-----BEGIN PGP MESSAGE-----
Charset: utf-8
Version: GnuPG v2
hQIMA5xNM/DISSENT7ieVABAQ//YbpD8i8BFVKQfbMy
I3z8R8k/ez3oexH+sGE+tPRIVACYMOVEMENTRvU+lSB
MY5dvAkknydTOF7xIEnODLSq42eKbrCToDMboT7puJSlWr
W

Meeting the Privacy Movement

d
76hzgkusgTrdDSXure5U9841B64SwBRzzkkpLra4FjR
/DzeF

Dissent in the Digital Age

0M00m
BIPhO84h4cCOUNTERREVOLUTION0xm17idq3cF5zS2
GXACTIVISTSXvV3GEsyU6sFmeFXNcZLP7My40pNc
SOCIALMOVEMENTgQbplhvjN8i7cEpAI4tFQUPN0dtFmCu
h8ZOhP9B4h5Y681c5jr8fHzGNYRDC5IZCDH5uEZtoEBD8
FHUMANRIGHTSwxZvWEJ16pgOghWYoclPDimFCuIC
7K0dxiQrN93RgXi/OEnfPpR5nRU/Qv7PROTESTaV0scT
nwuDpMiAGdO/byfCx6SYiSURVEILLANCEFnE+wGGpKA0rh
C9Qtag+2qEpzFKU7vGt4TtJAsRc+5VhNSAq8OMmi8
n+i4W54wyKEPtkGREENWALDk41TM9DN6ES7sHtA
OfzszqKTgB9y10Bu+yUYNO2d4XY66/ETgjGX3a7OY/vbIh
Ynl+MIZd3ak5PRIVACYbNQICGtZAjPOITRAS6E
ID4HpDIGITALAGEBhcsAd2PWKKgHARRISON4hN4mo7
LIlcr0t/U27W7ITTIEpVKrt4ieeesji0KOxWFneFpHpnVcK
t4wVxfenshwUpTlP4jWE9vaa/52y0xibz6az8M62rD9F/
XLigGR1jBBJdgKSba38zNLUq9GcP6YInk5YSfgBVsvTzb
VhZQ7kUU0IRyHdEDgII4hUyD8BERLINmdo/9bO/4s
El249ZOAyOWrWHISTLEBLOWINGrQDriYnDcvfIGBL
0q1hORVro0EBDqlPA6MOHchfN+ck74AY8HACKTIVISMy
8PZJLCBIjAJEdJv88UCZoljx/6BrG+nelwt3gCBx4dTg
XqYzvOSNOWDENTEahLZtbpAnrot5APPELBAUMzAW
Qn6tpHj1NSrAseJ/+qNC74QuXYXrPh9ClrNYN6DNJGQ
+u8ma3xfeE+psaiZvYsCRYPTOGRAPHYwkZFimy
R9bjwhRq35Fe1wXEU4PNhzO5muDUsiDwDIGITAL
A

Loes Derks van de Ven

XoJ91H0wJeEn23Sikk3WZ5s
XEGHpGBXz3njK/Gq+JYRPB+8D5xV8wI7lXQoBKDGAs
-----END PGP MESSAGE-----

Meeting the Privacy Movement
Dissent in the Digital Age

by

Loes Derks van de Ven

A thesis presented to the
Department of English Language and Culture
at the Radboud Univerity Nijmegen

In partial fulfillment of the requirements for the degree of
Master of Arts (MA) in North American Studies

Supervisor: Dr. Jorrit van den Berk

August 2015

Courage is Contagious.

- The Courage Foundation

Acknowledgements

There are a number of people without whom this thesis would not have been the same and to whom I owe many thanks.

I have met some extraordinary people in the process of doing research, both in the Netherlands and in Berlin, whose input has given me many valuable insights. Thank you Daniel J. Bernstein, Leif Ryge, Annie Machon, and Tatiana Bazzichelli. I especially owe thanks to Tanja Lange for pointing me in the right direction, and Jacob Appelbaum for taking the time to answer all my questions.

This thesis would have looked completely different without the help of my supervisor, Jorrit van den Berk. Thank you for supervising this process, your enthusiasm and positive outlook has been contagious.

Malou, thank you for putting so much effort into making the layout of this thesis perfect. You have been a great friend and a great support, especially during the many grammar emergencies.

Luuk, I cannot even begin to name all the things I want to thank you for. You took me to Hamburg, you came with me to Berlin... You have explained every technical detail, you have proofread every page, and you have been more patient while doing so than I could ever ask for. You have stood with me for every aspect of the entire process, and that means more to me than I am able to put into words. I love you to the moon and back.

Last, there are two people I can never thank enough: my parents, Will and Nelly. You have always encouraged me to study as much as I can for as long as I can, and you have set everything aside to help me do so. Thank you.

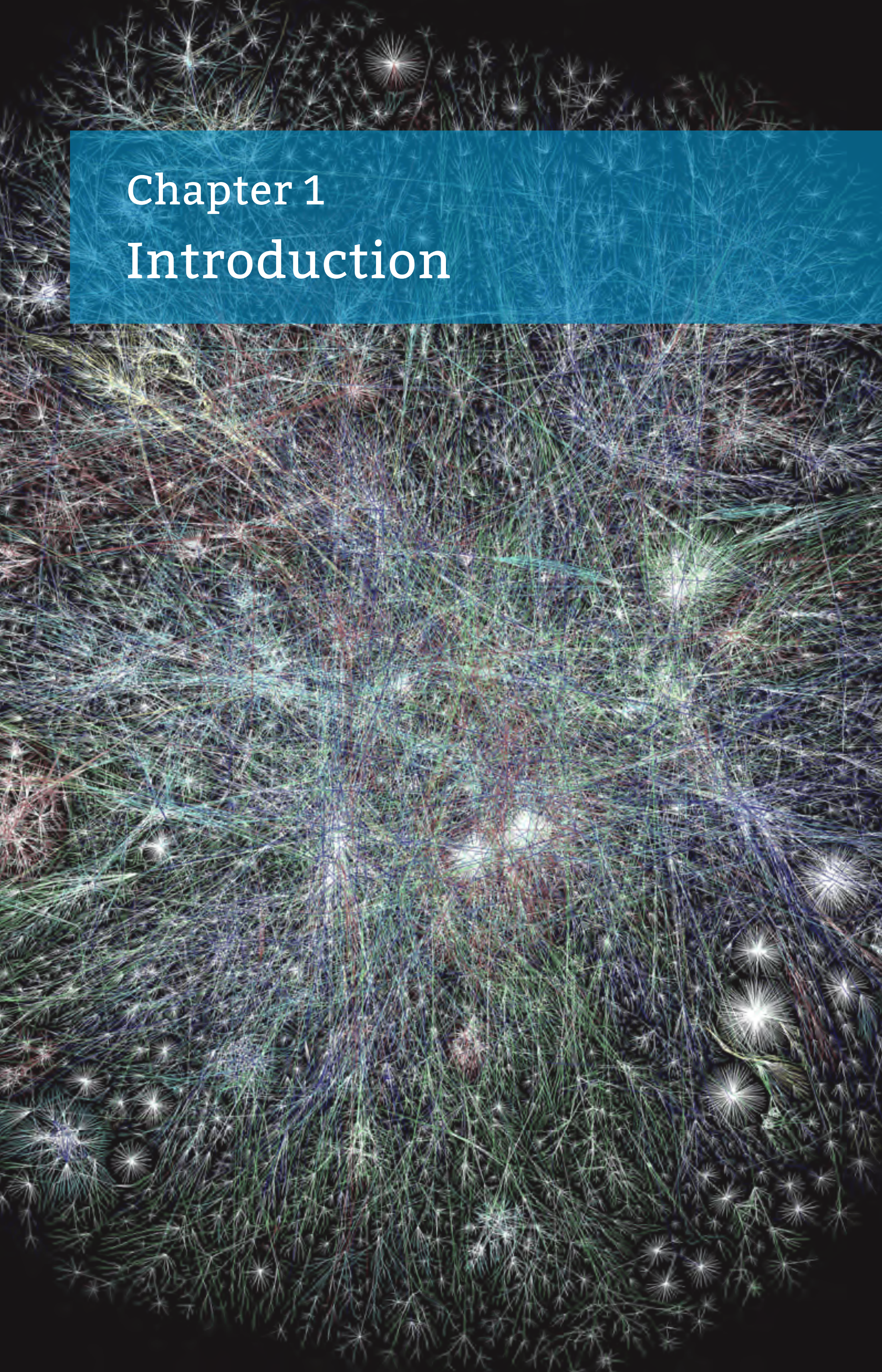
Cover design and layout by Malou Geurts Design

Chapter cover images:

1. The Opte Project, opte.org/maps/
2. Matthew Richmond, mattyrichy.wordpress.com
3. JohannesW, pixabay.com
4. Sebaso, flickr.com/photos/sebaso
5. Loes Derks van de Ven
6. Loes Derks van de Ven
7. Loes Derks van de Ven
8. Digitale Gesellschaft, flickr.com/photos/digitalegesellschaft
9. The Opte Project, opte.org/maps/

Contents

Chapter 1
Introduction



Introduction

It is December 29, 2013. After an eventful six months, digital activist, technologist, and researcher Jacob Appelbaum closes the year with a lecture called *To Protect and Infect, Part 2* at the 30th edition of the Chaos Communication Congress in Hamburg, Germany. In the lecture, which was connected to an at that moment released article in *Der Spiegel*, Appelbaum elaborates on the kind of surveillance activities the United States National Security Agency deploys (Spiegel Staff). He reveals, for instance, the existence of a dragnet surveillance system: TURMOIL. In addition, Appelbaum explains that the NSA, one of the United States' intelligence organizations, has many ways to break into computers, including the ability to adjust hardware, the ability to completely take over a mobile phone, and the ability to see a computer's screen by inserting a very small device into its hardware. It is not the first time Appelbaum speaks on this subject: he has been working on the subject of surveillance for a number of years and has already discussed similar issues in previous editions of the Chaos Communication Congress.

The classified documents that were shown in *To Protect and Infect, Part 2* came from whistleblower Edward Snowden and were an addition to the information that had already been leaked earlier that year. At the end of 2012, Snowden, then working for the NSA as a system administrator, had access to innumerable classified documents. Soon after the release of the documents he would explain that he does not "want to live in a world where we have no privacy and no freedom" and that he finds that the public has the right to know what their government is doing to them and doing on their behalf (Greenwald 47; Greenwald, MacAskill, and Poitras, par. 7). Later at the Dutch Big Brother Awards he added that he found the NSA's surveillance programs such a severe violation of human rights that it was his obligation to make the documents public. In the first part of 2013 Snowden undertook several attempts to contact research journalist Glenn Greenwald and documentary filmmaker Laura Poitras. They kept in contact through encrypted emails[1] during the months that followed. In early June 2013, Greenwald and Poitras finally met with Snowden in Hong Kong, China. On June 6 *The Guardian* published the first article: "NSA Collecting Phone Records of Millions of Verizon Customers Daily" (Greenwald). Soon after, Snowden fled from Hong Kong to Moscow, accompanied by WikiLeaks' Sarah Harrison. Among other things, the documents revealed the existence of PRISM, which is "a top-secret $20m-a-year NSA surveillance program" that grants the NSA access "to information on its targets from the servers of some of the USA's biggest technology companies: Google, Apple, Microsoft, Facebook, AOL, PalTalk and Yahoo" (Ball, par. 3). In addition, newspapers published documents that, for example, showed the existence of a controversial program that collects the telephone metadata of unknowing Americans, and that proved that the NSA had collaborated with the industry to weaken encryption and thus deliberately weaken security software (Ball, par. 2).

The discussion that the publication of the Snowden documents has sparked is certainly not new. What the

[1] A message is plaintext (sometimes called cleartext). The process of disguising a message in such a way as to hide its substance is encryption. An encrypted message is ciphertext. The process of turning ciphertext back into plaintext is decryption (Schneier, *Applied Cryptography* 1).

documents have revealed is related to a larger, ongoing public debate about surveillance: how much knowledge about citizens is just and necessary for governments to possess and what actions are legitimate to obtain that information? A landmark in this discussion is the Foreign Intelligence Surveillance Act of 1978. This act was passed after the Watergate scandal, when there was, as Glenn Greenwald mentioned in the 2013 Chaos Communication Congress keynote lecture, serious concern about the United States' surveillance capabilities and abuse. The FISA was "meant to rein in the intelligence community", and one of the ways in which this was done was through the establishment of a special court that would make decisions regarding wiretapping requests and warrants (Harris 63). It was, however, much easier to obtain a warrant through the Foreign Intelligence Surveillance Court than through a law enforcement case, and moreover, the warrants were assigned in secret. Author and journalist Shane Harris therefore describes the FISA as an "act of compromise, a way to give the spies the latitude they felt they needed to follow leads and expose foreign agents" (Harris 63). The attacks of September 11, 2001, sparked the debate again. In the aftermath of the attacks the United States' surveillance activities expanded drastically with the passing of the PATRIOT Act, the Intelligence Reform and Terrorism Prevention Act, and the broadening of the interpretation of the FISA.

Since Jacob Appelbaum, Glenn Greenwald, Sarah Harrison, and Laura Poitras have stood by Snowden during the process of the publication of the documents, they have formed a small group that has taken on a leading role in the debate. They are actively and publicly advocating freedom of information and government transparency, and are involved with several different organizations. Two features make this group particularly interesting. One of these features is its diverse composition. The group may share certain beliefs, but does not share a common background. Glenn Greenwald works as a journalist, Laura Poitras is a documentary filmmaker, Jacob Appelbaum is originally a technologist who is known for his work for the Tor Project and his affiliation with WikiLeaks, and Sarah Harrison is a journalist and legal researcher who is active for WikiLeaks. Appelbaum, Greenwald, Harrison, and Poitras are not the only individuals that are relevant to the larger group of individuals that works on privacy and surveillance issues. However, their diversity is a reflection of the diversity of the group concerned with these issues. The diversity of the individuals as well as the organizations working on the subject makes the group decentralized and distributed, and therefore complicated to define as a whole. Another striking feature of the group is that although they are United States citizens – except for Sarah Harrison, who is British – they have all had times in which it was not possible for them to live or work in their home country. Their previous work had aready drawn the attention of intelligence agencies, but since their involvement with Snowden they all have serious issues with the British and American authorities, especially while traveling. As a result, Greenwald currently lives in Rio de Janeiro, Appelbaum and Harrison live in Berlin, and Poitras has stayed in Berlin while working on her latest documentary on Snowden and has only recently returned to the United States. This leads to an interesting situation. On the one hand these individuals speak about issues that are strongly tied to the United States – the documents came from the United States' National Security Agency after all – yet they are not located in the same country as the discussion is tied to. On the other hand, the discussion goes beyond the United States borders. The core of the discussion is about human rights in the digital world, a world without clear borders, and is thus not tied one physical location.

