failed. When the scandal hit in 2016, institutions like the New York Times, who had years prior previously exposed Palantir thanks to the work of counter-surveillance actors, didn't connect the dots. This despite their own previous reporting to show how the data-mining company repeated the same pattern of excuses as before. This time, by blaming the work of a rogue employee, who then got promoted months later.

In this case, The New York Times, as well others, did not even report on their own previous reporting from 2011 to provide the right context for people to understand the severity of the issue. As Participant 2 explains, too often the press finds itself either unable or unwilling to provide accountability by failing, sometimes on purpose, to connect the dots between events even from within their own reporting:

> "They [The New York Times] can't go back and acknowledge it, because to acknowledge that it happens is to really pull the bandage off of the whole sort of half-hazarded modern journalism industry found today in this country [The United States] and the west [...] And that's we're at, a point where they cannot as an industry afford to go back and say 'yes these things happen, here's how it fails even as the work had been done for us [by activists]" (Participant 2 interview, 2019)

Theme 4: Activists-run platforms

This point of contention connects to another theme of this thesis related to the need for more activists-run platform. As Participant 2 stresses, the inability of institutions to do their job means that, for activists, they "have to get creative in terms of building up structures that can do this kind of work and also can marginalize and chastise these institutions that have failed over and over again." (Participant 2 interview, 2019). In this case, activists-run platforms become not only needed for organizational purposes or to simply avoid mediatized surveillance. For Participant 2, these platforms are in need especially to help reverse the tendentious disaster we now face. Especially when considering the inability of legislative bodies, as well of the fourth estate, to impose some form of accountability against what he sees as treason against both informed consent and

democracy.

Consequently, many of the participants interviewed had in fact been running activist-run platforms of their own, allowing activists to organize and work toward exposing surveillance and disinformation industries. Unsurprisingly, those who become the target of surveillance and heavy-handed state actions are often those who also build and maintain such platforms. This was the case for three participants interviewed, who all have endured various forms of persecution aiming, they claim, to hinder the ability of activists to build and maintain such structures. The lesson for counter-power groups, including those likely to belong to future privacy waves of activism, is to consider how vulnerable their platforms (and themselves) are before even launching them. Mostly because, chances are they together will inevitably become the target of both surveillance and disinformation campaigns. A point which virtually all participants agreed on.

This in turn connects with another theme, in which participants have attributed positive meanings out of a seemingly negative experience being on the receiving end of both surveillance and legal prosecutions. As one participant, who went through months long court cases due to his involvement in maintaining collaborative platforms used by activists admitted: “the intensity of surveillance proves you right” (Participant 3 interview, 2019) by telling you also that what are doing is actually working:

> “The level of threat and the extreme measures the state takes to shut us down can be interpreted to illustrate that we can effect change and make a difference.” (Participant 3 interview, 2019)

The same way, excess in prosecution as Participant 2 adds can also serve to create stories of martyrdom, as prosecution provides an opportunity to revisit discoveries and findings from activists by the press. Discoveries often overlooked by the media when they jump into a new news cycle. Even prison itself in his view can be turned into a positive experience of resistance to one’s cause. In a participant’s words, “If you play the long

game, going to prison for a few years is a bit of a boost." (Participant 2 interview, 2019). Indeed, for some participants, there are mechanisms by which one can turn heavy prosecution and surveillance into something positive to one's cause.

Managing to find positive out of the negative can help counter surveillance's more pernicious effects. Notably, if you can manage to use such situations to connect with other organizations and individuals to help break isolation. Finding like-minded people become an important facet to help combat social cooling effects and isolation stemming from surveillance and heavy-handed state actions. As one participant puts it, there is a reason why we "Somehow, we all ended up at Milliways" (Participant 7 interview, 2019), adding also that in their case, it may even have saved their own life. This acknowledgement is not too far-fetch when reminding oneself of the context surrounding the death of the late writer and author Ernest Hemingway, who after his passing his friends admitted regretting not having believed he underwent intense FBI surveillance. Surveillance which, unbeknownst to his friends, had then taken a toll on the writer's psyche. To the point where they believe the surveillance he endured may have the main factor behind him taking his own life[72][73]. While close friends and families may often lack the context to understand what one may go through, groups such as the CCC and assemblies not only help one resist and remain more n control of the situation but also, survive.

72 See: https://www.telegraph.co.uk/culture/books/booknews/8614094/Ernest-Hemingway-driven-to-suicide-over-FBI-surveillance.html

73 See: https://www.nytimes.com/2011/07/02/opinion/02hotchner.html

Chapter 7: Discussion & Conclusion

"If this government ever became a tyranny, if a dictator ever took charge in this country, the technological capacity that the intelligence community has given the government could enable it to impose total tyranny, and there would be no way to fight back because the most careful effort to combine together in resistance to the government, no matter how privately it was done, is within the reach of the government to know. Such is the capability of this technology." — Senator Frank Church, 1975[74]

This study aimed to explore the meanings, lessons learned, and control mechanisms inferred from the experiences of counter-surveillance actors involved in the third-wave of privacy activism (Postill, 2018). It has identified mechanisms to help deal with issues related to isolation and so-called social cooling effects based on individual perspectives. Furthermore, it explored the ways by which hacktivists and privacy activists

74 "The Intelligence Gathering Debate". NBC. August 18, 1975. https://www.youtube.com/watch?v=YAG1N4a84Dk

have dealt with the negative consequences associated with surveillance.

Moreover, this study sought to establish how the views of privacy activists and hacktivists' compare with the current literature within the fields of communication and surveillance studies. Diverging from current thinking, this study sought to establish a new perspective going beyond surveillance capitalism (Zuboff, 2015) as a lens to understand modern surveillance. A new perspective achieved using militant-based ethnography as this thesis' main research method (Juris, 2007). Judging the current literature on this subject as inconclusive in part due to a lack of counter-power based viewpoints within academic and mainstream discourse, this thesis asked the following research questions:

- (RQ1): What are the experiences of counter-surveillance actors in resisting modern surveillance?
- (RQ2): What types of positive lessons and views regarding the state of modern surveillance can be gleaned from their experiences?
- (RQ3): How do their experiences diverge from or relate to known concepts within the literature within the fields of media and surveillance studies?

7.1 Empirical findings: theoretical/policy implications

The main empirical findings of this study have been summarized in the introduction of **Chapter 6**. This section will thus lay out a synthesis of the findings considering the arguments presented in the first half of the thesis, more specifically in **Chapter 2**, **3** and **4**.

First, the theoretical framework of this thesis as presented in **Chapter 2** provided the groundwork to establish a theoretical counter-viewpoint to mainstream definitions of surveillance. Going beyond surveillance capitalism, it puts into perspective the release of the Snowden documents in 2013 and the events surrounding the 2016 election in the United States. To help achieve this, it introduced the concept of inverted regulatory capture to help clarify the symbiotic nature of the state-corporate surveillance partnerships

(Kubitschko, 2015). A concept introduced in light of the perceived lack of governmental regulations to protect individual and collective privacy.

Second, borrowing the allegory of The Golem (D'Souza, 2019) — a symbolic intermediary acting as an in-between Hobbes' Leviathan and the people — this thesis explains how corporate surveillance effectively acts as a proxy for the State to protect itself from accountability by The People. Both at the same time a benefactor of surveillance and an entity supposed to ensure personal and collective privacy rights, the State becomes in effect entangled in a conflict of interest. A position which prevents it from ensuring its end of the social contract. Pitted against this form of networked authoritarianism (MacKinnon, 2011), the repression against privacy activists, as notes Mehrabov (2016, p. 500), also serves to "affirm the futility of activism to a disillusioned public" (Pearce and Kendzior, 2012, p. 284).