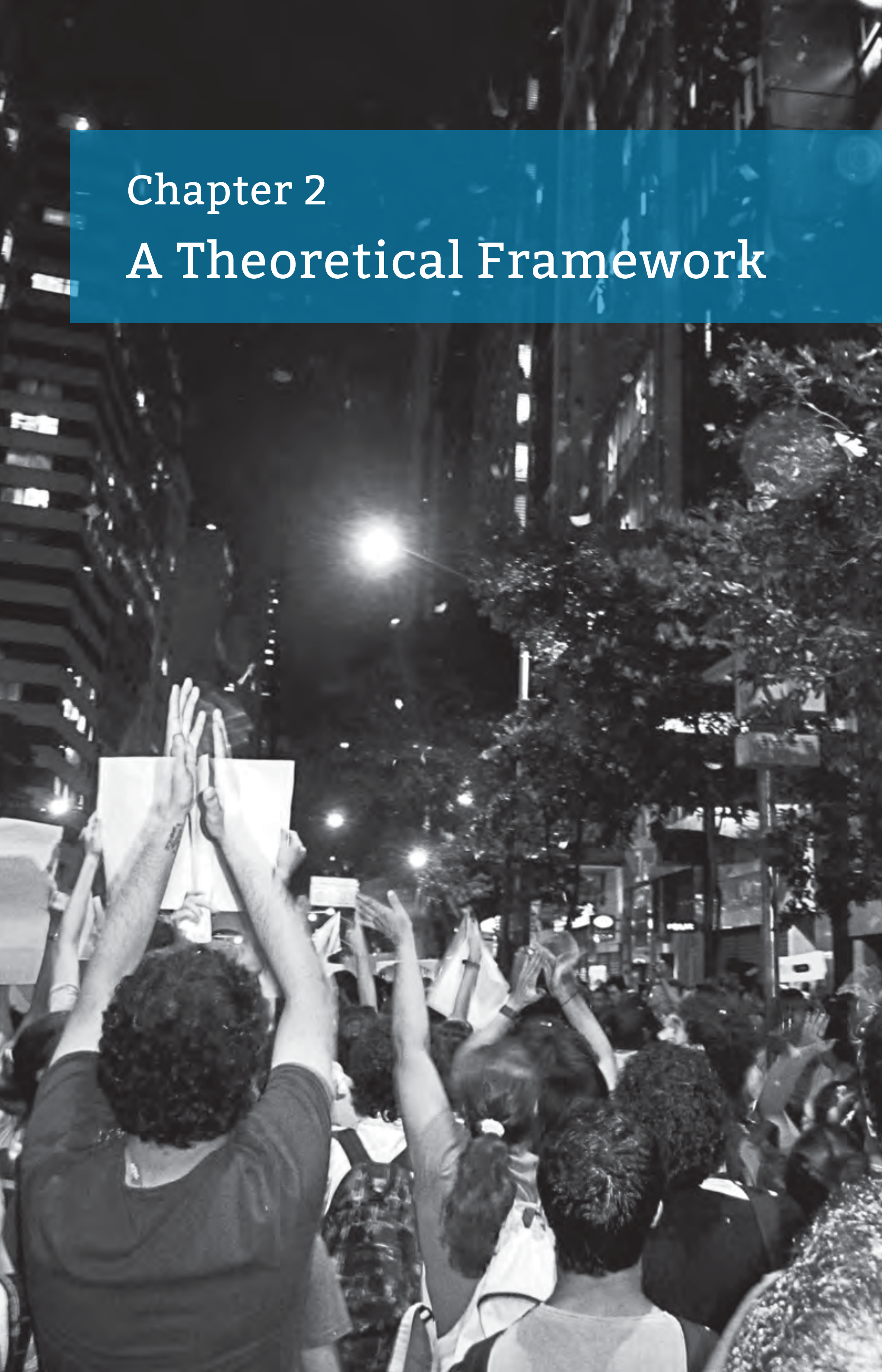
The debate on privacy and government surveillance may not be new, but by leaking the documents Snowden has, as Hans de Zwart of the Dutch digital rights organization Bits of Freedom points out in his lecture at the Big Brother Awards, changed the debate on this subject. Although Snowden is certainly neither the first nor the only whistleblower that has leaked information about this issue, the magnitude and impact of his revelations have caused the attention for both the debate and Snowden as an individual to grow immensely. This attention is constantly refueled: there are so many documents that even now, two years after the first publications, newspapers are still able to draw from them to publish stories. The documents have had a large impact on privacy activists: they have confirmed existing suspicion about the capabilities of intelligence agencies, and have therefore given more strength and a larger reach to the privacy activist's arguments.

Because the Snowden documents are still so recent, there is not a large body of academic work available on the subject. However, there have appeared a number of books on the subject since the publication of the documents. Some of the literature that is available focuses on Snowden's personal story, and analyzes his motives to blow the whistle and how he passed his documents on to the journalists. This is for example done in the first part of Glenn Greenwald's book *No Place to Hide. Edward Snowden, the NSA, and the U.S. Surveillance State*. The second part of the book further explores the Snowden documents and their implications. Security technologist Bruce Schneier's *Data and Goliath. The Hidden Battles to Capture Your Data and Control Your World* has a similar theme, and also explores the Snowden documents, the United States surveillance state and how it has affected society. However, not much work has appeared about how Snowden fits into a larger movement of privacy activists, or how that movement should be defined post-Snowden. Exploring the latter and thus bringing the movement of privacy activists in the post-Snowden era into sharper focus can contribute to our understanding of social movements in the digital age and the ways in which they perform dissent. A standard introductory work in the field of social movement theory is Della Porta and Diani's *Social Movements. An Introduction*. More focused on activism in the digital age is *Cyberactivism: Online Activism in Theory and Practice*, edited by Ayers and McCaughey. A standard work that analyzes culture, protest, and activism in the digital age is T.V. Reed's *The Art of Protest. Culture and Activism from the Civil Rights Movement to the Streets of Seattle*. De Cauter, De Roo, and Vanhaesebrouck have edited a book with a similar theme: *Art and Activism in the Age of Globalization*. All of the aforementioned literature focuses on different elements of social movements and are to some degree applicable to the privacy movement. There is, however, no complete work yet that fully concentrates on this movement post-Snowden. A more elaborate literature discussion of the literature can be found in chapter two.

By tying social movement theory and the elements of composition, leadership meeting places, and dissent together, this thesis as a whole will provide an understanding of how the group that initially helped Snowden fits into a larger movement of privacy activists. In order to do so, the group should be viewed as a movement, hence the choice to name it the privacy movement. Because of the far-reaching consequences of the Snowden documents, this thesis will focus on the privacy movement after the publication of those documents. A number of things are defining to the movement and are thus worth analyzing. First, it is useful to have a framework of theory that can offer some handles that help understand social movements before and in the digital age, and that can explain the larger academic and public debate the discussion is part of. This will be done in the second and third chapter of this thesis. The privacy movement as a whole seems to be diverse and quite decentralized, but Appelbaum, Greenwald, Harrison, and Poitras have taken on a leading role both in the discussion and within the movement. Chapter four will therefore explore loose forms of leadership and explain why leadership is important in social movements, who these leader figures are within the privacy movement, and what the movement's particular beliefs are. Despite the fact that the discussion on privacy and surveillance is cross-border, a place to meet in 'real life' still seems to be relevant to the privacy movement. Residence of Appelbaum and Harrison and former residence of Poitras, the flourishing digital culture of Berlin is increasingly turning the city into a place where many privacy activists gather. In chapter five will be further explored why physical spaces to meet still benefit movements in the digital age, and why Berlin proves to be that place for the privacy movement. These five chapters are subsequently followed by a case study about the privacy movement's expressions of dissent. The three different ways in which the privacy movement expresses dissent, namely through whistleblowing, through art, and through protest, each contribute to the understanding of the privacy movement as a whole. Whistleblowing is particularly interesting because its role is threefold. While it is one of the ways in which the privacy movement expresses dissent, whistleblowers are at the same time a vital source of information to the movement and also often become an activist within the movement. Chapter six will elaborate on the role of whistleblowers within the privacy movement. Activist art represents the privacy movement's ideas and goals, to movement members as well as to a larger public. Although there is only a small group of activists involved in the process of creating the art, it does affect the movement in its entirety. How art and activism merge becomes clear in two recent art projects associated with the privacy movement: *Panda to Panda* and *Anything to Say?* Chapter seven will explore the role of art within social movements, and the privacy movement in particular. Last, the privacy movement also expresses dissent through protesting. This is both done by traditional types of protest, for example street demonstrations, as well as by protest forms that can only exist online, for example the development, promotion, and use of programs that provide anonymity for Internet users. Chapter eight will explore how the digital age has influenced protest, and will focus on the Internet-supported and Internet-based forms of protest the privacy movement uses. The closing chapter of this thesis, the conclusion, will connect the previously mentioned elements of social movement theory, composition, leadership, meeting places, and dissent and will show how the group that has initially helped Snowden fits into a larger movement of privacy activists.

Chapter 2

A Theoretical Framework



A Theoretical Framework

In order to understand the privacy movement as a social movement, it is useful to have a framework of theory that can give an oversight of the academic debate this thesis fits into and the theories that can help to define the features that make a group of activists a social movement. Therefore, this chapter will first discuss literature relevant to this thesis. Subsequently, by looking at social movements before and during the digital age, the Right to Know Movement, and hacktivism it will provide the theory necessary to understand how the group of activists that the group around Snowden fits into can be understood as a social movement.

As the introductory chapter explained, the literature that has been published about Edward Snowden is limited. The general literature that is available, for example Glenn Greenwald's *No Place to Hide. Edward Snowden, the NSA, and the U.S. Surveillance State* and Bruce Schneier's *Data and Goliath. The Hidden Battles to Capture Your Data and Control Your World*, is mostly focused on Snowden's motives and the expansion of the surveillance state. Even less work is published about the group of privacy activists around Snowden. One of the books available is Michael Gurnow's *The Edward Snowden Affair: Exposing the Politics and Media Behind the NSA Scandal*. This book has a broader focus than just Snowden; it also looks at the media that published the documents and the politicians that were affected by the publication of the documents. It does, however, not focus on a group of activists as a whole. When focusing on academic work, a research paper that to a certain degree relates to this thesis is "Freedom Technologists and the New Protest Movements: A Theory of Protest Formulas" by John Postill. In the article, Postill describes a group that shows some similarities to the privacy movement. In order to define that group, he coined a new term: freedom technologists. Although the term freedom technologists comes close to describing the activists that make up the privacy movement, it is not included in this thesis. Freedom technologists are described as "geeks, hackers, online journalists, tech lawyers and other social agents who combine technological skills with political acumen to pursue greater Internet and democratic freedoms, both globally and domestically" (Postill 403). This does not entirely cover the activists that make up the privacy movement: while the term heavily focuses on technological skills, the composition of the privacy movement is more diverse than just technologically educated members. Furthermore, Postill does not see the freedom technologists as a movement in itself, but focuses on their contribution to other movements.

Although there is no research yet that is completely in line with this thesis, there are multiple aspects to the privacy movement that do fit in with other academic research. One of these aspects is social movement theory. A leading reference work is *Social Movements. An Introduction* by Donatella Della Porta and Marco Diani. This book gives an oversight of many different aspects of social movements. Similar to many other works about social movements, it makes extensive use of the Global Justice Movement and the protests in Seattle in 1999. Much has changed since the turn of the century, and the ways in which social movements use technology has advanced. Therefore this thesis can form a new example that adds to already existing, older examples such as the Global Justice Movement. Manuel Castells is an authority in the field of the information society and globalization. His book *Networks* *of Outrage and Hope. Social Movements in the Internet Age* explores, as the title implies, social movements and protests in the digital age. Although the research in this book concentrates on, for example, the Arab Uprisings and Occupy Wall Street, research into the privacy movement can be an addition to the research Castells does. Moreover, Castells defines a number of useful terms, which will be returned to later on in this chapter.

When looking at social movement theory, research shows that social movements started to change during the 1960s. In *Social Movements. An Introduction*, Italian researchers Donatella Della Porta and Mario Diani give an oversight in which ways they have changed and how that has affected academic research. The 1960s were a turbulent decade: political participation grew and elicited a rise in protests (Della Porta and Diani 20). These protests caused great change, including the way social movements are studied. Before the 1960s there was little interest in the study of social movements, but with the increase of protests the interest in social movements also increased. In the 1970s and 1980s it became "one of the most vigorous areas of sociology" and the theory available on social movements grew rapidly (1). Nowadays, social movement studies are well embedded in academic research (1).

It is not just the interest in the study of social movements that has changed after the 1960s. The increase of protest and the change in focus of that protest have also changed the academic approach to the interpretation of social movements. Before the 1960s, social movements focused on "capital-labor conflicts" (6). During and after the 1960s, however, the level of education rose and focus shifted to other social criteria, such as gender equality and environmental issues (6). Movements concerned with these new issues were named new social movements, and their change of focus left previous interpretation of social movements, through either the Marxist model or the structural-functionalist model, inaccurate (6). Although there was consensus among researchers that the focus had indeed shifted away from capital-labor related conflict in the 1980s, there was no agreement on how the central conflict in the new, programmed society should be identified. Della Porta and Diani mention a number of scholars who have diverse and interesting philosophies about new social movements. Alain Touraine, for example, thought that in essence not much had changed: in the programmed society, the ruling and the popular class will continue to oppose each other (8). Clause Offe noticed that the organizational structures of new social movements had become “decentralized and participatory”, that “interpersonal solidarity against the great bureaucracies” was defended, and that “autonomous spaces” instead of “material advantages” were reclaimed (9). Alberto Melucci claims that new social movements do not only seek material gain but also aim to protect “personal autonomy” and “try to oppose the intrusion of the state and the market into social life, reclaiming individuals’ right to define their identities and to determine their private and affective lives against the omnipresent and comprehensive manipulation of the system” (9). Last, Della Porta and Diani mention Manuel Castells. In his early work, Castells shifted the focus from the analysis of capital-labor conflicts to “social relations in the urban community” (10). In his later work, which will be explored further on in this chapter, new information technologies are central.

A Theoretical Framework

Della Porta and Diani use the Global Justice Movement as an example of what new social movements are and how they can be studied. The Global Justice Movement does not have "unitary, homogeneous actors", is concerned with a variety of issues, and protests through various ways (2). These three characteristics are a guidance of the three ways in which researchers tend to study social movements. First, researchers can focus on individuals. They are then seen as a group who express their opinion on social change (2). These individual opinions subsequently evolve in "various forms of political and social participation" (3). Second, researchers can opt to not focus on individuals but to look at events where individuals either meet their opponents or meet each other to "discuss strategies, to elaborate platforms, and to review their agendas" (3). Last, it is also a possibility to completely move away from studying individuals and focus on organizations concerned with certain issues (4).

Della Porta and Diani also have an own, current definition for social movements that can be helpful in defining the privacy movement:

> Social movements are a distinct social process, consisting of the mechanisms through which actors engaged in collective action:
>
> - are involved in conflictual relations with clearly identified opponents;
> - are linked by dense informal networks;
> - share a distinct collective identity. (20)

Especially relevant are the dense informal networks and the distinct collective identity. Having dense informational networks is what makes manifestations of collective action a social movement. When that happens a social movement process is in place, which means that "both individual and organized actors, while keeping their autonomy and independence, engage in sustained exchanges of resources in pursuit of common goals" (21). The contact between individuals and organizations is essential as they coordinate initiatives, coordinate individuals' actions, and coordinate strategies (21).

A social movement process can only be in place when a collective identity is developed that is not tied to a particular issue or campaign and continues after specific initiatives have ended (21). Della Porta and Diani explain what the function of a collective identity is:

> Collective identity is strongly associated with recognition and the creation of connectedness. It brings with it a sense of common purpose and shared commitment to a cause, which enables single activists and/or organizations to regard themselves as inextricably linked to other actors, not necessarily identical but surely compatible, in a broader collective mobilization. (21)

It is, however, important to note that individuals who feel part of a collective are not necessarily homogeneous and do not always share similar traits (24). It is also important to keep in mind that social movements are not the same as organizations, although networks can, but do not necessarily have to, include formal organizations (25). This indicates a certain kind of fluidness in the notion of social movements, which is necessary because social movements tend to dissolve when "organizational identities" become too dominant (26). Individual participation is therefore vital to social movements. This is never limited to "single protest events" but also occurs through "committees", "working groups", and "public meetings", as well as through the promotion of "ideas and viewpoints among institutions, other political actors, or the media" (26).

With the arrival of the Internet, society has entered the digital age. While technological advances and the rise of the Internet have strengthened the desire for government transparency and the need to rein in the power of the government, it has also altered the possibilities to perform civic activism and dissent immensely. In *Networks of Outrage and Hope. Social Movements in the Internet Age*, Manuel Castells explains this change through the analysis of, for example, the Arab uprisings and the Occupy Wall Street Movement. Castells makes use of a number of terms that are suitable to describe social movements in the digital age: contesting power, networks of counterpower, and the network society.

The Internet provides an autonomous space where individuals are free to connect and form networks (Castells 2, 7). The shift to the digital age has caused something that Castell calls mass self-communication, which means that the Internet and wireless networks are used "as [a] platform of digital communication" (6). 'Mass' is used here because it sends messages from many to many, and 'self' is used because even though the sender decides the content of the message, the sender (often) does not choose the recipient of the message.

In the introduction of his book, Castells elaborates on the notion of power in order to be able to explain the term counterpower. According to Castells the struggle for power always takes place in the mind of people, where meaning is created. Meaning is created through interaction between individuals and their environment and through the networking of neural networks with natural and social networks (5-6). This is done through communication, which is defined as "the process of sharing meaning through the exchange of information" (6). The digital age changed the technology that can be used to communicate with, which allows communication to reach every aspect of social life "in a network that is at the same time global and local, generic and customized in an ever changing pattern" (6). Although usually very diverse and different for each individual, there is one thing all processes of creating meaning have in common: they heavily depend on "the messages and frames created, formatted and diffused in multimedia communication networks" (6). The change in communication has directly influenced how meaning is created and how "power relations" are established (6). Castells subsequently analyzes power in our current society:

> In our society, which I have conceptualized as a network society, power is multidimensional and is organized around networks programmed in each domain of human activity according to the interest and values of empowered actors. Networks of power exercise their power by influencing the human mind predominantly (but not solely) through multimedia networks of mass communication. (7)

What Castells explains here makes communication networks a valuable source of power-making. These networks of power share their desire "to control the capacity of defining the rules and norms of society through a political system that primarily responds to their interests and values" (8). Counter-power then will deliberately attempt to contest that power through networks that have interests and values opposite, or alternative, to those of the dominant networks of power (9). In order for these networks to become stronger than the dominant networks already present in society, it needs to "reprogram the polity" of what they try to change by introducing other instructions in both the institution's programs as well as in their own lives (17). These networks of counterpower are social movements, defined by Castells as "producers of new values and goals around which the institutions of society are transformed to represent these values by creating new norms to organize social life" (9). At the birth of a social movement often stands a small group of individuals called agency, and the trigger of forming a movement always lies in injustice, for example the violation of privacy (13).The protest a social movement makes is usually based on emotions. Two kinds of emotions are particularly relevant: fear (negative) and enthusiasm (positive). These two emotions are linked to two motivational systems: approach and avoidance. From enthusiasm flows hope, but in order to achieve hope, individuals need to overcome anxiety, a negative emotion that comes from the avoidance motivational system. Anxiety is in general overcome by anger, which "increases with the perception of an unjust action and with the identification of the agent responsible for the action" (14). When anxiety is overcome, positive emotions will take over. This will however only happen when individuals connect to other individuals, which asks for "a communication process from one individual experience to another" and can only happen if there is "cognitive consonance between senders and receivers of the message" and if there is "an effective communication channel" available (15). The communication mediums available in the digital age are the "fastest and most autonomous, interactive, reprogrammable and self-expanding means of communications in history" (15). This influences the communication process between individuals, because the faster and the more interactive this process is, the more likely it is that it will form a collective action (15). This distinguishes social movements in the digital age from previous types of movements: because the communication mediums are so interactive and easy to configure, the organization of a network is not hierarchical but exceptionally participatory (16).

The Internet may have caused a change in social movements, many sources point to a time in which the Internet had yet to be invented as having an equally large influence on social movements. In the 1960s, many different movements and protests changed what the world looked like. Politics in the United States during the 1960s and 1970s were also quite eventful. Events such as the Vietnam War, the passing of both Martin Luther King Jr. and Robert Kennedy, and protests in cities and on campuses each "challenge the power and reach of the national security state" (Scott 4). The passing of the Foreign Intelligence Surveillance Act in 1978 was one of the changes that eventually came from the turbulent 1960s. In *Reining in the State. Civil Society and Congress in the Vietnam and Watergate Eras*, Katherine A. Scott introduces the Right to Know Movement, which came into existence during those tumultuous years. The individuals that compose the movement are diverse. The individuals Scott identifies as the movement's leaders include a newspaper editor, whistleblowers, politicians, and a staff member of the American Civil Liberties Union (2). The neo-progressive reformers of the Right to Know Movement believed in the power of good government (3). Its main objective was, as the name indicates, "transparency and accountability from public institutions" (184). It believed that the public is entitled to know about the actions their government undertakes, that transparency will strengthen democracy, and the state should not infringe on citizens' rights by expanding its powers without those citizens' consent (9). Although the movement did value the balance between the "right to know" and the "need to protect", there was a strong belief that the ability to freely exchange information was a pillar of a free society and that citizens could only control their government when they are well-informed (24). The movement hoped and expected that citizen activism would be able to put a halt to government abuse and thus make government transparency possible (184). Making efforts to terminate the surveillance programs that whistleblowers had revealed in the 1970s was a practical manifestation of these aims (4). However small and decentralized the movement may have been – existing of a small group of government activists, investigative journalists, elected officials, and public interest groups – its efforts were significant. Through the establishment of institutions as the Freedom of Information Committee and the passing of acts as the Privacy Act and the FISA it was able to influence both United States national security policies and the public opinion (7, 12, 184).

Another influence on the privacy movement is hacktivism, and digitally correct hacktivism in particular. In the chapter "Keynote: Not My Department" from the book *Talks 2005-2013*, Appelbaum explains the reasoning behind digitally correct hacktivism as follows:

> And we should do it towards some goals. We should try to consider that when we build free and opensource software[2], when we build free and opensource hardware, we are enabling people to be free in ways that they previously were not. Literally, people that write free software are granting liberties. (46)

In *Hacktivism and Cyberwars. Rebels with a Cause*, British researchers Tim Jordan and Paul Taylor give a detailed account of what hacking and hacktivism exactly is. They define hacktivism as follows:

> Hacktivism is the emergence of popular political action, of the self-activity of groups of people, in cyberspace. It is a combination of grassroots political protest with computer hacking. Hacktivists operate within the fabric of cyberspace, struggling over what is technologically possible in virtual lives, and reaches out of cyberspace utilizing virtual powers to mold offline life. Social movements and popular protest are integral parts of twenty-first-century societies. Hacktivism is activism gone electronic. (1)

[2] "Open source software is software whose source code is available for modification or enhancement by anyone" ("What is Open Source").

A Theoretical Framework

The roots of hacktivism come from three different currents, namely hacking, informational societies, and modern social protest and resistance (2). It is the seventh generation after six generations of hacking and emerged in the 1990s (6). Like Scott in *Reining in the State. Civil Society and Congress in the Vietnam and Watergate Eras*, Jordan and Taylor begin their explanation of social movements in the 1960s, when popular politics drastically changed and many new movements emerged (46). They too point to the 1960s and 1970s as decades that changed the "framework for radical, transgressive, non-institutionalized politics" (46). The framework that subsequently emerged did not exist of solely one movement, but exists of many different movements that each "engages and defines a form of radical struggle" (48). Combined, these movements form the whole of radical politics (48). In the 1990s another significant change took place: a new social and cultural form emerged that was often described as "informational, postmodern, postindustrial, complex, mobile and(/or) networked" (20). Jordan and Taylor call this "viral times", but also join Castells by using the terms "information society" and "networked society" to describe the digital age. It is in these viral times that hacktivism emerges: because information acts in a viral-like way it is increasingly difficult to assert institutional control on it (20). They state that "hacktivists are the marriage of the spirit of the hack and the spirit of protest in the context of viral times" (3).

Hacktivism can be distinguished into two streams: direct action hacktivism and digitally correct hacktivism. Jordan and Taylor explain the difference between the two through the example of FloodNet. FloodNet is a program designed by the Electronic Disturbance Theater and used by the Zapatista movement in Mexico. It slows a network server down and by that it limits the capacities of a network. Digitally correct hacktivism does not agree with these kinds of direct actions, because they hamper information to reach individuals. Canadian hacker Oxblood Ruffin, member of the hacker organization Cult of the Dead Cow, affirms this point of view in the following quotation:

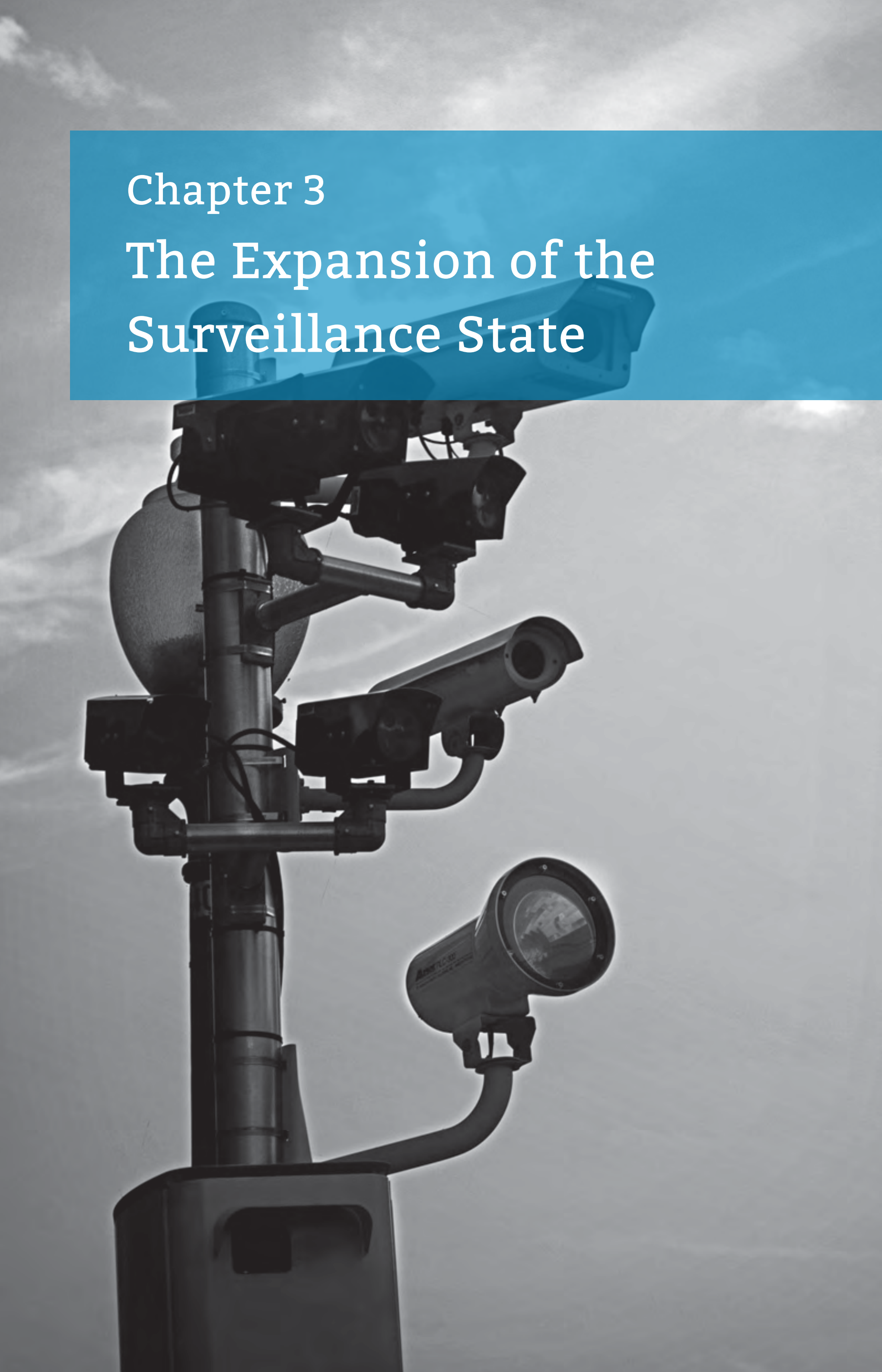
> Denial of Service attacks are a violation of the First Amendment, and of the freedoms of expression and assembly. No rationale, even in the service of the highest ideals, makes them anything other than what they are – illegal, unethical, and uncivil. One does not make a better point in a public forum by shouting down one's opponent. Say something more intelligent or observe your opponents' technology and leverage your assets against them in creative and legal ways […] Hacktivism is about using more eloquent arguments – whether of code or words – to construct a more perfect system. One does not become a hacktivist merely by inserting an 'h' in front of the word activist or by looking backward to paradigms associated with industrial organization. (98)

A free flow of information is a right that digitally correct hacktivists find extremely valuable. Their battle is not about the rights of technological appliances but about the social value those appliances offer humans (91). Digitally correct activism is a mix of politics and technology, summarized in the term "politico-technological formation" (110). The human right to free flows of information and secure access to information can be translated as "secure, private access to the Internet" (97). Similar to the Right to Know Movement, digitally correct hacktivists have a strong belief in the power of information and citizens' right to know what is going on in the world. A constant and unrestrained Internet flow is necessary to achieve that (97, 141). However, this does not mean that all information should be accessible, although the exact boundaries remain blurry (196).

To achieve unrestricted access to information, digitally correct hacktivists design programs that help to accomplish their political goals. Jordan and Taylor uses hacktivist group Cult of the Dead Cow and the peek-a-booty program as an example. Cult of the Dead Cow is a "loose network of individuals, ideas and actions" that is known for their hacking tools and willingness to publicly speak about them (98). Peek-a-booty is a peer-to-peer application developed by Cult of the Dead Cow. The program enables Internet users to avoid (by the government imposed) firewalls, which shows their disapproval of Internet surveillance.

Joining the debate on how social movements express dissent in the digital age, this chapter has given insight in several aspects that can help define the privacy movement. Della Porta and Diani's theory about social movements has given a short introduction into how social movements have changed since the 1960s and how new social movements function. Castells has complemented this with theories about counterpower and the network society, which has broadened the understanding of social movements in the digital age. The Right to Know Movement and digitally correct hacktivism are two influences on the privacy movement that help understand the roots and the body of ideas of this movement.

Chapter 3
The Expansion of the Surveillance State



The Expansion of the Surveillance State

The documents Snowden has leaked are related to an already existing public debate on government surveillance. The magnitude and the implications of the classified NSA documents, however, have given this debate a whole new dimension, in the United States as well as in the rest of the world. Without a global idea of the public debate around the expansion of the surveillance state it would be difficult to understand the impact of the Snowden documents and the privacy movement's beliefs, concerns, and goals regarding this topic. This chapter therefore aims to give an overview of the process of securitization, the rise of the surveillance state in the United States, and the Snowden documents in order to help understand the public discussion this thesis fits into.

> You had to live — did live, from habit that became instinct — in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized. (12)

This quotation, taken from George Orwell's novel *1984* and written as science fiction, is nowadays often used to illustrate a trend in the current Western world that is described as the process of securitization. In the Dutch article "Het recht op veiligheid schept een permanente noodtoestand" (The Right to Security Creates a Permanent State of Emergency), Beatrice de Graaf, professor in the University of Utrecht, and Willem Schinkel, professor in the Erasmus University Rotterdam, explain this process. Securitization means that politics assigns increasing importance to the notion of security. Threats and risks in general need to be suppressed, waiting for them to materialize is no longer an option. This causes a change in government policy. When security, instead of for example justice, becomes a central part of government politics, the priority of certain principles shifts. The focus on legal protection, proportionality, rehabilitation, and inclusion will move to selective protection through law, punishment, surveillance, and exclusion. This subsequently leads to a situation where there is constant surveillance on social life (De Graaf and Schinkel, par. 2, 6, 7, 9).

Similar to de Graaf and Schinkel, Dutch research journalist Bart De Koning describes this as a very subtle process in his book *Alles Onder Controle* (Everything under Control). In this book, De Koning explains the paradox of freedom: giving up freedom in order to be free (De Koning 67). He mentions two philosophical schools that each has developed its own view on how much freedom citizens should enjoy. One school, that includes thinkers such as Plato and Hegel, places the interest of the state above the interest of individual citizens. Individuals cannot and should not be trusted. Another school, to which thinkers such as Popper, Smith, and Von Hayek belong, assumes individuals are good by nature. The state should do what is necessary, it is merely there to safeguard the freedom and safety of its citizens. The United States proves a good example of how the viewpoints of the second school can be applied. By creating checks and balances, the Founding Fathers have tried to prevent the state from abusing its power. This shows a great trust in its citizens and certain mistrust in the power of the state. Through the notions of life, liberty, and the pursuit of happiness the Declaration of Independence protects the rights of American citizens (68-69). Slowly but surely this society, that once had greater faith in its individual citizens than in the state itself, is changing into what De Koning calls a low trust society: there is little mutual trust in each others capability and integrity and therefore surveillance is necessary (59).

Who is at the basis of this change, citizens or the state, seems to be in balance, according to De Koning. On the one hand citizens expect an increasing amount of safety from their government, on the other hand governments also respond to growing feelings of insecurity among citizens in order to legitimize the increase of government surveillance (60-61). De Koning notices that politicians often use war metaphors to legitimize security policy, for example the War on Terror that President Bush initiated after the attacks of September 11, 2001. He explains that research has shown that people who are afraid take a more radical stance than people who are not. When experiencing feelings of insecurity and fear, people tend to look for protection and support. Given the far-reaching consequences of (the threat of) war, people are generally not willing to take any risk and government measures are often easily accepted. Moreover, people are more prepared to give up certain liberties, like privacy, during times of war (53).

De Koning points to the advance of technology as an enhancing factor to this process. The advance of technology caused a change in our attitude towards privacy; before the Internet age it would have been unthinkable that people would voluntarily carry a small device with which every move becomes traceable. Yet this is exactly what has happened with mobile phones (35). In "Surveillance Blowback. The Making of the U.S. Surveillance State, 1898-2020", Alfred W. McCoy traces this development back to 1878 when the quadruplex telegraph and commercial typewriter were invented and allowed textual data to be send around the world (McCoy, par.