Second, **Chapter 3** introduced a negative approach (Fuchs, 2011) to help define the concept of surveillance. In the chapter, I defined surveillance as an inherently negative concept harmful to human beings. Using the concept of Social Cooling (Schep, 2017), a theory discovered during my visit at the CCC Congress, I explained the pernicious effects of surveillance. This, from both a collective and individual level, touching on issues of self-censorship and isolation, among other ills. From an individual and collective perspective, I explained how privacy should be valued together as both an individual and collective quality.

Third, **Chapter 4** suggested how we can, as academics, learn from counter-surveillance actors, as well as the ability of the hacker mindset to find novel solutions to existing problems. I hypothesized how organizations such as the CCC can offer us with an avenue to learn from those who have been at the forefront of the fight against surveillance. In this chapter, I defined the CCC as a constellation of counter-surveillance actors. Helped

by a strategy of positive chaos, they have helped bring about change and conscientization toward contemporary issues independently of the dynamics and influence of state and corporate interests. Based on my personal experience, I theorized that counter-surveillance actors belonging to the third wave of activism could provide us with valuable insights to better understand contemporary surveillance. This also includes how to better resist its negative consequences on both a communication and organizational perspective.

Fourth, **Chapter 6** presented my findings through the telling of an ethnographic tale, which is followed by an analysis of interviews conducted during and after the 2017 Chaos Congress and the 2019 Chaos Communication Camp in Germany. This study (based on answers taken from interview participants) clarifies unintended consequences associated with the current symbiotic public-private nature of contemporary surveillance and disinformation campaigns. Including but not limited to, the reasons why for the unlikelihood of a policy-based solution. Contrary to Garfinkel (2001), participants do not view a legislative solution to the problem of surveillance as possible or likely, although they confirm the author's view on the non-neutrality of surveillance technologies.

Furthermore, the study suggests how negative effects associated with surveillance on the individual can be remediated, or at the least managed, by international and collective-based solidarity. It argues how the CCC as an organization provides a platform by which counter-power can resist such effects with physical and virtual based collaboration. Finally, going against the "nothing to hide" meme previously described, it proposes a re-thinking of privacy-based policies, one which would consider individual privacy as essential to provide herd immunity. An immunity which serves the collective against both the pernicious effects of disinformation and mass-surveillance.

7.2 Future research

The scale of modern surveillance and the debate surrounding are both expansively

complex. I have attempted to provide perspectives from counter-surveillance actors, activists and hackers with unique insights based on their work and participation inside known counter-power movements. Perspectives I believe can help fill a gap between academic and activist knowledge within the current surveillance and communication literature. However, because this interpretative and critical study focused on a small minority part of many sub-worlds inside the counter-surveillance ecosystem, it does not claim to represent it fully. Further research may want to explore the personal experiences of other and less-represented groups. There is also a need for more individual perspectives coming from other disenfranchised groups and racial minorities often times unfairly targeted by the same corpo-state surveillance relationships. The views and the meanings derived from their own experiences could enlighten us further about the role played by power and symbiotic state-corporate relationships.

7.3 Discussion

Embracing my new role as an activist-scholar, I began this research carrying a set of assumptions composed of my own personal experiences and understanding of the literature surrounding surveillance and communication research. Although familiar with my research subject, the nature of online activism implies a certain degree of anonymity together with the people you work with and have known for years. For those targeted by the state and corporations via the judicial system and the media, to have your real name exposed publicly, while disturbing, can allow one to receive support. This can take the form of help and solidarity from communities and non-governmental organizations becoming aware of your case. There exists however another group of individuals targeted whose stories and experiences remain unknown to the public and thus, overlooked by researchers.

Falling into the second category, my personal experience with surveillance — which

led me to this thesis — had remained unknown even to most of my peers. Luckily in my case, I managed to find support and help from communities like the CCC who ensured I did not go through this experience alone. However, many among us may not have enjoyed the same opportunities as I did, making their stories and experiences more difficult to uncover. Although what Frey (1996) and others have written certainly rings true — familiarity with the group you study can help one get access — within this particular context the experience also came with its fair share of challenges. Realizing my situation, I had to find a way to join the two worlds I had for so long carefully kept apart. This, of course, to gain the trust needed from my peers to complete this research. Thus, from the onset, openness and transparency about both my background and experience certainly played in my favour. Noticing my struggle to find participants to participate in this research early on, a CCC organizer offered some suggestions. For example, by saying I first had to first be open about my story. Since, he explained, my familiarity with the community or my status as a researcher would not be enough to break the ice.

With this optic in mind, I began to reflect on what would convince me, as a privacy activist, to participate in a research such as this one. I remember how skeptical I used to myself toward academics demanding interviews; only for them to publish a paper or an article only to never be heard from again. This would often influence how seriously we would approach their own research questions during interviews. Maybe due to karma, throughout my fieldwork for this research this skepticism often came back together with questions regarding objectivity and the current state of academia. One study participant and I had a long discussion about the state of the relationship between academia and activism. What in my view helped counter such skepticism is when I explained the goals of Jeffrey Juris' method of militant ethnography. A method which denies upfront notions of objectivity by deliberately stepping on the line between activism and the academy.

Thankfully, this argument became well-received by the vast majority of the people I spoke to during field-work, especially when announcing my role as a participant observer. For the study participants, many have said how they would not have engaged with me at all without them learning about my own previous experience as an activist which gave weight to the rationale behind my research methods. Without the help of trusted third parties when introduced to would be participants and groups I observed, this thesis would not exist. Much like the voucher system used by the CCC for camp tickets, this particular trust-based system ensured that my words would not just stand on their own.

With Signal and other encrypted communication applications, I could not record the interviews with another application, as signals block third-party applications from recording encrypted calls. This forced me to find a way to record both my voice and the voice of the interviewee using two separate devices using a computer and a physical voice recorder. This made the transcription process more laborious than it should have due to difficulties syncing the two recordings together along with other technical issues. Another hurdle encountered along the way had to do with finding people who would agree to talk about their experiences and having them recorded at the same time. A process which makes for interviewing in academia difficult when dealing with more sensitive subjects as they relate to privacy and surveillance. Something which, due to my background as a privacy activist, I completely understood. For these cases, I tried to accommodate people as much as possible whenever I could so that they would feel comfortable throughout the process.

7.4 Conclusion

Lastly, this interpretative critical study of contemporary surveillance sought to establish how counter-surveillance actors, themselves the target of repressive surveillance, define contemporary surveillance considering their experiences. Using Fuchs (2011) negative approach to define surveillance as pernicious to human beings, my goal

aimed to glean from the participants' experiences positive lessons and control mechanisms. This based on their own experiences as privacy activists and counter-surveillance actors. By learning from their struggles, I hypothesized how both researchers and activists may gain from reaching a better understanding about where activism and academia meet on the topic of contemporary surveillance. This includes issues and subjects touching on isolation, social-cooling, and privacy. Contrary to my assumptions, I found that the two realms often overlapped when taking the time to dig deeper into the literature in comparison with what counter-surveillance actors believe.

Analysis of the participants' interviews demonstrates a profound skepticism toward liberal democracies' ability to reach a legislative solution to issues surrounding contemporary surveillance and disinformation. Gaining an understanding of current events helped by mass surveillance allows data-mining companies, marketers and state actors to more easily disrupt public discourse. A knowledge disparity gap helped by an incapacity by the media to connect the dots on the long term and between reporting. The rapid mediatization of society coupled with the centralization of social media platforms have allowed for an easier implementation of both mass surveillance and disinformation technologies. This study suggests that, as exemplified by the Snowden revelations, states and corporations together have incentives either stemming from economics, intelligence or control purposes[75] to preserve the current state of affairs. Hence, a solution to the current corpo-state surveillance relationships coming from within this same system appears to be improbable.

Even if a broad, and non-partisan political coalition desire to solve this problem, the nature of surveillance and disinformation technologies today means also that the cat is already out of the bag. Against this, a re-thinking of the concept of privacy may be in order.