9). Many technological developments followed, leading up to the ability to collect all sorts of data of individuals. But why do we collect, use, and store all that data? Because we can, claims De Koning. The data that modern electronic devices nowadays spread is fairly easy to access and is deemed incredibly valuable by both the police and intelligence agencies. In addition, the technology available for police and intelligence agencies is continuously becoming more advanced, which enables them to collect more (De Koning 38-39). Furthermore, security technologist Bruce Schneier makes two relevant remarks. First, due to the Internet the same hardware and software is used worldwide, which makes it much easier to break a system. Second, global communication has made it challenging make a selection of which data is collected, because the networks that are used are not tied to a specific country or group, for example criminals (Schneier, *Data and Goliath* 64).

In order give a brief insight in the history of surveillance, this part of the chapter will follow the example of Bruce Schneier in *Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World* and will focus on the United States. The United States' surveillance activities are strongly tied to the Snowden documents, have a global impact, and set a telling example of the capabilities of most modern day intelligence agencies.

Government surveillance activities have rapidly developed over the past hundred years. Alfred W. McCoy argues that the roots of government surveillance in the United States lie in the Philippine – American War at the end of the 19th century, when the United States started applying innovations such as "rapid telegraphy, photographic files, alpha-numeric coding, and Gamewell police communications" (McCoy, par.

14). Surveillance further developed in the twentieth century, in which three moments were particularly significant. First, there is the formation of the National Security Agency by President Truman in 1952. Originally, the NSA focused solely on foreign gathering (Schneier, *Data and Goliath* 62). When the Cold War ended in the late 1980s, focus logically shifted from foreign intelligence gathering to protecting communication "from the spying of others" (63).

A second significant moment is perhaps more an entire era than one specific moment in time. The 1960s were turbulent years in which United States intelligence agencies were discredited for several reasons. Both McCoy and Schneier point to 1960s and 1970s as times in which the NSA and the FBI spied on "all sorts of Americans [...] – antiwar activists, civil rights leaders, and members of nonviolent dissident political groups (Schneier, *Data and Goliath* 63). This was done through excessive actions such as operation COINTELPRO. The Church Committee, which investigated governmental intelligence activities, claimed that the operation deployed "unsavory and vicious tactics [...] including anonymous attempts to break up marriages, disrupt meetings, ostracize persons from their professions, and provoke target groups into rivalries that might result in deaths" (McCoy, par. 25). The 1970s are inextricably connected to the Watergate scandal, the illegal tapping of the Democratic National Committee that eventually caused President Nixon to resign ("The Watergate Story"). Not long after President Nixon's resignation, amidst the already existing commotion, *The New York Times* reporter Seymour Hersh published about Operation Chaos, which was "a program to conduct massive illegal surveillance of the antiwar protest movement" (McCoy, par. 24). It held a database with

300,000 names (McCoy, par. 24). After these events, the power of intelligence agencies was under discussion. The Foreign Intelligence Surveillance Act and the accompanying FISC court were established. As the first chapter mentioned, the FISA was meant to restrain intelligence organizations' power and create oversight in requests for wiretapping and warrants (Harris 63). Opinions do, however, vary on how well these measures actually worked. Schneier calls the FISA one of the current pillars of the NSA's authority. In 2008, an Amendment Act was added to the original act. Section 702 retroactively allowed the collection of data from non-U.S. citizens and was used by the NSA to "monitor the Internet backbone connections entering the country, harvesting data on both foreigners and Americans" (Schneier, *Data and Goliath* 66). Schneier also mentions two other pillars that give the NSA its authorities: Executive Order 12333 and the USA PATRIOT Act. Executive Order 12333 was signed by President Reagan in 1981 and "permits the NSA to conduct extensive surveillance abroad [and] allows for extensive collection, analysis, and retention of American's data" (66). The USA PATRIOT Act was enacted after September 11, 2001. Through this act, and specifically through section 215, the NSA was authorized to collect "any tangible things (including books, records, papers, documents, and other items) [...] for an investigation to protect against international terrorism or clandestine intelligence services" (66).

The enactment of the USA PATRIOT Act has everything to do with the third significant moment: the terrorist attacks of September 11, 2001. Although this was a poignant event for the entire Western world, it was particularly upsetting for the United States' intelligence agencies. On September 10, the day before the attacks, intelligence agencies had already intercepted calls that indicated the next day's attacks. In addition, the names of some of the perpetrators were already on terrorist watch lists that United States intelligence agencies kept (Schneier, *Data and Goliath* 9). The systems of the intelligence agencies had failed to solve the puzzle in time and the government had, as Shane Harris puts it in *The Watchers. The Rise of America's Surveillance State*, "failed to connect the dots" (Harris 9). The United States government was determined to never let this happen again. Schneier concludes that "the only way to have any hope of preventing something from happening is to know everything that is happening" (Schneier, *Data and Goliath* 63). This has eventually led to striking slogans found in NSA presentations: "collect it all", "know it all", and "exploit it all" (64).

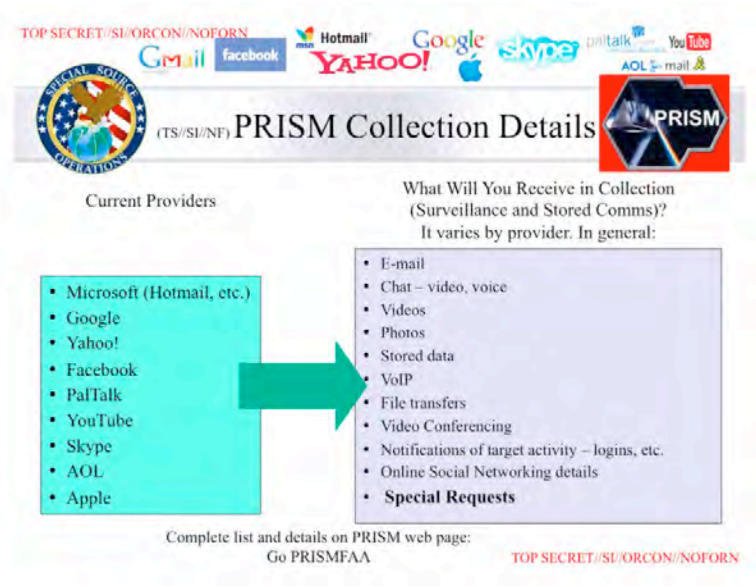
In the Dutch documentary *De Jacht op Edward Snowden* (The Hunt for Edward Snowden), former director of the National Security Agency Michael Hayden describes Snowden's revelations as follows:

> What Snowden disclosed wasn't information; it disclosed how we collected information. In other words: he didn't reveal a bucket of water, he revealed the plumbing.

In addition, he also calls it "the most serious hemorrhaging of legitimate American secrets in the history of my country" ("De Jacht op Edward Snowden"). In *No Place To Hide. Edward Snowden, the NSA, and the U.S. Surveillance State*, Greenwald explains that statements of people such as former NSA official William Binney had helped to form a general idea of the surveillance capabilities of the NSA – in 2007 *The Washington Post* already published how the NSA intercepted and stored data of different means of communication of American citizens. The Snowden documents were the first documents that could confirm and exceed those suspicions (Greenwald 99). The documents were very recent, from 2011 to 2013; were all marked top secret; and included, among other documents, FISA court orders and a Presidential Decision Directive on offensive cyber-operations (91). In addition, the documents revealed an extensive web of secret surveillance programs (90). These surveillance programs were both aimed at Americans and foreigners, including United States allies, and with these programs the NSA had the ability to intercept virtually all means of communication. The programs were used to spy on suspected terrorists and criminals. However, they were also used to spy on political leaders of foreign (allied) countries as well as on "ordinary" United States citizens and foreigners (92). By tapping Internet servers, satellites, underwater fiber-optic cables, telephone systems, and computers the NSA collected both metadata and content (133). Although content refers to the actual content of an individual's Internet and telecom communications, metadata is often more valuable because it provides information about the nature of the communications. Whereas it can be difficult to decipher the meaning of content, metadata gives very clear, easily accessible information about the sender, the receiver, the time, their location, the device used, et cetera (133).

Over the course of time, newspapers such as *The Guardian*, *Der Spiegel*, and *The Washington Post* have released information about many of the NSA's surveillance programs. The first release in the string of articles that would follow was in *The Guardian* and was about the BOUNDLESS INFORMANT program. With BOUNDLESS INFORMANT the NSA can keep track of how many telephone calls are made and how many emails are sent around the entire globe. The existence of this program showed that the NSA had not been honest with the United States Congress when they denied they were capable "of providing specific numbers," as that was the exact purpose of the program (Greenwald 92). In addition, the program also revealed the existence of a FISA court order that forced American telecom company Verizon to hand over the metadata of their American customers to the NSA (92-93).

Another high-profile surveillance program of which information was published is PRISM. With the PRISM program the NSA has unlimited access to the data of the nine largest Internet companies. In order to collect the data of a United States citizen a warrant is necessary, but for mass surveillance of non-American citizens outside of the United States this is not the case (108-112). Figure one shows an official slide of the program and summarizes the scope of PRISM.


SPECIAL SOURCE OPERATIONS
Gmail
facebook
msn Hotmail
YAHOO!
Google
skype
paltalk
YouTube
AOL mail
PRISM

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) PRISM Collection Details

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)?
It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

Fig. 1. Official slide of the PRISM program. "NSA Prism Program Slides." theguardian.com. *The Guardian*, 1 Nov. 2013.

In addition to BOUNDLESS INFORMANT and PRISM, many more programs were revealed. There were for instance PROJECT BULLRUN, which is a collaboration with the British Government Communications Headquarters (GCHQ) aimed at eliminating the most common forms of encryption, and STORMBREW, a collaboration with the FBI that provides the NSA access to certain points where Internet and telephone traffic enters the United States (94-107). The documents also showed that the NSA uses several methods to obtain information. As mentioned, it can tap directly into fiber-optic lines that transmit international communications. Another method it uses is the redirection of "messages into NSA repositories when they traverse the US system", which the majority of international communication does (101).

Sometimes the NSA forces telecom companies to pass on information, but in other cases it has partnerships with these companies. With a program named BLARNEY, the NSA uses the access United States telecom companies have to certain international systems. Among the states that are targeted are the entire European Union, the United Nations, and United States allies like France, Germany, and Israel (103). In addition, the NSA also has partnerships with private organizations, for example with Edward Snowden's former employer Booz Allen Hamilton, and foreign governments (101-121).

The expansion of the surveillance state has been an ongoing process of which the roots can be traced back to the end of the 1800s. Although there was, of course, a certain awareness of the scope of intelligence agencies' surveillance capabilities, information on surveillance programs is generally not made public. The Snowden documents thus gave an unprecedented insight into those surveillance capabilities. What the documents revealed has shocked many, including members of the privacy movement. The movement has very specific beliefs and aims regarding the subject of surveillance and privacy. What these beliefs and aims exactly are will be explained in chapter four.

Chapter 4
Leadership in the Privacy Movement

Leadership in the Privacy Movement

The previous two chapters have created a theoretical framework that has explored the theory necessary to understand the privacy movement as a social movement, and has explained the public debate the privacy movement is concerned with. In order to get a good image of what is defining for the privacy movement, this chapter will explore the role of leaders in a movement in the digital age, who the individuals are that take on a leading role in the privacy movement, and what the privacy movement's core beliefs and aims are.

Within the privacy movement there is a small group of individuals active that acts as movement leaders. They are often at the forefront, bring individuals and organizations together, and have generated quite some attention for the privacy movement's cause, especially after the release of the Snowden documents. Their leadership is not traditional in the sense that the relationship with followers is "dyadic [and] asymmetric", or that their leadership relies on the followers' recognition of their charisma (Diani 106). In *Social Movements and Networks. Relational Approaches to Collective Action*, Mario Diani explains that leadership can also occur without these traditional types of relationships. Moreover, Diani argues that leadership does not have to occur within a "unified organization" in which leaders dominate supporters and have the capacity to impose sanctions on them (106). Instead, these leaders have other forms of influence: they can, for example, have the ability to "promote coalition work among movement organizations" or are "perceived by media and political institutions as movement "representatives"" (106).

There are two ways in which leaders are important for social movements: they can function as a communication link and thereby form alliances and coalitions, and can persuade other individuals to join a movement. Making links, alliances, and coalitions is particularly important for the privacy movement. The movement as a whole is currently quite decentralized, according to Appelbaum in a personal interview (Appelbaum). The initiators of Code Red, an initiative aimed at the reform of security organizations, affirm this. They, too, notice that there is often not enough contact between different domains and activists, and that valuable data is not always widely shared and sufficiently available ("Modus Operandi"). This lack of communication can be caused by "specific political or social barrier[s]", such as differences in "specific goals", strategy, and "tactical options" (Diani 107). The role of movement leaders can potentially have a beneficial influence according to a 1970s research Della Porta and Diani refer to in *Social movements. An Introduction*. The research considers activists as links between organizations that form the basic organization of a movement (Della Porta and Diani 127). They also mention studies, on both movements and political organizations, that conclude that when leading activists share experiences and have a denser relationship, there is a higher chance they will cooperate (Della Porta and Diani 129). When these leading activists are linked and are involved in multiple organizations, this can then be seen as "a specific form of social capital" that can benefit from cooperation among organizations, even when there is no public mobilization yet (Diani 108-109). Thus, leaders within the privacy movement fulfill the role of something Diani calls a "communication link": they form alliances and coalitions, which has a positive effect on the strength of a movement (Diani 106).

When leaders enter into multiple collaborations and are solidly embedded in their communities, it has a second advantage: the presence of a social network increases the chance of other individuals becoming involved. To explain this, Della Porta and Diani refer to an environmental movement in Milan in the 1980s where 78 percent of its members had become involved through personal contact (Della Porta 117-118). Involvement, in turn, increases the movement's significance (115). Furthermore, when new individuals become involved in a movement, their "participation also forges new links, which in turn affect subsequent developments in their activist careers" (115). These connections are not solely created within organizations. Surveillance and privacy are very current issues and innumerable events are organized around this theme. These social and cultural activities prove to be quite important. When activists participate in these sorts of activities, they "reproduce specific subcultural or countercultural milieus that offer both opportunities for protest activities and for the maintenance and transformation of critical orientations even when protest is not vibrant" (117). With regard to the digital age, Della Porta and Diani touch upon another significant issue, namely the importance of "real" social contact between activists. The modern technological possibilities that are now available may lead one to suspect that maintaining solely virtual contact is sufficient. This is, according to Della Porta and Diani, not the case. Although there is certainly evidence that the Internet develops social links, there is also evidence that suggests that "real life" links are necessary for virtual networks in order to operate sufficiently (133). This also applies to transnational networks. While the Internet does make it easier to coordinate global campaigns, within this context the Internet also mostly links individuals that have previously met in person and thus know each other in real life (133).

One of the individuals that can be seen as a movement leader within the privacy movement is Jacob Appelbaum. Keywords to describe him include hacker, activist, photographer, writer, journalist, and public speaker. However diverse his activities may be, the connecting thread in his work is his concern with human rights issues. In the past he has spent time working for environmental organizations such as Greenpeace and the Rainforest Action Network, and has traveled to the Middle East as well as to New Orleans after hurricane Katrina to provide technical assistance to those who needed it the most. He also became involved with the Tor Project, for which he is still active as a developer and trainer, and later became the only American working for WikiLeaks (Hill, par. 10; Appelbaum, "Archive"). Appelbaum can nowadays perhaps be best described as computer security researcher; he still travels the world to promote the Tor Project, lectures on topics related to cyber-security, and is engaged in research for different newspapers, including *Der Spiegel* for which he continues to work on Snowden's documents. He currently lives as a digital exile in Berlin, Germany, due to ongoing investigations about his affiliations with WikiLeaks (Appelbaum; Hill, par. 46).

Journalist Glenn Greenwald, another individual who functions as a movement leader, shares Appelbaum's concern with human rights. In the early years of his career, Greenwald worked as a litigator defending civil rights (Reitman, par. 8). Later Greenwald made a career switch to journalism. He first started keeping a blog, *Unclaimed Territory*, in which he criticized United States politics, and in particular the United States' security strategy (Reitman, par. 25). In 2007 Greenwald became a contributing writer for *Salon* and a few years later he started writing a column in *The Guardian*, where he continued to write about civil liberties and United States security issues. He has also written a number of books, with titles as *How Would a Patriot Act? Defending American Values From a President Run Amok*, *With Liberty and Justice for Some: How the Law Is Used to Destroy Equality and Protect the Powerful*, and *Great American Hypocrites: Toppling the Big Myths of Republican Politics*. In 2014 he released his latest book, *No Place to Hide: Edward Snowden, the NSA and the U.S. Surveillance State*. Greenwald has received numerous awards for his work and was indicated as one of the 25 most influential political commentators in the United States by *The Atlantic* ("Glenn Greenwald"). Together with Pierre Omidyad, Jeremy Scahill, and Laura Poitras he founded First Look Media in 2013. First Look Media is a non-profit news organization that has launched *The Intercept*, an online publication of which Greenwald is a co-founding editor ("About Us").

Glenn Greenwald and Jacob Appelbaum have both collaborated with documentary filmmaker Laura Poitras, for example when they were working on the publication of the Snowden documents. Laura Poitras is originally a trained chef, but found herself more interested in film and therefore studied at the San Francisco Art Institute and the New School. While studying in New York, Poitras witnessed the 9/11 attacks on the Twin Towers and decided to capture the reactions of bystanders. The images resulted in her first (short) film: *O'Say Can You See* (Vasseur, par. 4-6). A number of films have followed since, such as the post-9/11 trilogy consisting of *My Country, My Country*; *The Oath*; and *CITIZENFOUR* ("Films"). Her films critically address civil liberties and political issues through personal stories. Where Appelbaum and Greenwald tend to generate much attention, Poitras does not often seek publicity, but lets her films speak for her instead. That, however, does not mean that she does not receive much attention: her work is highly praised and she has recently won an Academy Award for Best Documentary for *CITIZENFOUR*. Poitras has lived in Berlin while working on *CITIZENFOUR*, and has only recently returned to the United States. She is currently working on a new film and on a solo exhibition at The Whitney Museum, and is a co-founding editor at *The Intercept* (Hill, par. 39).

While Greenwald, Poitras, and Appelbaum have worked on the publication of Snowden's documents, British Sarah Harrison has stood by Snowden during his transit from Hong Kong, China, to Moscow, Russia. Not much is known about Harrison's background, and much of the information that is available is unconfirmed. In an article in *Vogue* is written that she has attended a private school in Kent and has subsequently studied at a university in London and has traveled the globe. In 2008, Harrison did an internship as a researcher at the Center for Investigative Journalism, where she met WikiLeaks' Julian Assange. Soon after, she started verifying documents and writing reports for WikiLeaks (Corbett, par. 2). On her WikiLeaks profile she is described as a journalist and legal researcher who works on WikiLeaks' Legal Defence team ("Profile: Sarah Harrison"). When Snowden had to flee out of Hong Kong, Assange arranged for Harrison to help him. Together, they have stayed at the airport of Moscow for 39 days, until Snowden was granted asylum in Russia. After staying with Snowden for a couple of months, Harrison moved to Berlin and has resided there since (Corbett, par. 6). Like Poitras, Harrison does not seek much publicity. And like Poitras, this does not mean that she is not very active professionally or does not receive much attention. Harrison is currently still working for WikiLeaks and has dedicated herself to the legal defense of whistleblowers through The Courage Foundation.

Appelbaum, Greenwald, Harrison, and Poitras share involvement in quite a large number of organizations and initiatives. They are for example active in advisory boards, share presentations and publications, and participate in art projects. Initially, after the first publications, Snowden stayed in the background, but through public speeches and the acceptance of various awards he now increasingly seems to fulfill qualities of a movement leader. That these individuals can be marked as leaders of the privacy movement does not detract from the fact that there are a number of technologists, whistleblowers, journalists, and politicians who are also very active and influential in the movement, and perhaps also show qualities of leaders. However, Appelbaum, Greenwald, Harrison, and Poitras are the individuals who have been in the public eye the most after the Snowden revelations and who form a clear reflection of the diversity of the group that is concerned with these issues.

Because of the technological advances that have helped society enter the digital age it may seem as if the discussion is solely limited to a technological aspect. In a personal interview Appelbaum explains that this is not completely true: the digital is not a new space but rather an augmentation on the old instead. Technology is merely an addition to a broader discussion of which its core pertains to notions such as human rights and social justice (Appelbaum). In order to explain the necessity of privacy, Glenn Greenwald refers in *No Place To Hide. Edward Snowden, the NSA, and the U.S. Surveillance State* to the 1928 court case of Olmstead v. United States, in which the wiretapping of private telephone calls was under review. He quotes Court Justice Louis Brandeis' statements on privacy, who uses the constitution to explain the importance of privacy:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone – the most comprehensive of rights and the right most valued by a free people. (172)

In an interview conducted after speaking to the European Parliament about the NSA's surveillance activities, Appelbaum refers to the same principles of privacy, dignity, confidentiality, and integrity. He remarks that he finds a situation in which citizens have to ask for these rights unjust, "[...] when you ask someone for those things, they may not grant them and then you will know you are not free" (Gutbub).

Leadership in the Privacy Movement

The right to privacy was established in Article 12 of the Universal Declaration of Human rights in 1948, a moment Annie Machon calls a "highpoint in civilization" in her lecture *The War on Concepts*. The United Nations Human Rights Council has recently released a report on the promotion and protection of the right to freedom of opinion and expression. This report, too, refers to a number of "universal and regional human rights instruments" in which the right to privacy and freedom of opinion and expression has been laid down (United Nations 6). It specifically mentions Article 1 of the Universal Declaration of Human rights, which "recognizes that everyone is endowed with reason and conscience" (8). This article is further developed in other human rights laws and includes "the protection of opinion, expression, belief, and thought" (8). The report also mentions Article 19 of the International Covenant on Civil and Political Rights, which is based on the Universal Declaration of Human Rights and states that "everyone shall have the right to hold opinions without interference" (8). Although opinion and expression are two closely related terms, there is a larger emphasis on the right to hold an opinion. While drafting the International Covenant on Civil and Political Rights this right was deemed as a "fundamental element of human dignity and democratic self-governance" that could not be interfered, limited, or restricted (8).

The privacy movement finds that the relation between government and its citizens becomes asymmetrical when these laws are infringed upon and citizens are denied basic human rights. In an interview conducted shortly after the publications of the first documents leaked by Edward Snowden, Glenn Greenwald spoke about the Total Information Awareness program that was run by the United States government for a short period in 2003. Although officially terminated after four months, Greenwald remarks that he feels it is exactly what the NSA is aiming for: creating a global total information awareness system (Gutbub). With government surveillance programs, citizens are denied the (online) privacy and anonymity that governments do enjoy themselves. The level of secrecy the NSA maintains is generally condemned within the movement. This is often illustrated by the questioning of former NSA Director Keith Alexander by Congressman Hank Johnson. In early 2012 Alexander appeared in front of the United States Congress and was asked questions such as if the NSA routinely intercepted American citizen's emails, if the NSA intercepted American citizen's cellphone conversations, and if the NSA intercepted text messages and Google searches. At the time Alexander denied each of these claims (Gutbub). When the release of the Snowden documents confirmed suspicion that Alexander had not told the truth in front of Congress, it was received with outrage. Greenwald denounces the level of secrecy that goes with the United States intelligence agency's programs, calling it a "secretive" and "shadowy world" of which is unclear how much money is spent on it, how many employees it has, and how many programs actually exist (Greenwald 171).

While debating these issues, there are three elements that often recur and cover the essence of privacy and surveillance related discussions. One of those recurring elements is the comparison to philosopher Jeremy Bentham's Panopticon. Bentham invented the Panopticon in the late 18th century and believed that the structure allows "institutions to effectively control human behavior" (Greenwald 175). The structure consisted of a "large central tower from which every room, - or cell, or classroom, or ward – could be monitored at any time by guards" (175). Although the guard was able to see all prisoners, prisoners could not be sure whether they were or were not being watched and by whom. It is, of course, highly unlikely that it is possible to surveil all inhabitants at the same time. That does not pose a problem, because the structure does not allow inhabitants to know if they are being surveilled and therefore an inspector will always be present in the minds of the inhabitants (175). "Control through surveillance", as Appelbaum puts it in *Cypherpunks: Freedom and the Future of the Internet* (Assange et al. 34). In *No Place To Hide. Edward Snowden, the NSA, and the U.S. Surveillance State*, Greenwald compares the Panopticon to the NSA's current surveillance activities: although the NSA does not have enough capacity to listen in on every conversation, spoken or written, the possibility is always present (175). Therefore, citizens can never be sure if they are being surveilled and by whom.

The second element is the comparison to George Orwell's novel *1984*. In *1984*, Winston Smith lives in Oceania, a nation controlled by The Party. The Party, led by a figure called Big Brother, forbids free thought and expressions of individuality. One of The Party's aims is to implement a language that does not know words related to civil protest, so that dissenting thoughts will no longer be able to exist. A secret police, the Thought Police, oversees that all rules are obeyed. In Oceania, people have telescreens in their homes that are able to both broadcast propaganda and surveil people in their private domain. The view that Orwell's warning from 1949 has come true seems interwoven into the privacy movement's discourse. In an introduction film of CryptoParty Berlin, an organization hosting gatherings to have discussions about and assist with online anonymity, an actor that is meant to represent Orwell ironically mentions that us noobs[3] have used *1984* as an instruction manual (Gutbub). Snowden took a more serious tone in his 2013 Alternative Christmas Message on the British Channel 4. He stated the following:

> Great Britain's George Orwell warned us of the danger of this kind of information. The types of collection in the book – microphones and video cameras, TVs that watch us – are nothing compared to what we have available today. We have sensors in our pockets that track us everywhere we go. (Channel 4)

Glenn Greenwald endorses this statement. He too sees the similarities between our and Winston Smith's society, which both "rely on the existence of a technological system with the capacity to monitor every citizen's actions and words" (Greenwald 174). Greenwald explains that people who are being watched will instinctively adjust their behavior to what they feel is desired of them (176). In addition, in the United Nations Human Rights Council's report is mentioned that with the right to freedom of expression comes the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice" (United Nations 9). In *The War on Concepts* Machon agrees with the report, claiming that a recent report shows that 28

[3] A noob is someone "who is inexperienced in a particular sphere or activity, especially in computing or programming"("Noob").

percent of the people in the United Kingdom censors what they write, what they read, what they watch, and what they communicate. If citizens stop being fully informed, Machon believes this can easily lead to a totalitarian state.

The issue of self-censorship is tied to the third element: the "having nothing to hide" argument. Privacy activists generally do not agree to the idea that when an individual does not do anything wrong, they have nothing to hide. In their view, everybody has something to hide, whether this is their bank account details, the password of their Facebook account, the content of their emails, or the subject of last night's Google search (Gutbub). Two views here are exact opposites of each other. Greenwald quotes a striking statement by the executive chairman of Google, Eric Schmidt:

> If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place. (170)

In other words; if you have something to hide you are doing something you are not supposed to do, and if you are not doing anything you are not supposed to you have nothing to hide. This is at odds with the opinion the privacy movement generally holds. In a recent discussion on *Reddit*, Snowden summarized the essence of the discussion in the following quotation:

> Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say. (SuddenlySnowden)

Moreover, Snowden claims that everybody can fall under suspicion at some point, even if it is just by mistake (Gutbub). Or, as artist and researcher Addie Wagenknecht states in the lecture *Art and Hacking in the Post-Snowden Age*, "anyone can become a dissident with a few clicks". When this happens the system can be used "to go back in time and scrutinize every decision you have ever made [and] every friend you have ever discussed something with and attack you on that basis [...] and paint anyone in the context of a wrongdoer" according to Snowden (Gutbub).

Even when an individual's behavior may (eventually) not fall under suspicion, privacy is still essential to and instinctively understood by individuals, according to Greenwald. When people imagine they are in a private sphere, they will "say things to friends, psychologists, and lawyers that they do not want anyone else to know" (Greenwald 171). The content of their thoughts, fears, and desires, whether expressed on- or offline, is not always something people like to have linked to their person. It is only when people feel unwatched that they feel free to explore and express new thoughts, ideas, boundaries, and dissent. Once, the Internet was the perfect place for these kinds of anonymous experiments to take place (Greenwald 174). The report of the United Nations Human Rights Council is of the opinion that it should stay that way, and finds that "individuals enjoy the same rights online that they enjoy offline" (United Nations 9). It therefore attaches great value to encryption and online anonymity, which provides the privacy needed for holding opinions and exercising freedom of expression "without arbitrary and unlawful interference or attacks" (7).

What the privacy movement is aiming for is a counter-revolution. In a personal interview with Appelbaum in Berlin, he explains that, in contrast to what is oftentimes assumed, whistleblowers such as Edward Snowden and Julian Assange should not be seen as revolutionists. Instead, President Bush and former NSA director Keith Alexander are the revolutionists, since they created a major turn with their security policy after the terrorist attacks on 9/11. What the movement now asks for is the return of a situation that has already existed, to observe human rights that have already been obtained. Therefore it should be viewed as a counter-revolution rather than a revolution, says Appelbaum (Appelbaum). Whether obtaining the goal of a free and open Internet needs to come through policy change or technological solutions is not always clear and will depend on who is asked. The opinion of American research journalist Leif Ryge seems to be representative for a larger group: both law and technology need to be altered, although technical solutions are more promising (Ryge). Annie Machon also believes in the combination of policy change and technological solutions. In *The War on Concepts* she asks the audience to go through the democratic system to accomplish policy change. In addition, she also encourages the audience to take the responsibility for privacy in their own hands through the use of technological solutions such as open source software, strong encryption, and the Tor Project[4]. Moreover, in *Putting the "Revolution" back in Internet Revolution: Programmers and Social Movements*,

[4] When an Internet user makes use of the Tor browser, its computer connects to the website via a number of intermediate servers instead of connecting to its destination directly. This process hides the identity of the Internet user.

Appelbaum states that old structures need to be used for new structures and stresses the importance of organization. He states that old structures need to be used for new structures. If we want to regain our basic human rights, Appelbaum argues, we need to organize like in the 1960s: the use of technological solutions will be entirely useless if people are not in contact with each other.

The privacy movement as a whole defends the right to (online) privacy and aims for a counter-revolution to restore the human rights that are currently infringed upon. Within the movement, a small group of individuals, consisting of Appelbaum, Greenwald, Harrison, and Poitras, has started to fulfill the role of movement leaders. Their leadership is important to the privacy movement, as the links they form among activists and organizations contribute to the process of a decentralized movement forming a whole. Moreover, it increases the movement's significance because the links they form in their turn contribute to a social network through which new members become involved.

Chapter 5
Where the Privacy Movement Meets: Berlin

Where the Privacy Movement Meets: Berlin

> In 2006, I was placed on a secret watchlist after making a film about the Iraq War. In the following years I was detained and interrogated at the US border dozens of times. (…) I move to Berlin to protect my film footage from being seized at the US border. When the first emails arrive, I increase security. (*CITIZENFOUR*)

The German capital Berlin is a significant place for the privacy movement. It is a safe haven for Appelbaum and Harrison, and has been a place where Poitras could work on *CITIZENFOUR* relatively undisturbed. But Berlin is also a vibrant city with a lively digital culture and rich history that creates a favorable atmosphere where privacy activists gather. Considering the fact that digital times may create the assumption that real life contact has largely become redundant, this is an interesting given. This chapter will explain the importance of physical meeting places in a time where all contact can take place online, and it will explore why Berlin, instead of another city, proves to be such a place for the privacy movement.

Even though it is tempting to assume that real life contact has become redundant for a movement that is in essence so intertwined with technology and the Internet, real life contact still remains necessary. The Internet can have a reinforcing effect on movements, according to Della Porta and Diani. It can maintain networks of which the participants are scattered over different locations and it can help to develop "cultural and socio-spatial enclaves" (Della Porta and Diani 133). In addition, the Internet enables communities to connect that would perhaps otherwise not be able to because of their geographical locations (133). Online interaction, however, lacks a number of elements that real contact does have, such as regular participation, a basis to build mutual trust and commitment, and a discussion between a substantial number of individuals. Moreover, participants in online discussions often hide their identities. Although hidden identities and online anonymity can be ways in itself to challenge power, it seems that "virtual networks operate at their best when they are backed by real social linkages" (133).