75 See: Propaganda, Censorship, and Surveillance are attributes of the same underlying aspect: Monopoly and Centralised Control. https://joindiaspora.com/posts/7bfcf170eefc013863fa002590d8e506

One which strongly considers a consent-based approach to individual privacy and its collective notions to guide in the enactment of stronger privacy laws. Such a view would ideally understand the concept of privacy as one providing immunity to the herd by protecting individual risk-takers and those seeking to resist repressive surveillance and disinformation. Nonetheless, this study suggests how some negative consequences engendered by surveillance — including social-cooling effects and isolation — can be remediated using a collective-based approach ideally fuelled by international solidarity.

Such free spaces enacted by groups like the CCC can provide a template to follow and learn from. These spaces offer an outlet enabling the sharing of best practices and control mechanisms helping counter-surveillance actors better resist and combat issues of isolation and other negative consequences associated with surveillance. Most of all, they provide support, understanding and the necessary context to understand the issues we confront today and this, independently of the dynamics of corporate and state influence.

References

Al-Bassam, M. (2017). *Uncovering British spies' web of sockpuppet social media personas*. /v/34c3-9233-uncovering_british_spies_web_of_sockpuppet_social_media_personas

Alberts, G., & Oldenziel, R. (2016). *Hacking Europe*. Springer.

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*, *13*(3). https://doi.org/10.5210/fm.v13i3.2142

Andrejevic, M. (2014). Big data, big questions| the big data divide. *International Journal of Communication*, *8*, 17.

Angwin, J., Ashby, M., & Bedoya, A. M. (2018). *McSweeney's Issue 54: The End of Trust* (D. Eggers, Ed.). McSweeney's Publishing.

Anonymous. (2013). *Arrest Tracker—ParAnoia*. https://web.archive.org/web/20130406162836/http://wiki.par-anoia.net/wiki/Main_Page

Antoine, D. (2020). *Spinning Violence: Examining Competing Discourses of State Force and Indigenous Identity in Mi'kma'ki, 2013* [PhD Thesis]. Carleton University.

Apoifis, N. (2016). *Anarchy in Athens: An ethnography of militancy, emotions and violence*. Oxford

University Press.

Apoifis, N. (2017). Fieldwork in a furnace: Anarchists, anti-authoritarians and militant ethnography. *Qualitative Research*, *17*(1), 3–19. https://doi.org/10.1177/1468794116652450

Attride-Stirling, J. (2001). Thematic networks: An analytic tool for qualitative research. *Qualitative Research*, *1*(3), 385–405. https://doi.org/10.1177/146879410100100307

Austin, L. M. (2014). Lawful Illegality: What Snowden has Taught us about the legal infrastructure of the Surveillance State. *Available at SSRN 2524653*.

BalCCon. (2019). *BalCCon2k19*. https://2k19.balccon.org/index.php?title=Main_Page

Ball, J. (2013). *GCHQ taps fibre-optic cables for secret access to world's communications | UK news | The Guardian*. https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

Ball, K. (2009). Exposure: Exploring the subject of surveillance. *Information, Communication & Society*, *12*(5), 639–657. https://doi.org/10.1080/13691180802270386

Ball, K. S., Green, N. C., Koskela, H., & Philipps, D. J. (2009). Surveillance studies needs gender and sexuality. *Surveillance and Society*, *6*(4), 352–355.

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

Bauer, M. W., & Gaskell, G. (2000). *Qualitative researching with text, image and sound: A practical handbook for social research*. Sage.

Bello, G. (2017). *Anonymous revealed to be under attack from both corporate and government spies*. Free Press. http://freepress. org/departments/display/20/2014/5336. Accessed.

Bennett, C. J. (2008). *The Privacy Advocates: Resisting the Spread of Surveillance*.

Bentham, J., & Božovič, M. (1995). *The panopticon writings*. Verso Trade.

Bourdieu, P., & Wacquant, L. J. (1992). *An invitation to reflexive sociology*. University of Chicago press.

Bradbury, D. (2011). Routing around censorship. *Network Security*, *2011*(5), 5–8. https://www.sciencedirect.com/science/article/abs/pii/S1353485811700496

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

Cameron, R. (2009). A sequential mixed model research design: Design, analytical and display issues. *International Journal of Multiple Research Approaches*, *3*(2), 140–152. https://doi.org/10.5172/mra.3.2.140

Canada, S. of. (2016, November 4). *Senate of Canada—Committees*. Senate of Canada. https://sencanada.ca/en/committees/

Caruso, G. (2012). *Networking Futures: The Movements Against Corporate Globalization*. Taylor & Francis.

Casas-Cortés, M., & Cobarrubias, S. (2007). Drifting through the knowledge machine. *Constituent Imagination: Militant Investigations//Collective Theorization*, 112–126.

CCC. (n.d.). *Re-enactment of the Wau-Pengo debate (1989) at the 31C3, Wau Holland Foundation webpage.* http://www.wau-holland-stiftung.de/en/news/2015/02/re-enactment-of-the-wau-pengo-debate-1989-at-the-31C3/

CCC. (2017a). *34C3_Wiki*. https://events.ccc.de/congress/2017/wiki/index.php/Main_Page

CCC. (2017b). CCC | Chaos Communication Congress is moving to Leipzig. *Chaos Communication Congress Is Moving to Leipzig*. https://www.ccc.de/en/updates/2017/34C3-in-leipzig

CCC. (2019). *CCCamp 2019 Wiki*. https://events.ccc.de/camp/2019/wiki/Main_Page

Choudry, A. (2015). *Learning Activism: The Intellectual Life of Contemporary Social Movements*. University of Toronto Press. https://books.google.com/books/about/Learning_Activism.html?id=2W0hCwAAQBAJ

Choudry, A. (2018). *Reflections on Knowledge, Learning and Social Movements: History's Schools, 1st Edition (Hardback) - Routledge* [Text]. Routledge.Com.

https://www.routledge.com/Reflections-on-Knowledge-Learning-and-Social-Movements-Historys-Schools/Choudry-Vally/p/book/9781138059108

Choudry, A. (2019). *Activists and the Surveillance State: Learning from Repression*. Pluto Press; JSTOR. https://doi.org/10.2307/j.ctv893hzw

Choudry, A., & Kapoor, D. (2010). Learning from the ground up: Global perspectives on social movements and knowledge production. In *Learning from the Ground Up* (pp. 1–13). Springer.

CIJ. (2019, January 8). *CIJ Logan 2018: Cyber Crime and IRL Punishment*. https://vimeo.com/310078581

Clifford, J. (1988). *The predicament of culture: Twentieth-century ethnography, literature, and art*. Harvard University Press.

Cohen, J. E. (2012). What privacy is for. *Harv. L. Rev.*, *126*, 1904.

Coleman, G. (2010a). Ethnographic approaches to digital media. *Annual Review of Anthropology*, *39*. https://doi.org/10.1146/annurev.anthro.012809.104945

Coleman, G. (2010b). The hacker conference: A ritual condensation and celebration of a lifeworld. *Anthropological Quarterly*, 47–72.

Coleman, G. (2013a). *Anonymous in context: The politics and power behind the mask*.

Coleman, G. (2013b). *Coding freedom: The ethics and aesthetics of hacking*. Princeton University Press.

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

Coleman, G. (2017). From Internet farming to weapons of the geek. *Current Anthropology*, *58*(S15), S91–S102. https://doi.org/10.1086/688697

correspondent, O. B. L. affairs. (2020, February 21). UN warns of rise of “cybertorture” to bypass physical ban. *The Guardian*. https://www.theguardian.com/law/2020/feb/21/un-rapporteur-warns-of-rise-of-cybertorture-to-bypass-physical-ban

Couldry, N. (2019). *Nick Couldry: The Emerging Social Order of Data Colonialism* [Video]. https://www.youtube.com/watch?v=56BTNFfInWU&t=2341

Cox, K. (2019, October 24). *Zuckerberg faces heat in Congress: "It's almost like you think this is a joke."* Ars Technica. https://arstechnica.com/tech-policy/2019/10/zuckerberg-faces-heat-in-congress-its-almost-like-you-think-this-is-a-joke/

Cunliffe, A. L. (2010). Retelling Tales of the Field: In Search of Organizational Ethnography 20 Years On. *Organizational Research Methods*, *13*(2), 224–239. https://doi.org/10.1177/1094428109340041

Curasi, C. F. (2001). A Critical Exploration of Face-to Face Interviewing vs. Computer-Mediated Interviewing. *International Journal of Market Research*, *43*(4), 1–13. https://doi.org/10.1177/147078530104300402

Dal Bó, E. (2006). Regulatory capture: A review. *Oxford Review of Economic Policy*, *22*(2), 203–225.

Dawes, S. (2014). Press Freedom, Privacy and The Public Sphere. *Journalism Studies*, *15*(1), 17–32. https://doi.org/10.1080/1461670X.2013.765637

de Zwart, M. (2016). Privacy for the Weak, Transparency for the Powerful. *De Zwart, Melissa,'Privacy for the Weak, Transparency for the Powerful'in Andrew T. Kenyon (Ed), Comparative Defamation and Privacy Law (Cambridge University Press, 1st Ed, 2016)*, 224–245.

Deleuze, G. (1992). Postscript on the Societies of Control. *October*, *59*, 3–7.

Dencik, L., & Cable, J. (2017). The Advent of Surveillance Realism: Public Opinion and Activist Responses to the Snowden Leaks. *International Journal of Communication*, *11*, 763–781. http://ijoc.org/index.php/ijoc/article/view/5524/1939

Dencik, L., Hintz, A., & Cable, J. (2016). Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society*, *3*(2), 205395171667967. https://doi.org/10.1177/2053951716679678

Denker, K. (2014). Heroes yet criminals of the German computer revolution. In *Hacking Europe* (pp. 167–187). Springer.

Dixon, C. (2012). Building'Another Politics': The Contemporary Anti-Authoritarian Current in the US and Canada. *Anarchist Studies*, *20*(1).

Doctorow, C. (2020, August 27). *How to Destroy 'Surveillance Capitalism.'* Medium. https://onezero.medium.com/how-to-destroy-surveillance-capitalism-8135e6744d59

Doğan, B. (2019). *Contextualizing Hacktivism: The Criminalization of Redhack*.

Drephal, A. (2019). *Media.ccc.de—The KGB Hack: 30 Years Later*. Media.Ccc.De. https://media.ccc.de/v/36c3-11031-the_kgb_hack_30_years_later

D'Souza, R. (2019). The Surveillance State: A Composition in Four Movements. In A. Choudry (Ed.), *Activists And The Surveillance State* (pp. 23–52). Pluto. https://westminsterresearch.westminster.ac.uk/item/q9zy6/the-surveillance-state-a-composition-in-four-movements

Eckersley, P. (2010, January 26). *A Primer on Information Theory and Privacy*. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy

Elliott, & Meyer. (2013, October 23). *Claim on "Attacks Thwarted" by NSA Spreads Despite Lack of Evidence* [Text/html]. ProPublica. https://www.propublica.org/article/claim-on-attacks-thwarted-by-nsa-spreads-despite-lack-of-evidence

Fairhurst, G. T., & Putnam, L. (2004). Organizations as discursive constructions. *Communication Theory*, *14*(1), 5–26.

Ferrell, J. (2009). Against method, against authority... For anarchy. In *Contemporary Anarchist Studies* (pp. 89–97). Routledge.

Fitzpatrick, A. (2013). *Watch Aaron Swartz Explain "How We Stopped SOPA."* Mashable. https://mashable.com/2013/01/14/aaron-swartz-sopa/

Foucault, M. (1978). *The History of Sexuality, vol. 1, An Introduction, trans. Robert Hurley*.

Fuchs, C. (2007a). *Internet and society: Social theory in the information age*. Routledge.

Fuchs, C. (2007b). *Internet and society: Social theory in the information age*. Routledge.

Fuchs, C. (2009). Some Reflections on Manuel Castells' Book "Communication Power." *TripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society*, *7*(1), 94–108.

Fuchs, C. (2011). How to define surveillance? *MATRIZes*, *5*(1), 109–136. https://doi.org/10.11606/issn.1982-8160.v5i1p109-136

Fuchs, C. (2013). Critique of the political economy of web 2.0 surveillance. In *Internet and Surveillance* (pp. 51–90). Routledge.

Fuchs, C. (2015). Surveillance and Critical Theory. *Media and Communication*, *3*(2), 6. https://doi.org/10.17645/mac.v3i2.207

Fuchs, C., & Qiu, J. L. (2018). Ferments in the Field: Introductory Reflections on the Past, Present and Future of Communication Studies. *Journal of Communication*, *68*(2), 219–232. https://doi.org/10/gdb9fq

Fuchs, C., & Trottier, D. (2017). Internet surveillance after Snowden: A critical empirical study of computer experts' attitudes on commercial and state surveillance of the Internet and social media post-Edward Snowden. *Journal of Information, Communication and Ethics in Society*, *15*(4), 412–444. https://doi.org/10.1108/JICES-01-2016-0004

Galič, M., Timan, T., & Koops, B.-J. (2017). Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation. *Philosophy & Technology*, *30*(1), 9–37. https://doi.org/10.1007/s13347-016-0219-1

Gandy Jr, O. H. (1993). *The Panoptic Sort: A Political Economy of Personal Information. Critical Studies in Communication and in the Cultural Industries.* ERIC.

Garfinkel, S. (2000). *Database Nation: The Death of Privacy in the 21st Century*. O'Reilly Media, Inc.

Garfinkel, S. L. (2000, February 10). *What They Do Know Can Hurt You*. https://www.thenation.com/article/what-they-do-know-can-hurt-you/

Giddens, A. (1981). *A contemporary critique of historical materialism* (Vol. 1). Univ of California Press.

Giddens, A. (1984). *The constitution of society: Outline of the theory of structuration*. Polity Press.

Giddens, A. (1995). *A contemporary critique of historical materialism* (2. ed., [Nachdr.]). Macmillan Press.

Giorgi, A. (1975). An application of phenomenological method in psychology. *Duquesne Studies in Phenomenological Psychology*, *2*, 82–103.

Glasius, M. (2018). What authoritarianism is… and is not: A practice perspective. *International Affairs*, *94*(3), 515–533.

Glasius, M., & Michaelsen, M. (2018). Authoritarian Practices in the Digital Age| Illiberal and Authoritarian Practices in the Digital Sphere—Prologue. *International Journal of Communication*, *12*, 19.

Green, M. (2019, September 24). Looking back at the Snowden revelations. *A Few Thoughts on Cryptographic Engineering*. https://blog.cryptographyengineering.com/2019/09/24/looking-back-at-the-snowden-revelations/

Greenberg, A. (2015). *This Machine Kills Secrets: How WikiLeakers, Cypherpunks, and Hacktivists Aim to Free the World's Information*.

Greene, T. (2020). *Amazon Engineer: "Ring should be shut down immediately and not brought back."* The Next Web. https://thenextweb.com/artificial-intelligence/2020/01/28/amazon-engineer-ring-should-be-shut-down-immediately-and-not-brought-back/

Greenwald, G. (2014a). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state* (First Edition.). Metropolitan Books/Henry Holt.

Greenwald, G. (2014b, February 24). How Covert Agents Infiltrate the Internet to Manipulate,

Deceive, and Destroy Reputations. *The Intercept*. https://theintercept.com/2014/02/24/jtrig-manipulation/

Greenwald, G., & Gallagher, R. (2014, February 18). Snowden Documents Reveal Covert Surveillance and Pressure Tactics Aimed at WikiLeaks and Its Supporters. *The Intercept*. https://theintercept.com/2014/02/18/snowden-docs-reveal-covert-surveillance-and-pressure-tactics-aimed-at-wikileaks-and-its-supporters/

Grey, S. (2016). Is your secret safe with me? Difficulties of protecting sources amid mass surveillance. *Index on Censorship*, *45*(2), 58–61.