The presence of real social linkages influences movements in a number of ways. First, when individuals know each other in real life and have the opportunity to regularly meet, like the privacy movement has in Berlin, it helps to shape a collective identity within a movement. Sebastian Haunss and Darcy K. Leach explain this in their paper "Scenes and Social Movements" through movement scenes. Haunss and Leach observe that the space in which new social movements act is situated between "the public and private spheres" and that it is "political, but non-institutional" (Haunss and Leach 2). This is where movement scenes come into being. Scenes are not the same as social movements, subcultures, or countercultures, but are rather situated at a crossroads where the three influence each other. The exact relation between social movements and scenes is specific to each individual movement (11). Haunss and Leach claim that movement scenes are a crucial factor in developing the collective identity that Della Porta and Diani deem important for a social movement, since scenes are places where links between "lifestyles" and "collective action" can come into being (21). This is particularly important for movements that strive for social change, because the building blocks they create by developing "commitment frames" are central to "processes of collective identity" and are integrated in "different spheres of the activists' lives" (21). When these collective identity processes cross paths with the lifestyles of a scene, a situation can arise that secures the movement's existence in between protests (21). Although a movement scene relies on a network of people who share certain values and ideas, it can also not exist without a certain location where its members can meet and share experiences (3). Visiting physical spaces and venues helps informal social networks to form "subcultural oppositional dynamics", which in turn helps to maintain a collective identity (Della Porta and Diani 131). Della Porta and Diani mention that this can provide the structure for social movement free spaces, which they define as "areas of social interaction in which holders of specific worldviews reinforce solidarity and experiment with alternative lifestyles" (131). As individuals share their culture and lifestyle, meeting each other in free spaces brings forth scenes (Haunss and Leach 3). Locations allow scene members to "physically experience" their membership in, for example, "bars, clubs, parks, street corners, [and] parts of town" (5). Knowing what these locations are can in itself be a sign of membership (5).

Although a collective identity is created when individuals participate in various organizations and maintain contact with other activists, this does not lead to a fixed identity but rather to one that is variable, flexible, and different for each individual activist (Della Porta and Diani 131). Haunss and Leach notice a similar flexibility within movement scenes. While they acknowledge the existence of a central group of leaders, at the same time they notice that it is not very clear-cut when someone belongs to a movement's core or periphery or when someone is a member and when someone is not. The form of a movement scene, for example its ideas or codes of conduct, can change at any moment and therefore it is difficult to know what defines the membership criteria (5). Just like a collective identity does not automatically lead to a fixed and stabile movement structure, it also does not lead to a homogeneous idea of collective action, and this can cause a difference in position between the movement as a whole and the scene (19). For the privacy movement this becomes for example apparent in the way in which activists view outsiders. Some groups within the movement are very open to interaction with outsiders, value cooperation with different disciplines, and are dedicated to drawing attention to their cause. In contrast, there are also groups within the movement that can be called closed. These groups prefer not to be involved in research and sometimes reject individuals who are not part of their network.

A second effect of having social linkages is that it enables a movement to act quickly when a political situation requires immediate action. When necessary, a large group of people can be reached, for example by distributing flyers and posters, and these people can then easily access information about the movement (13). This happened for example when a number of street demonstrations were organized almost immediately after the first publication of the Snowden documents appeared.

Appelbaum explains in a personal interview that within the privacy movement, too, there is still a need for "real" contact. He stresses that the physical and the digital are not separated and that it is still necessary to have "reflection points for action" (Appelbaum). Another advantage the physical has over the virtual that Appelbaum mentions is specifically tied to the privacy movement; conducting surveillance is more difficult and less common in the physical world (Appelbaum). Privacy activists are usually deeply concerned with issues of surveillance and privacy in general and are extremely aware of governments' capabilities to intercept communication. Moreover, some individuals have valid reasons to assume they have drawn the specific attention of intelligence agencies. It is much easier to perform surveillance in the online world than in the offline world, and that hampers activists in their free online communication. Therefore, a physical place to meet is perhaps even more valuable for the privacy movement than for other groups.

Previous sections have explained the significance of physical meeting places for a social movement. The reason that Berlin turns out to be that place for the privacy movement is twofold: Berlin's recent history still influences German's attitude towards privacy and surveillance, and it has a vibrant digital culture. With regard to Germany's history, there are two factors that make Berlin attractive for privacy activists: the German Constitution and its history with the GDR. Germany's Constitution origins from 1949 and the current version is a modified version of the West Germany's Constitution before the country was reunited in 1990. The Constitution was composed with Germany's history in mind; the foreign nations that occupied Germany at the time were closely associated with the drafting and took great care to shield the country from a recurrence of the fragmented Weimar Republic democracy or the totalitarianism of the 1930s and 1940s ("Constitutional History"). Whistleblower and part-time Berliner Annie Machon explains that the Constitution was one of the initial reasons she chose Berlin as her (part-time) residence (Machon). *The Guardian*, too, assigns certain significance to German law. In an article from 2014, called "Berlin's digital exiles: where tech activists go to escape the NSA", the newspaper claims "Germany has some of the strongest laws in the world when it comes to surveillance and privacy" (Cadwalladr, par. 20).

Regarding the Constitution, a number of articles in particular are worth highlighting. The Constitution starts by stressing the importance of human rights and human dignity, deeming them "inviolable and inalienable" (15). Article two addresses personal freedoms and states that every individual should have the freedom to develop oneself as long as it does not harm the rights of others or the law (15). Although it is not explicitly mentioned in the article, this does pertain to the notion of privacy. As explained in chapter four, Greenwald, Appelbaum, and the United Nations Human Rights Council argue that privacy is essential in order for people to feel comfortable enough to explore and express their thoughts, ideas, and desires and thus to freely develop their own personality. In 1983, this article received an additional protection ("Privacy Laws"). When the German government initiated to "conduct a general population census", citizens were apprehensive and feared that the census would invade their privacy (Hornung 84). After extensive debate the census was terminated and the Federal Constitutional Court of Germany established a new basic right: the right of informational self-determination. Today, it still influences decisions regarding data protection (Hornung 85). In addition to the right of Article 2 to freely develop a personality, Article 5 protects the formation of a well-informed opinion and the freedom to express that opinion. It states that "every person shall have the right freely to express and disseminate his opinions in speech, writing and pictures, and to inform himself without hindrance from generally accessible sources" (16). In addition to the value that is attached to the development of citizen's personality and the freedom of speech, Article 10 describes another right the privacy movement values, namely the right to private communications. It focuses on the privacy of correspondence, posts, and telecommunications and has two relevant sections. Section one of this article states that "the privacy of correspondence, post and telecommunications shall be inviolable" (18). Section two specifies rigid restrictions the law imposes on the state that make it difficult to conduct surveillance on citizens. In 2013, the Directorate-General for Internal Policies of the European Parliament published a study called "National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility With EU Law". In this study, Article 10 is explicitly highlighted and is connected to the G-10 Law, which is Germany's "main federal law regulating communications surveillance" (European Parliament). The G-10 law is double-edged: on the one hand it limits "the secrecy of communications" according to Article 10, on the other hand it allows intelligence services to wiretap domestic and international communications in order to fight terrorism or protect the Constitution and to "search up to 20% of foreign communications according to certain keywords [including] telephone conversations, e-mails, and chats" (European Parliament). However, the German Federal Constitutional Court has also put limitations on the Law. In 2008 it declared North Rhine Westphalia's regional law that allowed the secret gathering of data on "private computers" unconstitutional (European Parliament). The Court appealed to Article 1 and 2 of the Constitution, deciding that it is a fundamental right for citizens for their state to respect the "integrity and confidentiality of [their] IT systems" (European Parliament). Although the secret searches were not entirely forbidden, the Court did set up a number of restraining conditions (European Parliament). The exploration of these articles and laws is certainly not meant to be exhaustive, but rather to give an idea of why the German Constitution's articles related to privacy can be a reason for privacy activists to come to Germany.

Germany, and Berlin in particular, has quite a unique and turbulent history that still influences citizens' attitude towards privacy and surveillance today. World War Two left Germany divided. In 1949, four years after the war had ended, Germany was definitively split up into four zones: the British, American, and French zone formed the Federal Republic of Germany in the West, while the Soviet Union established the Democratic Republic of Germany, the GDR, in the East ("East Germany Created"). Similar to the rest of the country, Berlin too was divided into a British, American, French, and Soviet zone ("Berlin is Divided"). Life in the German Democratic Republic did not offer much perspective for its citizens. In the years between 1949 and 1961, between 2.5 million and 3 million East-Germans fled to the West, hoping for a better future. With the rest of the country already fenced off, Berlin was one of the few options to escape from the East to the West. The GDR could not afford to lose such large numbers of workers, and decided to interfere. In the night of August 12 to 13, 1961, soldiers sealed off the border between the East and the West with barbed wire: the beginning of the Berlin Wall. This would later be replaced with a "six-foot-high, 96-mile-long wall of concrete blocks, complete with guard towers, machine gun posts and search lights" ("Berlin is Divided"). Many years later, after severe protests, the border between East and West was opened and the wall was torn down on the evening of November 9, 1989 ("Berlin is Divided").

One of the aspects that made life unpleasant in the GDR was the surveillance apparatus the then ruling Socialist Unity Party of Germany, the GED, had in place. A comparison between the GED's means of surveillance and the present day government surveillance is easily made. Surveillance in Germany started with the People's Police, that had Kommissariat 5, which was an "unseen controlling level [...] that had nothing to do with conventional crime fighting" (Schmeidel 5). Chapter three mentioned that politicians often use war metaphors to legitimatize policy, because people who experience feelings of fear tend to avoid risk and accept government measures more easily. This technique was also used when the Ministry for State Security, often abbreviated to Stasi, was established in 1950. The establishment of the Stasi was announced by the daily newspaper of the party, which took a small event of infiltration by saboteurs out of its context and blew it up to "an alarming picture of terrorism, including whole factories blown sky high, and unfettered espionage upon the territory of the newly proclaimed [GDR]" (Schmeidel 5). The GED continued to use this technique throughout the GDR's existence, continually spreading alarming messages of how the GDR's existence was threatened by the enemy in the West and how the West was responsible for the failure of the GDR's economy. Moreover, "critical opinions, unconventional lifestyles and oppositional conduct within the population were regarded as hostile-negative manifestations controlled by Western manipulators" (DDR Museum).

Responsible for Western espionage, domestic surveillance, and the suppression of opposition, the Stasi grew rapidly. In 1989 it had 93,000 full-time employees (DDR Museum). These employees were recruited through targeted searches and they, as well as their families, were thoroughly screened. Having any sort of relation with people in the West was not allowed, while supporting the GED and the Soviet Union unconditionally was mandatory (Stasi Museum). Materialistically seen, it was rewarding to work for the Stasi: its employees received an above-average salary, could move into one of the Stasi's 18,000 flats, and could spend their free time in one of the 300 recreation centers. This resulted in satisfied employees, but most beneficial for the Stasi was that the employees kept each other in check (Stasi Museum). The Stasi did not only have official employees, but also a large network of informants. Some GDR citizens were willing, but others were forced to work as unofficial collaborators for the Stasi. They were forced to sign a declaration of commitment and had to personally report on friends, neighbors, and colleagues (DDR Museum). During the 40 years the Stasi existed, approximately 250,000 people were convicted (DDR Museum).

The way in which the party surveilled its citizens shows similarities to the ways in which modern day intelligence agencies do. The control the party exercised started at a young age for East Germans, with Kundi. Kundi was "a dwarf with jug ears and a blue hat that was on hand to help children grow up as clean and tidy citizens" (DDR Museum). The way in which Kundi kept an eye on children is reminiscent of a Panopticon:

it had a magic telescope that enabled him to see whether children had obeyed him. Surveillance was also conducted through infiltration, by for example disguising as a tourist or infiltrating in certain events, or by tapping telephone conversations. Furthermore, one of the most valuable ways of surveillance for the Stasi was the control of the mail system, like the intelligence services nowadays collect data from e-mail traffic (Schmeidel 21). Letters were "steamed open, photographed and resealed" (23). This could happen at random, in order to identify individuals who perhaps misbehaved, or sometimes as part of an investigation as simple as a "routine security clearance" (21). The Stasi also followed specific individuals, sometimes thus by inspecting their mail. Employees of the postal service were then instructed to open and sometimes hold back mail that came from or was sent to specific addresses (22). Sometimes, if a suspect were already under permanent personal surveillance, Stasi employees would dress in postal uniforms and collect the mail from the mailbox the suspect had just dropped his mail in. This was called "special collection" (23). All information the Stasi gathered was stored in card file indexes. One index, the F 16, was used for information about individuals and contained their real name and accompanying registration number. Another index, the F 22, stored information about the reason the Stasi followed an individual (Stasi Museum). This kind of surveillance was also conducted on Stasi employees: the Main Department for Cadre and Training collected and documented extensive information on their private lives and professional careers (Stasi Museum). This storage of data is reminiscent of the ways in which modern intelligence agencies store data. The NSA, for example, has a storage facility in Utah, which is estimated to be able to “hold zettabytes (1,000,000,000,000,000,000,000 bytes) of information” (Bamford, par. 49)

Thus, that the data collection of the current intelligence services evokes strong emotions in a city like Berlin makes sense given its history: Germans still remember what it feels like to be under surveillance. Although not exactly similar, it is possible to see the similarities between the way data is currently collected and stored by intelligence agencies and the way it was done in the GDR. Not long after the disclosure of the Snowden documents, German author and journalist Jan Fleischhauwer explains in *Der Spiegel* that surveillance is still a much more sensitive subject for German citizens than for, for example, United States citizens. While Americans in general have no problem with giving up privacy in return for security, Germans “are more than happy to consign their children to state care [...] but would go through hell and high water to keep their personal information out of state hands”, as Fleischhauwer describes it (par. 5). As a reason for this, Fleischhauwer points to Germany’s experience with “two dictatorships – one with a Gestapo, the other with a Stasi” (par. 8). In *Exberliner*, a monthly magazine for expats in Berlin, head of the Stasi prison memorial Hubertus Knabe explains that he finds it important to also shed light on the difference between the Stasi and modern intelligence services. Although today’s surveillance methods show a strong resemblance to those of the Stasi, their aims are different. Where the Stasi tried to create fear, intelligence services nowadays claim to try to protect citizens, according to Knabe (Wilde 20). Also important to note is that Germany’s recent experiences with surveillance do not mean that the effects of surveillance are different on Germans than on others, but merely that Germans in general are more aware of the effects of surveillance.

> Berlin has an incredible culture of resistance. I have been coming to Berlin for many years because of the Chaos Computer Club, and I've worked with *Der Spiegel* in the context of WikiLeaks. I have a lot of close friends here in the art world and in the computer hacker world and in the journalistic world. [...] We often joke that it's this sort of last stand for democracy. Where people are really having real dialogues. (10)

This quotation from an interview *Exberliner*'s Schneider held with Appelbaum captures second reason why Berlin is popular among digital activists. In addition to the city's history and culture of resistance, activists are also drawn by the large number of organizations and initiatives Berlin has, as well as by the presence of other activists. This seems to form a circle, in which each element has a reinforcing effect on the other elements. The presence of organizations and initiatives concerned with digital themes attracts activists, but the presence of these activists also attracts new activists and helps to establish new organizations and initiatives. A digital culture then arises, which in its turn also reinforces the number of organizations, initiatives, and activists. What the digital culture brings forth is at the same time what creates the digital culture.

One of the most influential organizations in Berlin is the Chaos Computer Club. Active since the early 1980s, this hackers association is currently the largest of Europe. The CCC organizes several events, such as the four-yearly Chaos

Communication Camp, the annual Chaos Communication Congress, and the monthly Datengarten ("Events"). The CCC also has its clubhouse in Berlin: Club Discordia. That these events draw (h)activists to Berlin is confirmed by Leif Ryge in a personal interview. He is originally from the United States and explained that, like others, he, too, first came to Berlin because of the CCC and later decided to stay (Ryge). Berlin also has many spaces, both large and small, where hackers and digital activists gather. One of the larger spaces is c-base, founded in 1995 and designed to resemble a "crashed space station in the center of Berlin" ("c-base"). C-base often organizes workshops, seminars, exhibits, presentations, and parties through which it tries to create new ideas and enhance communication between different groups ("c-base Official Handout"). The existence of these initiatives has also brought about new initiatives and organizations. One of these initiatives is, for example, the CryptoParty. Originated in Australia in 2012, the CryptoParty is now a global initiative held in many countries around the world where technologists discuss and teach privacy enhancing tools to those whose technical expertise is a bit more limited. Berlin belongs to the cities in which these parties are held most often: there are usually multiple parties held each week ("What is CryptoParty?"). A new organization that has its roots in Berlin is, for example, The Courage Foundation. Founded by WikiLeaks' Sarah Harrison, this foundation works to support the protection of whistleblowers.

> If you want to know what's really going on, you don't read the newspapers, you read the streets. Literally. Someone who arrives in Berlin for the first time, even if they don't know a single person,

> can find entry into the political scene simply by reading the posters and graffiti that cover the walls, overpasses, and telephone poles all over town. Posters especially convey all kinds of political information, announcing protest actions, meetings, informational events, the formation of new groups, and social events like street festivals, parties, and concerts. (14)

These initiatives, together with many others, have created a vibrant digital culture that is apparent throughout the entire city. Like the above quotation of Haunss and Leach suggests, the streets of Berlin are filled with political messages. Figure 2 shows an example of this: the Netzpolitik stickers can be found all over Berlin.