Groll, E. (2016, October 4). *How American Companies Enable NSA Surveillance – Foreign Policy*. https://foreignpolicy.com/2016/10/04/how-american-companies-enable-nsa-surveillance/

Gustavo, S. (2019). *Amazon's Ring doorbell partners with Florida police departments to make everyone a snitch*. Orlando Weekly. https://www.orlandoweekly.com/orlando/amazon-partners-with-florida-police-departments-to-make-everyone-a-snitch/Content?oid=26147546

Hafner, K., & Markoff, J. (1995). *Cyberpunk: Outlaws and Hackers on the Computer Frontier, Revised*. Simon and Schuster.

Haggart, B. (2019, February 14). Evaluating scholarship, or why I won't be teaching Shoshana Zuboff's The Age of Surveillance Capitalism. *Blayne Haggart's Orangespace*. https://blaynehaggart.wordpress.com/2019/02/15/evaluating-scholarship-or-why-i-wont-be-teaching-shoshana-zuboffs-the-age-of-surveillance-capitalism/

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

Haggerty, K. D., & Samatas, M. (2010). *Surveillance and democracy*. Routledge.

Hammond, J. (2019). Imprisoned Activist Jeremy Hammond Called Against His Will to Testify Before Federal Grand Jury in the EDVA | Courage Foundation. *Courage Foundation*. /2019/09/imprisoned-activist-jeremy-hammond-called-against-his-will-to-testify-before-federal-

grand-jury-in-the-edva/

Harvey, D. (1996). Justice, nature and the geography of difference Blackwell. *Malden MA*.

Hintz, A., & Milan, S. (2018). *Through a Glass, Darkly: Everyday Acts of Authoritarianism in the Liberal West*.

Hollway, W., & Jefferson, T. (2000). *Doing qualitative research differently: Free association, narrative and the interview method*. Sage.

Horkheimer, M. (1976). Traditional and critical theory. *Critical Theory: Selected Essays*, 288–243.

Hudig, K. (2012). State Trojans: Germany exports "spyware with a badge." *Statewatch Journal*, *21*(4).

Humby, C. (2006). Data is the new oil. *Proc. ANA Sr. Marketer's Summit. Evanston, IL, USA*.

Huxley, A. (1941). *Grey eminence: A study in religion and politics*. Harper & brothers.

Jorgensen, D. L. (1989). *Participant observation: A methodology for human studies* (Vol. 15). Sage.

Juris, J. S. (2005a). The New Digital Media and Activist Networking within Anti–Corporate Globalization Movements. *The ANNALS of the American Academy of Political and Social Science*, *597*(1), 189–208. https://doi.org/10.1177/0002716204270338

Juris, J. S. (2005b). Violence performed and imagined: Militant action, the Black Bloc and the mass media in Genoa. *Critique of Anthropology*, *25*(4), 413–432.

Juris, J. S. (2007). Practicing militant ethnography with the movement for global resistance in Barcelona. *Constituent Imagination: Militant Investigations, Collective Theorization*, 164–178.

Juris, J. S. (2008). *Networking futures: The movements against corporate globalization*. Duke University Press.

Juris, J. S., & Khasnabish, A. (2013). *Insurgent encounters: Transnational activism, ethnography, and the political*. Duke University Press.

Kelty, C. M. (2008). *Two bits: The cultural significance of free software*. Duke University Press.

Kinsman, G. W., Buse, D. K., & Steedman, M. (2000). *Whose National Security?: Canadian state surveillance and the creation of enemies*. Between the Lines.

Knappenberger, B. (n.d.). *The Internet's Own Boy: The Story of Aaron Swartz (2014)—IMDb*. Retrieved March 4, 2020, from https://www.imdb.com/title/tt3268458/

Kofinas, D. (2019). *Surveillance Capitalism in the Age of the Unprecedented | Shoshana Zuboff* [Podcast]. Hidden Forces. https://www.hiddenforces.io/podcast/shoshana-zuboff-surveillance-capitalism

Krasmann, S., & Kühne, S. (2014). 'My fingerprint on Osama's cup.'On objectivity and the role of the fictive regarding the acceptance of a biometric technology. *Surveillance & Society*, *12*(1), 1–14.

Krotz, F. (2007). The meta-process ofmediatization'as a conceptual frame. *Global Media and Communication*, *3*(3), 256–260.

Krotz, F. (2009). Mediatization: A concept with which to grasp media and societal change. *Mediatization: Concept, Changes, Consequences*, 21–40.

Kubitschko, S. (2015a). Hackers' media practices: Demonstrating and articulating expertise as interlocking arrangements. *Convergence: The International Journal of Research into New Media Technologies*, *21*(3), 388–402. https://doi.org/10.1177/1354856515579847

Kubitschko, S. (2015b). *Media practices of civil society organisations: Emerging paths to legitimation and long-term engagement* [Ph.D., University of London, Goldsmiths' College (United Kingdom)]. http://search.proquest.com/docview/1827515721?pq-origsite=primo

Kubitschko, S. (2015c). The Role of Hackers in Countering Surveillance and Promoting Democracy. *Media and Communication*, *3*(2), 77. https://doi.org/10.17645/mac.v3i2.281

Kubitschko, S. (2018a). Acting on media technologies and infrastructures: Expanding the media as practice approach. *Media, Culture & Society*, *40*(4), 629–635. https://doi.org/10.1177/0163443717706068

Kubitschko, S. (2018b). Chaos Computer Club: The Communicative Construction of Media

Technologies and Infrastructures as a Political Category. In *Communicative Figurations* (pp. 81–100). Springer.

Kubitschko, S., & Kaun, A. (Eds.). (2016). *Innovative methods in media and communication research*. Palgrave Macmillan.

Kubitschko, S., Richterich, A., & Wenz, K. (2017). „There Simply Is No Unified Hacker Movement.“Why We Should Consider the Plurality of Hacker and Maker Cultures. *Digital Culture & Society*, *3*(1), 185–195. https://doi.org/10.14361/dcs-2017-0112

Kulwin, N. (2019, February 24). *Shoshana Zuboff Talks Surveillance Capitalism's Threat to Democracy*. Intelligencer. https://nymag.com/intelligencer/2019/02/shoshana-zuboff-q-and-a-the-age-of-surveillance-capital.html

Kvale, S. (1996). The 1,000-page question. *Qualitative Inquiry*, *2*(3), 275–284.

Levina, M. (2017). Under Lenin's watchful eye: Growing up in the former Soviet Union. *Surveillance & Society*, *15*(3/4), 529–534. https://doi.org/10.24908/ss.v15i3/4.6640

Lubbers, E. (2012). *Secret Manoeuvres in the Dark: Corporate and Police Spying on Activists*. Pluto Press.

Lubbers, E. (2015). Undercover Research: Corporate and police spying on activists. An introduction to activist intelligence as a new field of surveillance. *Surveillance & Society*, *13*(3/4), 338–353. https://doi.org/10/gfvqnk

Luciano, T. (2011). Doing a literature review: Releasing the social science research imagination. *Evaluation & Research in Education*, *24*(4), 303–304. https://doi.org/10.1080/09500790.2011.588012

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, *1*(2), 2053951714541861. https://doi.org/10.1177/2053951714541861

Lyon, D. (2015). *Surveillance after Snowden*. John Wiley & Sons.

Lyon, D. (2017). *Surveillance Culture: Engagement, Exposure, and Ethics in Digital Modernity*.

19.

MacKinnon, R. (2011). Liberation Technology: China's" Networked Authoritarianism". *Journal of Democracy*, *22*(2), 32–46.

MacLean, J. (2016). *Striking at the root problem of Canadian environmental law: Identifying and escaping regulatory capture*.

Manokha, I. (2018). The Cambridge analytica scandal contextualized: Platform capital, surveillance, and data as a new "fictitious commodity", Le scandale Cambridge Analytica contextualisé: Le capital de plateforme, la surveillance et les données comme nouvelle « marchandise fictive». *Cultures et Conflits*, *109*(1), 30–59. https://doi.org/10/gfzvvn

May, T. (1992). The crypto anarchist manifesto. *High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace*.

McCurdy, P. (2009). '*I Predict a Riot' – mediation and political contention: Dissent!'s media practices at the 2005 Gleneagles G8 Summit* [Phd, The London School of Economics and Political Science (LSE)]. https://etheses.lse.ac.uk/5/

McCurdy, P., & Uldam, J. (2014). Connecting Participant Observation Positions: Toward a Reflexive Framework for Studying Social Movements. *Field Methods*, *26*(1), 40–55. https://doi.org/10.1177/1525822X13500448

McLuhan, M., Fiore, Q., & Agel, J. (1968). *War and peace in the global village* (Vol. 127). Bantam Books New York.

Mehrabov, I. (2015). Exploring Terra Incognita: Mapping Surveillance Studies from the Perspective of Media and Communication Research. *Surveillance & Society*, *13*(1), 117–126.

Mehrabov, I. (2016). When States Strike Back: Failures of Mediatized Activism in Azerbaijan and Turkey. *TripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society*, *14*(2), 496–515. https://doi.org/10/gftn5q

Mehrabov, I. (2017). *"All Watched Over by Machines of Loving Grace": Activist Practices in an*

Era of Mediatized Surveillance [PhD Thesis]. Karlstads universitet.

Merrigan, G., Johnston, R. T., & Huston, C. L. (2012). *Communication research methods*. Oxford University Press.

Michaelsen, M. (2017). Far Away, So Close: Transnational Activism, Digital Surveillance and Authoritarian Control in Iran. *Surveillance & Society*, *15*(3/4), 465. https://doi.org/10.24908/ss.v15i3/4.6635

Miessler, D. (2018). *Stop Trying to Violently Separate Privacy and Security*. Daniel Miessler. https://danielmiessler.com/blog/more-confusion-on-the-difference-between-data-security-and-privacy/

Mills, C. W. (2000). *The sociological imagination*. Oxford University Press.

Mols, A., & Janssen, S. (2017). Not interesting enough to be followed by the NSA: An analysis of Dutch privacy attitudes. *Digital Journalism*, *5*(3), 277–298. https://doi.org/10/gfkqpc

Morozov, E. (2013). *Why our privacy problem is a democracy problem in disguise*. MIT Technological review.

Morozov, Evgeny. (2019, February 4). *Capitalism's New Clothes*. The Baffler. https://thebaffler.com/latest/capitalisms-new-clothes-morozov

Morse, J. M. (2016). *Mixed method design: Principles and procedures*. https://doi.org/10.4324/9781315424538

Morse, V. (2019). Spies Wide Shut: Aoteraroa New Zealand – The Unstable State: Why New Zealand Needs Ever More Surveillance. In Activists and the Surveillance State: Learning from Repression. In *Activists and the Surveillance State: Learning from Repression* (pp. 199–214).

Moser, A., & Korstjens, I. (2018). Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis. *European Journal of General Practice*, *24*(1), 9–18.

Munk, T. B. (2017). 100,000 false positives for every real terrorist: Why anti-terror algorithms don't work. *First Monday*, *22*(9). https://doi.org/10.5210/fm.v22i9.7126

Munkholm, J. L. (2020). The Pursuit of Full Spectrum Dominance: The Archives of the NSA. *Surveillance & Society*, *18*(2), 244–256.

Nehf, J. P. (2003). Recognizing the Societal Value in Information Privacy. *Washington Law Review*, *78*, 1. https://heinonline.org/HOL/Page?handle=hein.journals/washlr78&id=11&div=&collection=

Newman, A. (2009). Bennett, Colin. 2008. The Privacy Advocates: Resisting the Spread of Surveillance. Cambridge: MIT Press. *Surveillance & Society*, *6*(3), 343–344.

Nissenbaum, H. (2019, September 25). The Fantasy of Opting Out [Blog]. *The MIT Press Reader*. https://thereader.mitpress.mit.edu/the-fantasy-of-opting-out/

Ogura, T. (2006). Electronic government and surveillance-oriented society. *Theorizing Surveillance: The Panopticon and Beyond*, 270–295.

Orgad, S. (2005). *From online to offline and back: Moving from online to offline relationships with research informants*.

Paddison, R., Philo, C., Routledge, P., & Sharp, J. (2002). *Entanglements of power: Geographies of domination/resistance*. Routledge.

Palmer, M. (2006). Data is the New Oil. *ANA Marketing Maestros*. https://ana.blogs.com/maestros/2006/11/data_is_the_new.html

Pearce, K. E. (2018). *Socially Mediated Visibility: Friendship and Dissent in Authoritarian Azerbaijan*. 22.

Pearce, K. E., & Kendzior, S. (2012). Networked authoritarianism and social media in Azerbaijan. *Journal of Communication*, *62*(2), 283–298.

Penney, J. (2016). *Chilling Effects: Online Surveillance and Wikipedia Use*. https://papers.ssrn.com/abstract=2769645

Pew Research Center. (2017). Most in U.S. say government could be monitoring their phone calls, emails. *Pew Research Center*. https://www.pewresearch.org/fact-tank/2017/09/27/most-americans-

think-the-government-could-be-monitoring-their-phone-calls-and-emails/

Plows, A. (1998). In With the In Crowd: Examining the Methodological Implications of Practising Partisan, Reflexive,'Insider. *Research', Unpublished Manuscript*.

Postill, J. (2018). *The Rise of Nerd Politics: Digital Activism and Political Change*. Pluto Press.

Roseneil, S. (1995). *Disarming patriarchy: Feminism and political action at Greenham*. Open University Press.

Rossler, B. (2018). *The value of privacy*. John Wiley & Sons.

Routledge, P. (2003). Convergence space: Process geographies of grassroots globalization networks. *Transactions of the Institute of British Geographers*, *28*(3), 333–349.

Rudmin, F. (2006). *Why Does the NSA Engage in Mass Surveillance of Americans When It's Statistically Impossible for Such Spying to Detect Terrorists?* CounterPunch.Org. https://www.counterpunch.org/2006/05/24/why-does-the-nsa-engage-in-mass-surveillance-of-americans-when-it-s-statistically-impossible-for-such-spying-to-detect-terrorists/

Ryan. (2018, May 3). *Under the Skin* [Text]. Mises Institute. https://mises.org/wire/under-skin

Ryan, A. (n.d.). *Ryan, A. B. (2006) Analysing qualitative data and...*

Saldaña, J. (2015). *The coding manual for qualitative researchers*. Sage.

Saulnier, A. (2017). Surveillance as Communicating Relational Messages: Advancing Understandings of the Surveilled Subject. *Surveillance & Society*, *15*(2), 286–302. https://doi.org/10.24908/ss.v15i2.6334

Schares, G. (1988). *A German Hacker's Club that promotes creative chaos*.

Schatzki, T. R. (2005). Practice mind-ed orders. In *The practice turn in contemporary theory* (pp. 50–63). Routledge.

Schep, T. (2017). *Media.ccc.de—Social Cooling—Big data's unintended side effect* [Media]. Media.Ccc.De. https://media.ccc.de/v/34c3-8797-social_cooling_-_big_data_s_unintended_side_effect

Schlembach, R. (2018). Undercover policing and the spectre of ‘domestic extremism’: The covert surveillance of environmental activism in Britain. *Social Movement Studies*, *17*(5), 491–506. https://doi.org/10/gfvsnk

Schwartz-Shea, P., & Yanow, D. (2009). Reading and writing as method: In search of trustworthy texts. *Organizational Ethnography: Studying the Complexities of Everyday Life*, 56–82.