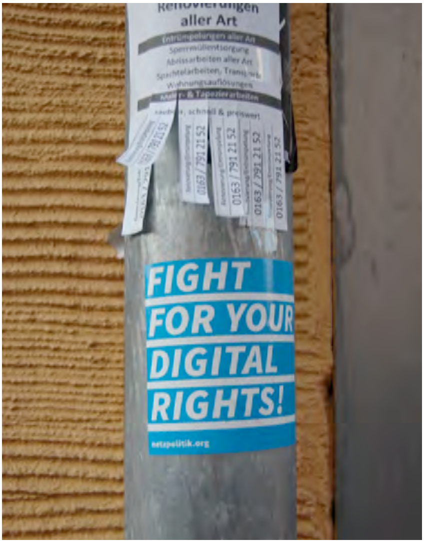


Fig. 2. A Netzpolitik sticker on a downspout in Berlin (Loes Derks van de Ven).

While expressions of political opinions are not limited to certain parts of the city, the former Eastern part of Berlin has definitely been fertile breeding ground for these initiatives. Haunss and Leach explain that this has a historical cause: after the wall fell it was very cheap, if not free, to rent living space in the East. This resulted in a “strong radical leftist presence” in the neighborhoods of East Berlin (Haunss and Leach 16). The presence of this culture, and thus all these possibilities to meet, has lead to a community that is has a shared culture and that maintains close social contact (13). The presence of a strong digital culture in Berlin has lead to the presence of a large group of activists, which gives them the opportunity to not only meet at political events, but also at social events (13). These social events are an opportunity to quickly exchange information about, for example “political campaigns and first-hand accounts of protest actions” (13). With this, politics and culture become entangled and that creates a fertile situation for both the movement and the locations where those events take place. When activists visit social events they will likely come into contact with people who do not belong to the core of their movement in a relaxed and informal way, which allows a relationship to develop naturally. The positive feelings that the contact evokes are then linked to both the location and the movement (13). This process is, naturally, not limited to Berlin. Haunss and Leach explain that scenes are not local: networks, communication systems, and other processes can overlap and can cause similarities between several places. When members of the larger scene share this experience in different places, it can have a positive effect on the activists’ solidarity (23).

Where the Privacy Movement Meets: Berlin

Places where activists can meet face-to-face and thereby form real social linkages are important to social movements in general and the privacy movement in particular, despite the opportunities the Internet has to offer. A movement scene such as Berlin, with its many events and organizations, gives privacy activists a place to form a flexible collective identity. The reason why this process works well in Berlin is because of both its history and active digital culture. The privacy-conscious en digitally fertile climate of Berlin attracts activists, which in turn attracts more activists and which eventually allows the digital culture to grow.

Chapter 6

The Privacy Movement and Dissent: Whistleblowing

The Privacy Movement and Dissent: Whistleblowing

This is the first of three chapters that will together form a case study of the ways in which the privacy movement expresses dissent. Whistleblowing is a suitable expression of dissent to begin the second part of this thesis with: whistleblowing in itself is not protest, but it does lay a foundation for protests and is at the same time also closely related to it. Moreover, it is also a way of expressing dissent that is specifically tied to the privacy movement. Information regarding the subjects that privacy activists work on is not always publicly available. The information whistleblowers reveal is thus an important source of information for the activists. Whistleblowers can therefore count on protection by members and organizations within the movement. At the same time these whistleblowers often also become active in the movement themselves at a certain point, joining it in its other expressions of dissent and helping to protect other whistleblowers. This chapter will explain how whistleblowing, and particularly Edward Snowden's whistleblowing, can be understood as an expression of dissent and what role whistleblowing plays within the privacy movement.

Whistleblowing is related to three different terms: dissent, civil disobedience, and protest. Although the term whistleblowing is relatively new, dating back to the 1950s, the history of the act of whistleblowing goes back much further, presumably to pamphlet writers of the eighteenth century (Jubb 77). In "Whistleblowing: A Restrictive Definition and Interpretation", Peter B. Jubb gives a clear account of what whistleblowing is and how it should be interpreted as a form of dissent. Studying a number of other researchers' definitions of whistleblowing has led Jubb to one definition that entails the most relevant elements of whistleblowing:

> Whistleblowing is a deliberate non-obligatory act of disclosure, which gets onto public record and is made by a person who has or had privileged access to data or information of an organization, about non-trivial illegality or other wrongdoing whether actual, suspected or anticipated which implicates and is under the control of that organization, to an external entity having potential to rectify the wrongdoing. (78)

Jubb emphasizes that a whistleblower always deliberately discloses the information and has always intended to make the information public, and that a whistleblower seeks an unconventional way to release information because conventional paths within the organization turned out to be a dead end (79). Whistleblowing is different from other forms of informing Jubb claims, because it is not just the release of information but at the same time also an “indictment” that “identifies wrongdoing” and that challenges a person or an organization (79). If it is an individual who is challenged, it is always someone in a higher function than the whistleblower: a whistleblower cannot change what he or she finds unacceptable, but can “empower lesser individuals with respect to their concerns” (79). Although whistleblowing functions as a control instrument and is usually done out of concern for the public interest, whistleblowers are still often associated with negative images of “sneaks, spies, squealers, and other despised forms of informer[s]” (77-78).

The elements of disagreement and complaint are what characterize whistleblowing as an expression of dissent. Jubb explains this through Hirschman’s response categories: exit, loyalty, and voice. Where the exit response means that an individual chooses to dissociate oneself from the problem and the loyalty response means that an individual will remain loyal to the organization despite of its wrongdoings, the voice response means that an individual chooses to express their "concern or disagreement" (79). The disagreement becomes dissent when it is expressed and has led to a complaint. This comes in many different shapes and forms, and can vary from "negative body language [to] documented and publicized statements" (79). Whistleblowing is the most "direct" and "unambiguous" variant. It has a clear aim to enforce a change within an organization and is often done because of ethical considerations, but never under threat or under oath (79).

In addition to dissent, whistleblowing can also be seen as civil disobedience, especially when zooming in on Snowden's whistleblowing. In "Whistleblowing As Civil Disobedience: The Case of Edward Snowden", William E. Scheuerman claims that the way in which Snowden blew the whistle fully meets the criteria of the following definition of civil disobedience:

> [Civil disobedience is a] public, nonviolent, conscientious yet political act contrary to the law usually done with the aim of bringing about a change in the law or policies of the government. (611)

The following quotation, taken from a statement Snowden made at the airport in Moscow, entails all elements of the previously given definition of civil disobedience.

> (...) I did what I believed right and began a campaign to correct this wrongdoing. I did not seek

> to enrich myself. I did not seek to sell U.S. secrets. I did not partner with any foreign government to guarantee my safety. Instead, I took what I know to the public, so what affects all of us can be discussed by all of us in the light of day, and I asked the world for justice. ("Statement by Edward Snowden")

The aims Snowden tried to achieve by disclosing the documents are politically motivated: he wanted to inform the public about government surveillance activities so that policies could be adjusted as the public wished. By turning to the press he addressed this issue openly, and by addressing this issue openly he took the entire discussion out in the open and thereby turned it into a public discussion (612). What he wanted to achieve with his disclosures and the subsequent public discussion was clear, and the way in which he did this was deliberate and, as the definition describes, conscientious. The above quotation is but one of the many examples that show that Snowden was aware of what he was doing and what his motives were. Furthermore, Scheuerman points out that Snowden meets the criteria of a specific form of civil disobedience, namely indirect disobedience. Indirect disobedience means that the civil disobedient does not breach a law because he or she opposes it, but breaches it to make clear there is another law or policy he or she does oppose ("Civil Disobedience"). By blowing the whistle, Snowden has breached the non-disclosure agreement he had with the United States government because he was convinced that this was the only way to generate attention for what he perceived as wrongdoings of the NSA (Scheuerman 611).

While whistleblowing can be considered as civil disobedience or an expression of dissent, it is not entirely similar to protesting. In "Whistleblowers and Organizational Protesters. Crossing Imaginary Borders", Australian researcher William De Maria studies if there can be some sort of alliance between whistleblowing and protest. By giving definitions of both whistleblowing and protesting, it becomes clear that the two are not the same. De Maria's definition of whistleblowing is nearly similar to the aforementioned definition of Jubb, except that De Maria emphasizes that a whistleblower is a citizen who is concerned with and motivated by the public interest (De Maria 866). Within the definition of protesting, De Maria stresses that protesting, in contradiction to whistleblowing, is something that is done by a group and hardly ever by one single individual. He also points out that mobilization is the most powerful element of protesting, because it is usually the mobilization of "human and non-human resources" that bring organizations wrongdoings to light (867). How whistleblowing and protesting can influence each other is shown through the case of Paul van Buitenen, who worked as an auditor for the European Commission's Financial Control Directorate. When he decided to send a letter and documentation of financial wrongdoings within the commission to the president of the Green Party, an influential protest group, he initiated a powerful collaboration. The Green Party had reached its goal when the president of the European Commission resigned, and Van Buitenen benefited when he changed from a bureaucrat into a "moral campaigner [and] politician" (873-874).

Whistleblowing and protesting do not only influence each other, the two can also have such an overlap that the boundary can become vague. The similarities De Maria mentions include that both whistleblowing and protesting are a “morally propelled action”, involve “personal risk-taking”, are “changed-focused”, are “vulnerable to name calling”, and involve “strategic planning” (874). De Maria also mentions a number of differences, namely that whistleblowers, in comparison to protesters, are more vulnerable to reprisals, do not endorse violence, operate solo, have an intra-organizational focus, have few strategic options and only approach the media as a last resort (874). While these similarities and differences seem to be correct in general, the differences between whistleblowing and protest become smaller when analyzing how Snowden blew the whistle. The similarities remain the same, but the differences do not. Snowden’s actions, for example, already stopped being individual when he contacted Greenwald and Poitras months before he gave them the entire set of documents and the moment of actual publication. Also worth noting is that the use of media was certainly not Snowden’s last resort but rather one of his first choices instead. In a personal interview, Appelbaum explains this was done for a specific reason, namely to create a maximum impact: the more newspapers that cover the story, the more people who will read the story. Directly approaching the media and spreading documents among several media outlets also has another advantage: it reduces the risks for journalists and researchers involved. The more newspapers that publish the story, the more difficult it is for governments to start a procedure against those newspapers. Moreover, Appelbaum also believes that individuals bond with the newspaper they read, and therefore will defend their newspaper when that newspaper is threatened (Appelbaum).

Furthermore, Snowden did not focus on changes within the organization, as whistleblowers do according to De Maria, but focused on changes that entail a complete social and political turn, not just of the NSA but also of a larger group of intelligence agencies and governments. De Maria also argues that whistleblowers "often embrace the corporate direction of their organization [and] seek an improvement, a reform, and some ethical change, without the demise of the system", while protesters "often have fundamental worldview clashes with their targets and often seek radical overhaul, if not their demise" (875). Looking at Snowden, along with other whistleblowers within the privacy movement, this difference between whistleblowers and protesters also seems to disappear. Whistleblowers within the privacy movement do have a different worldview than their opponents and are looking for a fundamental change.

Whistleblowers take up an exceptional place within the privacy movement. They are indispensable sources of information. Part of the developments around privacy and surveillance issues the privacy movement is concerned with is public, for example because policies or certain documents are made public. However, much of what the privacy movement is concerned with is related to the actions of intelligence services of which the exact conduct is not made public. Activists are therefore quite reliant on the information whistleblowers disclose to know what is really happening in the field of surveillance. The importance of whistleblowers is often made clear in public speeches by members of the movement, for example in Annie Machon's speech at the launch event of Code Red. In the 1990s, Machon blew the whistle herself while working as an intelligence officer for the British MI5. She is now the Director of Operations of Code Red. One of the first remarks she makes in her speech is that we live in the era of whistleblowers, and that they are, unfortunately, needed to tell a truth that would otherwise not be known. Later on during the event this statement is endorsed by Anne Roth, a German blogger and Internet activist who has been working for the German Parliamentary Committee investigating the NSA spying scandal. The committee researches the collaboration of the German secret service, the Bundesnachrichtendienst, with the Five Eyes[5] on the topic of surveillance ("Untersuchungsausschuss ("NSA")"). She too claims that both the committee and society as a whole are depending on whistleblowers to provide certain information that would otherwise remain hidden. She explains that the Investigative Committee on Mass Surveillance can only ask the government for information if they know certain things exists. As long as there is a lack of knowledge of the existence of something, no action can be taken.

Once whistleblowers have decided to blow the whistle and make certain classified information public, their position often changes. By blowing the whistle they have excluded themselves from the organization they were previously working for, physically but also mentally. Subsequently, they are often admitted by the privacy movement. There are a number of whistleblowers within

[5] "The Five Eyes alliance is a secretive, global surveillance arrangement of States comprised of the United States National Security Agency (NSA), the United Kingdom's Government Communications Headquarters(GCHQ), Canada's Communications Security Establishment Canada (CSEC), the Australian Signals Directorate (ASD), and New Zealand's Government Communications Security Bureau (GCSB)" ("The Five Eyes").

the privacy movement who set a good example of this. After disclosing information about the MI5, Annie Machon has developed into an intelligence expert, author, and public speaker. She has written a book, is the director of LEAP, a member of the advisory board of the Courage Foundation, and Director of Operations of Code Red ("About"). William Binney was a crypto-mathematician who worked as Technical Director of the World Geopolitical and Military Analysis Reporting Group at the NSA until his resignation in 2001. He undertook several attempts to seek attention for what he perceived as wrongdoings of the NSA ("Bio: William Binney"). In the years after, Binney started to give interviews and public speeches and became a member of, for example, the Advisory Group of Code Red. More recently, Edward Snowden seems to go through a similar development. The first year after his revelations he kept a relatively low profile. Later, Snowden, too, started to accept awards and give public speeches, for example at the Dutch Big Brother Awards; took his first steps in publishing articles, for example in *The New York Times*; and is a member of the Board of Directors of the Freedom of the Press Foundation (Snowden; "About Freedom of the Press Foundation"). De Maria explains that it is indeed a possibility that whistleblowers develop into protesters. Whistleblowing as well as protesting can be "metamorphic": a disclosure can move from internal to external, like protest can also move from internal to external (De Maria 869). When whistleblowers join protest, they then lose their status of an "individualist" operating solo. A whistleblower can also decide to reverse their action and go from collective action back to solo disclosures (869).

Chapter 6

Because whistleblowing can have such drastic consequences, whistleblowers often receive respect and protection by the privacy movement. There is an enormous awareness among privacy advocates of the sacrifices whistleblowers make. Respect for them is often one of the first things mentioned while speaking about this subject. Of the many instances that can be found, three of them set a particularly striking example. In *Surveillance and You*, a lecture at The Eindhoven Institute for the Protection of Systems and Information, Jacob Appelbaum spoke about cryptography and surveillance-related subjects. He opened his talk by mentioning the names of Edward Snowden, Julian Assange, and Sarah Harrison. He first stressed that without them it would not have been possible to speak about this subject and they should be thanked whenever possible. He then continued to thank them, and subsequently put an image of Snowden's head on his stand. He added that Snowden, contrary to what the general public may think, should not be seen as a saint: he looks at humanity instead of to an "interventionist God" to change the state of our current society. While explaining this, he simultaneously expressed his admiration for his deeds: Snowden has done an enormous favor to mankind.

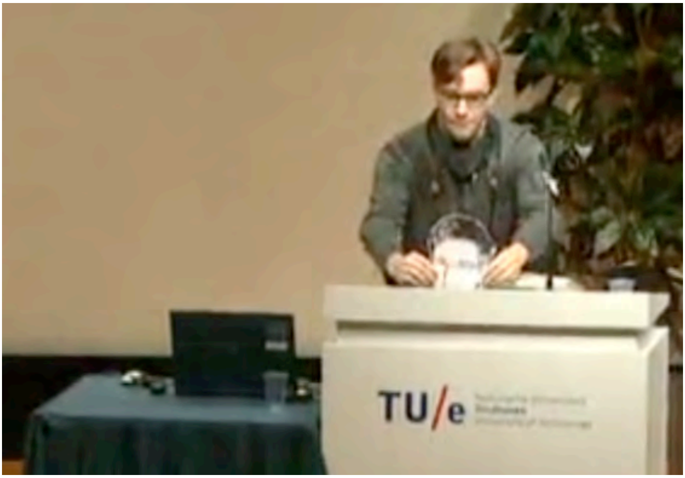


Fig. 3. Still from the video of the lecture at The Eindhoven Institute for the Protection of Systems and Information, Appelbaum places an image of Snowden on his stand. *win.tue.nl*.