Shubber, K. (2013, June 10). A simple guide to the Prism controversy. *Wired UK*. https://www.wired.co.uk/article/simple-guide-to-prism

Silverman, D. (2004). *Qualitative Research: Theory, Method and Practice*. SAGE.

Silverman, D. (2013). *Doing qualitative research: A practical handbook* (Fourth edition). SAGE.

Silverman, D. (2015). *Interpreting qualitative data*. Sage.

Silverman, D. (2016). *Qualitative research*. Sage.

Solove, D. (2007). “I’ve Got Nothing to Hide” and Other Misunderstandings of Privacy. *The San Diego Law Review*, *44*(4), 745.

Solove, D. J. (2011). Why privacy matters even if you have ‘nothing to hide.’ *Chronicle of Higher Education*, *15*.

Stankiewicz, K. (2019a, October 9). *Cambridge Analytica whistleblower: US heading in “same direction as China” with online privacy*. CNBC. https://www.cnbc.com/2019/10/09/cambridge-analytica-whistleblower-us-following-china-with-privacy.html

Stankiewicz, K. (2019b, October 9). *Cambridge Analytica whistleblower: US heading in “same direction as China” with online privacy*. CNBC. https://www.cnbc.com/2019/10/09/cambridge-analytica-whistleblower-us-following-china-with-privacy.html

Stoll, C. (1988). Stalking the wily hacker. *Communications of the ACM*, *31*(5), 484–497. https://doi.org/10.1145/42411.42412

Trottier, D., & Lyon, D. (2012). Key features of social media surveillance. *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*, *16*, 89–105.

Tue, D. 3rd 2019 3:33pm-T. C. (2019). *Cops Are Running Ring Camera Footage Through Their Own Facial Recognition Software Because Who's Going To Stop Them*. Techdirt. https://www.techdirt.com/articles/20191128/17192943475/cops-are-running-ring-camera-footage-through-their-own-facial-recognition-software-because-whos-going-to-stop-them.shtml

Uldam, J., & McCurdy, P. (2013). Studying social movements: Challenges and opportunities for participant observation. *Sociology Compass*, *7*(11), 941–951. https://doi.org/10.1111/soc4.12081

Van Maanen, J. (2011). *Tales of the field: On writing ethnography*. University of Chicago Press.

Van Teijlingen, E. (2014). Semi-structured interviews. *PGR Workshop December*.

Warren, S. D., & Brandeis, L. D. (1890). Right to privacy. *Harv. L. Rev.*, *4*, 193.

Wäscher, T. (2017). Framing Resistance Against Surveillance: Political communication of privacy advocacy groups in the "Stop Watching Us" and "The Day We Fight Back" campaigns. *Digital Journalism*, *5*(3), 368–385. https://doi.org/10.1080/21670811.2016.1254052

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2005). Organizing and the process of sensemaking. *Organization Science*, *16*(4), 409–421.

Widener, P. (2016). E-Fears, E-Risks and Citizen-Intelligence: Surveillance Impacts on Research and Confidentiality. *Surveillance & Society*, *14*(2), 277–285.

Wiener, N. (1948). *Cybernetics or control and communication in the animal and the machine*. Technology Press.

Williams, A., Gibb, A., & Weekly, D. (2012). Research with a hacker ethos: What DIY means for tangible interaction research. *Interactions*, *19*(2), 14–19. https://doi.org/10.1145/2090150.2090156

Wired. (2020). Protests Renew Scrutiny of Tech's Ties to Law Enforcement. *Wired*. https://www.wired.com/story/protests-renew-scrutiny-tech-ties-law-enforcement/

Wood, D. M. (2017). Editorial The Global Turn to Authoritarianism and After. *Surveillance & Society*, *15*(3/4), 358.

Wood, D. M., Ball, K., Lyon, D., Norris, C., & Raab, C. (2006). A report on the surveillance

society. *Surveillance Studies Network, UK*.

Wood, D. M., & Wright, S. (2015). Before and After Snowden. *Surveillance & Society*, *13*(2), 132–138. https://doi.org/10/gfzvvk

Wuermeling, U. (1989). New dimensions of computer-crime—Hacking for the KGB — A report. *Computer Law & Security Review*, *5*(4), 20–21. https://doi.org/10.1016/0267-3649(89)90055-1

Yanow, D. (2009). Dear author, dear reader: The third hermeneutic in writing and reviewing ethnography. In *Political ethnography: What immersion brings to the study of power* (pp. 275–302). University of Chicago Press.

Ybema, S., Yanow, D., Wels, H., & Kamsteeg, F. H. (2009). *Organizational ethnography: Studying the complexity of everyday life*. Sage.

Zizek, S. (2008). *Violence: Six Sideways Reflections*. Picador.

Zizek, S. (2011). From democracy to divine violence. *Democracy in What State*, 100–120.

Zuboff, S. (1988). *In the age of the smart machine*. Basic books.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89. https://doi.org/10.1057/jit.2015.5

Zuboff, S. (2019). Surveillance capitalism. *Esprit*, *5*, 63–77.

Appendices

Appendix 1: Participant Information

PARTICIPANT IDENTIFIER	LOCATION	OTHER INFO
Participant 1	Leipzig	
Participant 2	Online	
Participant 3	Online	
Participant 4	Online	
Participant 5	Online	
Participant 6	Mildenberg Park	
Participant 7	Mildenberg Park	
Participant 8	Online	

Appendix 2: Duration of Interviews

PARTICIPANT IDENTIFIER	INTERVIEW LENGTH
Participant 1	55 minutes
Participant 2	1 hour 14 minutes
Participant 3	55 minutes
Participant 4	1 hour
Participant 5	1 hour 32 minutes
Participant 6	1 hour 32 minutes

Participant 7	1 hour 9 minutes
Participant 8	1 hour 30 minutes

Appendix 3: Events Attended During Fieldwork

A) 34th iteration of the Chaos Communication Congress

Date: 26. to 30. December 2017

Location: Leipzig, Germany, Earth, Milky Way.

Dates (DD/MM/Year)	**Event or Milestone**	**Additional Information**
26/12/2017	Meeting organizers.	
27/12/2017	Radio Interview.	
28/12/2017	First interview with Participant 1 and meeting with other potential interviewees.	
29/12/2017	Workshops and talks attendances.	
30/12/2017	Workshops and talks attendances.	

B) 2019 Chaos Communication Camp

Date: 21. to 25. August 2019

Location: Ziegeleipark Mildenberg, Zehdenick, Germany, Earth, Milky Way.

Dates (DD/MM/Year)	**Event or Milestone**	**Additional Information**
21/09/2019		
22/09/2019		
23/09/2019	Interview.	

24/09/2019		
25/09/2019	Interview.	
26/09/2019		

Appendix 4: Interview Guide

Researcher: Guillaume Thibault-Rochefort

Supervisor: Patrick McCurdy

Research Goal

This research in communication and surveillance studies aims to increase our understanding of targeted surveillance practices against privacy rights and tech activists. As a militant ethnographic research, this study aims to glean something positive out of the experiences collected as a way to help develop strategies and best practices against the effects of surveillance from a communication point of view (1). The interview consists of questions related to your personal experiences dealing with targeted surveillance and its effects.

Consent

Before the interview begins, informed consent must be obtained from the participant. The first step of the interview process involves reading the consent form and obtaining verbal consent from the interviewee. The researcher will remind the interviewee of the recording process and how the data will be stored on an encrypted device at all time, to ultimately be destroyed at the end of the study. Once the ethical consent form is read and understood and the participant made aware of their rights, the interview can begin.

Interview process

• I (the researcher) will introduce myself, and then explain the process and the purpose of the research

• I (the researcher) will advise the participant that if, at any time, they are asked a question that they would rather not answer, all they have to do is to let me (the researcher) know, and we will move on to another question.

• I (the researcher) will make it clear that participant has the right to not participate, and the right to opt out at any time and without penalty.

1) <u>Interviewee Profile</u>

The objective of this section is to get some background on the person interviewed and the context behind his or her story/experience:

a. Can you tell me about your experience with surveillance ?

b. How did it happen?

c. When did it happen?

d. When/How did it stop?

e. Other/Further experiences?

The goal is to better understand, from the interviewee's perspective, why they think the surveillance happened and for what reason(s).

2) <u>Purpose behind the surveillance</u>

Conversation shifts to specific discussion about their experience with surveillance and the purpose, from their own perspective, behind the surveillance. The points below are prompts, questions may vary and follow-ups encouraged:

a. What was, in your view, the purpose/reason behind the surveillance? (protect a

corporation, nip dissent, disturb organization, etc)

b. What role if any did the media play in your case? (mediatization)

- **More questions related to the theme of this question may be asked:** recruitment purposes, to protect a corporation, as a form of intimidation, to turn you into an informant...?

3) <u>Social cooling/Isolation Issues</u>

Conversation shifts from the purpose behind the surveillance, in their view, to so-called social cooling effects, or isolation, as a result of the surveillance from a communication perspective. The interviewee is invited to define, in their own words, surveillance as a concept.

a. How would you define surveillance?

... According to surveillance theory, the main goal of surveillance is to hinder, alter or simply stop communication altogether. In your own experience, how has surveillance affected your communication behaviours?

b. Can you discuss your experience with isolation during the surveillance?

c. What strategies helped mitigate these behaviours?

- Further questions, in relation to the theme of this particular question and depending on where the conversation goes, may be asked.

4) S<u>ecurity applications and social media.</u>

Conversation shifts from isolation itself to privacy/security applications and social media.

a. Could you elaborate on the ways by which you mediated the negative effects of surveillance on yourself?

b. How did it affect your use of social media, the internet, smart phone use and so on? (spotlight)

c. In this context, what is your view on security and privacy applications, such as Signal, Wire (silo environment, backward compatibility, ease of use)

- Further questions about the theme of this particular question and depending on where the conversation goes may be asked.

5) <u>Dealing with self-censorship/social cooling effects.</u>

Conversation shifts from isolation and privacy applications to questions of autonomy, self-censorship and other social cooling effects.

Besides the threat to privacy, surveillance is said to be a threat to people's autonomy and their ability for them to choose their actions freely.

a. Would you say this was your case during the surveillance?

If so, what were there strategies or methods adopted to help mediate and deal with this kind of effects on a personal level?

b. What did not?

- Further questions in relation to the theme of this particular question and depending on where the conversation goes may be asked.

6) <u>The media, journalists, civil society.</u>

Conversation shifts from social-cooling effects to collaboration, trust in the press, journalists, and other civil society actors and organizations (CCC)

a. One important part of my research on surveillance concerns the media and how privacy/digital activists perceive them. In short, I am curious to know more about how you see the value of journalists, and if, from a surveillance point of view, you see them as a potential risk? Do you trust or hate certain journos ? Outlets? Do you make time for journalists?

b. For many counter-surveillance actors and activists, collectives such as the Chaos Computer Club and others have been an essential outlet to help alleviate some of the effects related to isolation as a consequence of targeted surveillance. Knowing you are not alone and being part of a collective can be key in keeping yourself together in these types of situation.

Would you agree with this view?

- If disagree: other factors? (Other organizations? Family? Online/offline friends? School/professors? Lawyers?)
- If agree: Ask how it helped them and how it affected their situation.
- Depending on where the conversation may go, further questions in relation to the

theme of this particular question may be asked.

7) Best Practices guide

From collaboration, we move on to counter-surveillance strategies and best-practices from a communication perspective.

a. As I have explained before, the main goal of this militant ethnographic study is to accumulate experiences related to targeted surveillance with the hope of crafting a best practices, lessons learned type of guide. My hope is that, from our collective experiences, we can help others in the future who may be confronted with similar challenges to avoid making the same mistakes.

What, in your view, are the most important points to remember? (How to keep it together, how to seek help, who to talk to, what patterns of behaviour to avoid, how to help alleviate effects of isolation and so on)

b. Are there anything else you think I should know that I did not ask? Something I may have missed that you want to add?

Appendix 5: Consent Form

Consent form Interviews

Project Title: Collaborative Chaos: Counter-Surveillance Actors and Symbiotic Resistance to Pervasive Surveillance

Researcher: Guillaume Thibault-Rochefort

Department of Communication, Faculty of Arts

University of Ottawa

Supervisor: Patrick McCurdy, PhD, Associate Professor

Department of Communication, Faculty of Arts

University of Ottawa

Invitation to Participate: You are invited to participate in the study named above as part of Guillaume Thibault-Rochefort (the researcher) Masters' thesis, under the supervision of Professor Patrick McCurdy. As the interview will be held in English, you should be fluent in English.

Purpose of the Study: The purpose of the project is to explore the lived experiences of counter-surveillance actors/activists with surveillance, related to questions of isolation, social cooling, the use of privacy applications and your views on the state of modern surveillance today.

Participation: Your participation will primarily consist of an interview session lasting between 30 and 60 minutes, during which you will answer questions from the researcher about your experience and views as they relate to surveillance and privacy applications. The meeting will be scheduled for (place, date and time). In the case that the interview is done online, the interview will be conducted exclusively via Jabber and the OTR/OMEMO extensions.

Risks: You understand that your participation in this research requires that you provide information on your experiences and views as an activist on the subject of surveillance and privacy. To alleviate any risks related, all data will be stored securely on the researcher's

computer, protected by full disk encryption. To ensure confidentiality of the interview process, the encryption communication platform Jabber, with the plugin OMEMO installed, will be used for the conduct the interview.

Benefits: Your participation in this research will effectively contribute to the advancement of knowledge in the field of surveillance studies and social movement scholarship.

Confidentiality and Anonymity: You understand that action will be taken to protect and ensure your anonymity and confidentiality.

In this case, you have the assurance that any information to be shared with the researcher that could lead to your identification will remain strictly confidential. You can expect that the content is used only for research purposes and, according to confidentiality, only the researcher and his supervisor will have access to identifiable data collected during the interviews. Anonymity will be guaranteed as follows: your name and your specific position will not be mentioned in documents. The researcher will refer to you using a generic term that does not allow readers to identify you. (e.g. 'Participant1').

Data Retention: Transcriptions logs of interviews will be collected. The documents will also be printed and stored securely in a locked cabinet for a period of five years in the office of the Principal Researcher (Patrick McCurdy). The encrypted electronic data will be kept for 5 years on the Principal Researcher’s computer protected by full disk encryption.

Voluntary Participation: Your participation in this research is voluntary. You are free to withdraw at any time, and / or refuse to answer certain questions without negative

consequences. Should you wish to withdraw from the study, you will also be given the opportunity to withdraw your data from the study.

Acceptance: I, (Pseudonym), agree to participate in this research as part of Guillaume Rochefort's Masters' Thesis, of the Department of Communication, Faculty of Arts, University of Ottawa and to the interview being transcribed.

For additional information about this study, you may contact the researcher or his supervisor:

Researcher: Guillaume Rochefort
Department of Communication, Faculty of Arts,
University of Ottawa

Supervisor: Patrick McCurdy, PhD, Associate Professor
Department of Communication, Faculty of Arts
University of Ottawa
613-562-5800, poste 2728
pmccurdy@uottawa.ca

For information on ethical aspects of this research, you can speak to the Head of Research Ethics, University of Ottawa, Tabaret Hall, 550 Cumberland Street, Room 154; Telephone: 613-562-5387; Email: ethics@uottawa.ca

Participants should print a copy of the consent form to keep for their personal records.

Signature of Participant: (Signature) Date: (Date)

_____

Signature of researcher: (Signature) Date: (Date)

_____