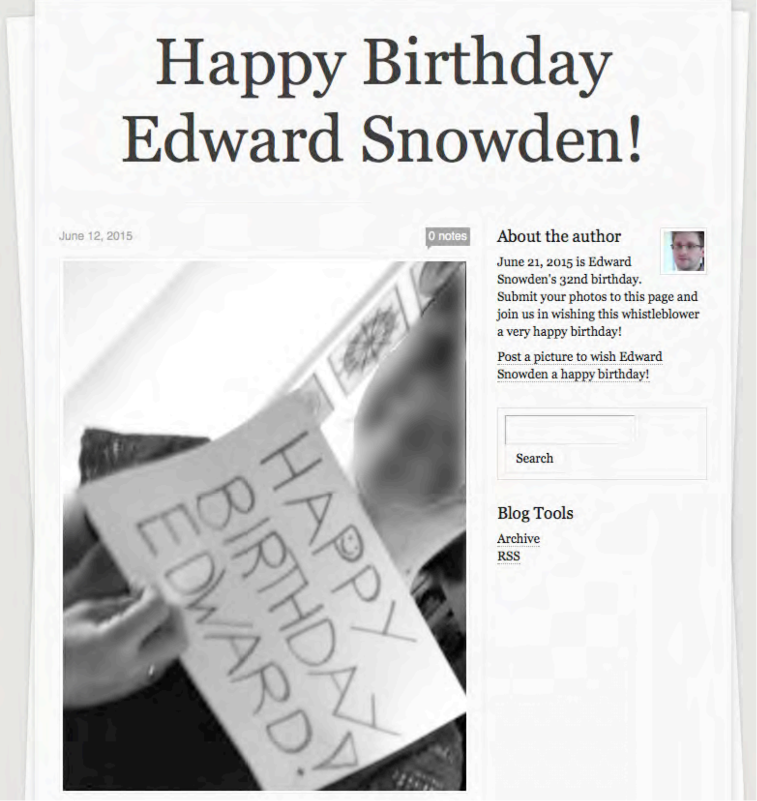
In the keynote speech of the 30th edition of the Chaos Communication Congress, Glenn Greenwald had a similar message for his audience, which is summarized in the following quotation:

> It is really hard to put into words what a profound effect his choice has had on me, and on Laura, and on the people with whom we've worked directly, and on people with whom we've indirectly worked, and then millions and millions of people around the world. The courage and the principled act of conscience that he displayed [...] will inspire and convince millions and millions of people to take all sorts of acts that they might not have taken because they've seen what good for the world can be done by even a single individual. But I think that

> it's so important to realize, and to me this is the critical point, is that none of us [...] did what we did in a vacuum. We were all inspired by people who have done similar things in the past. I'm absolutely certain that Edward Snowden was inspired in all sorts of ways by the heroism and self-sacrifice of Chelsea Manning. And I'm quite certain that, in one way or another, she, Chelsea Manning, was inspired by the whole litany of whistleblowers and other people of conscience who came before her to blow the whistle on extreme levels of corruption, wrongdoing and illegality among the world's most powerful factions. They in turn were inspired, I'm certain, by the person who is one of my greatest political heroes, Daniel Ellsberg, who did this forty years ago.

Just before he made this statement, Greenwald, similar to Appelbaum, took the time to thank his source, Edward Snowden. Greenwald stated that Snowden "has been utterly indispensable and deserves every last accolade and to share in every last award" (Greenwald). The audience received this with loud applause. Moreover, as becomes clear from the quotation, Greenwald also emphasized Snowden's courage and the influence he has had on mankind. He points out that it is not just Snowden who deserves respect, but that the people who inspired Snowden, such as Chelsea Manning and Daniel Ellsberg, deserve an equal amount of respect.

Another example of how whistleblowers, and Snowden in general, are valued within the privacy movement is the "Happy Birthday Edward Snowden" Tumblr. This website was hosted by CODEPINK and The Courage Foundation, and gave supporters a chance to upload congratulatory messages to Snowden for his 32nd birthday.



Happy Birthday Edward Snowden!

June 12, 2015

0 notes

About the author

June 21, 2015 is Edward Snowden's 32nd birthday. Submit your photos to this page and join us in wishing this whistleblower a very happy birthday!

Post a picture to wish Edward Snowden a happy birthday!

Search

Blog Tools

Archive

RSS

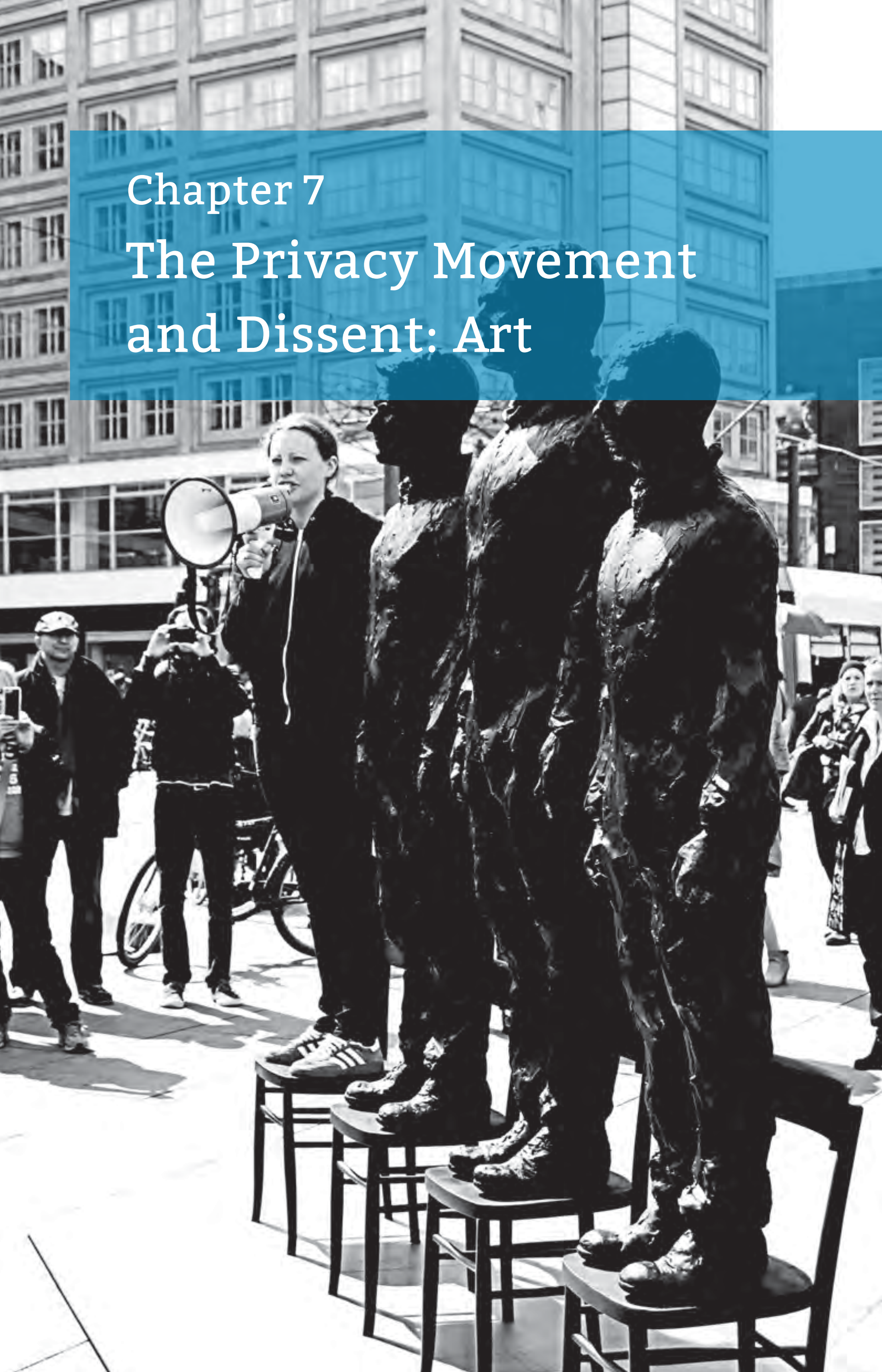
Fig. 4. Screenshot of the "Happy Birthday Edward Snowden!" Tumblr. *snowdenbday.tumblr.com*.

Initiatives like this show the impact Snowden's revelations have had, both on activists within the privacy movement as well as on a larger audience. That Snowden sought publicity and stepped forward as the source of the leak relatively early in the process was quite unique for a whistleblower. Not revealing his identity had never been an option for Snowden, feeling that "anyone who does something this significant has the obligation to explain to the public why he did it and what he hopes to achieve" (Greenwald 51). This has given the public a face behind the stories. Combined with his motives and the magnitude of the documents it has made him become a personification of what the privacy movement stands for and someone privacy activists respect and look up to for his courage.

This respect for whistleblowers also shows through organizations that support whistleblowers. When whistleblowers leak classified information, there is much at stake for them and they largely depend on others to help them. They are at risk of losing their freedom, either because they are given a prison sentence or because they are forced to live in exile like, for instance, Snowden. In *The War on Concepts*, Machon even claims that whistleblowers face prison sentences up to 35 years, that politicians call for their assassination, and that they are often under investigation and criminalized. This is a high price to pay, and activists and organizations within the movement dedicate themselves to helping them. WikiLeaks' Sarah Harrison, who accompanied Snowden on his escape from Hong Kong to Moscow, is aware of whistleblowers' need for help. Therefore, she has founded The Courage Foundation, an organization that protects whistleblowers (Corbett par. 10). Its Advisory Board consists of a growing number of prominent privacy activists from around the world. One of the aims of The Courage Foundation is to support citizens' right to information, and deems whistleblowers necessary to obtain that goal. Because blowing the whistle can put an individual in a vulnerable situation, the foundation works to gain public attention for their case and provide legal defense. In addition, the foundation recognizes that it is becoming increasingly difficult for journalists and publishers to protect their sources. Therefore, by protecting whistleblowers the organization aims to "engender a culture of support for radical transparency, adversarial journalism and democratic accountability" ("About Courage"). The Courage Foundation currently works on an "advisory system for journalists to improve their online security and better protect their sources" (Corbett, par. 22). Better online security in order to protect sources is an issue Greenwald and Poitras are also dedicated to. Together with, among others, whistleblowers Edward Snowden and Daniel Ellsberg they make up the Board of Directors of the Freedom of the Press Foundation. Appelbaum functions as one of the members of the foundation's Technical Advisory Board. This foundation, too, acknowledges the significance of digital security for journalists. The foundation offers tools that help to assert secure communication between journalists and their sources. It supports a number of encryption tools that enable secure communication and it has developed SecureDrop, "an open-source whistleblower submission system for news organizations" ("About Freedom of the Press Foundation"). In addition, the organization offers training to journalists to enhance their knowledge about digital security and encryption tools ("About Freedom of the Press Foundation").

Whistleblowing is one of the three ways in which the privacy movement expresses dissent. It should be characterized as dissent because of its elements of disagreement and complaint, but because of its public, non-violent, conscientious, and political character it can also be seen as civil disobedience. Literature does not view whistleblowing as protesting. However, because Snowden's whistleblowing can hardly be called a solo action, because he immediately sought the help of journalists, and because he is aiming for a fundamental change, the earlier defined boundary between whistleblowing and protest becomes vague in Snowden's case. The exceptional role of whistleblowers is characteristic of the privacy movement, and is threefold. Whistleblowers are a valuable source of information, as the information relevant to the movement is often meant to remain classified. After making a disclosure, whistleblowers often shift from whistleblower to member of the movement, and at the same time their actions also cause them to have a special position within the movement.

Chapter 7
The Privacy Movement and Dissent: Art



The Privacy Movement and Dissent: Art

Art is the second way in which the privacy movement expresses dissent. Although there are relatively few movement members involved in the actual process of creating the art, it does affect the movement as a whole and is a reflection of its beliefs. Art as "interventions", art as a "weapon of resistance", and art as a "weapon against injustice" are three of the most common terms to describe activist art and are all three applicable to the privacy movement's use of art (Goris 309; Reed 255; Simonds 5). This chapter will first explore the role of art in social movements. How art and activism can merge will subsequently be shown through the analysis of two recent art projects associated with the privacy movement. *Panda to Panda* is a collaboration between Ai Weiwei and Jacob Appelbaum for the online art and technology organization Rhizome. Twenty pandas were stuffed with shredded documents Edward Snowden leaked, together with a micro SD card with the same documents on it. *Anything to Say?*, designed by Charles Glass and Davide Dormino, is a bronze sculpture of Assange, Manning, and Snowden who each stand on a chair. A fourth chair is left empty and is meant for others to take place on and express themselves.

Art can be valuable in a number of ways for a social movement. In *The Art of Protest. Culture and Activism from the Civil Rights Movement to the Streets of Seattle*, T.V. Reed explains that art can fulfill ten different functions within a social movement. First, art encourages and makes individuals experience the strength of the group, for example through collective singing during rallies. In addition to experiencing the strength of the group, art can also help individuals to feel their own strength and commitment towards the movement. It can also bridge the gap between "age, class, region, [and] ideology" and thereby shape an "overarching connection that [...] subordinates differences" (Reed 299). Moreover, art informs both internally and externally: it expresses or reinforces "movement values, ideas, and tactics" to members within the movement as well as to individuals outside the movement (Reed 299). Some forms of art do not just express values and ideas, but are more direct. These forms then materialize the goals of a movement, for example when a mural is created in order to adjust the looks of a neighborhood (Reed 299). Connected to the function of informing is the function of historicizing, which captures different aspects of the movement, for example through a documentary. Furthermore, by evoking certain emotions art can also critique or alter movement ideology and tactics, which can change the tone and the direction in which a movement is going. Last, art can give the activists a welcome pause from the movement's work (Reed 299-300). Which of these functions are applicable to *Panda to Panda* and *Anything to Say?* will be returned to later on in this chapter.

How art can go hand in hand with activism can be explained through the notions of subversivity and subversion. Although philosopher and activist Lieven de Cauter problematizes these notions in the first chapter of *Art and Activism in the Age of Globalization*, they still prove to be useful terms to explain the relation between art and activism. In the chapter, de Cauter makes a distinction between subversivity and political subversion: despite the fact that subversivity aims to disrupt "the dominant system or hegemonic culture" where political subversion tries to overthrow it, they both have "an aversion for the center" and are therefore able to communicate or merge (De Cauter 9).

Subversivity and political subversion are, according to de Cauter, closely related to notions such as for example "criticism, dissent, protest, resistance, activism, [and] dissidence" (10). Subversion, then, has three different, autonomous forms. The subversion of truth undermines accepted theories, "dogmas", and "myths" (12). Aesthetic subversion can, for example, be found in modern art's subversion of traditional art. De Cauter, however, claims that this form of subversion no longer exists because there is nothing left to subvert. Ethico-political subversion is subversion as it is generally understood, and undermines or overthrows authority (12-13).

In a later chapter of the book, Belgian journalist Gie Goris elaborates on three requirements that art should meet if it wants to help subvert dominant power. First, art has to strive to "retain and cultivate its proper voice" (Goris 312). That proper voice is, according to Goris, cultural, as cultural power defines how we understand the world around us. The challenge in this is to not limit this to individuals or areas of society that are already share similar views, but instead reach and convince those who do not (312). Second, if art wants to be subversive, it needs to move away from the context it originally belongs to, for example a museum, to a place where power is located and decisions are made, for example "the street, the (mass) media, [or] religious spaces" (312). Third, art cannot be subversive unless it is well informed about the conflicts that influence our modern day world. Contributions to vague terms such as "peace, tolerance, and solidarity" are not enough to make a true impact (312).

There are a number of general features of activist art that *Panda to Panda* and *Anything to Say?* share, for example the way activist art comes into being. The art activists create almost always comes from personal experiences and wants to draw attention to and gain recognition for those experiences. It problematizes "authority, domination, and oppression" and seeks to alter the current situation. Moreover, activists like their work to evoke emotions and provoke intellectually, and aim to form a community among those who share a similar aversion to oppression (Simonds 2, 5). These features converge in a quotation from Ai Weiwei, taken from an interview he had with Andelman for *World Policy Journal*:

> In any society, if there is going to be change, it will take individuals, who come from different backgrounds, to show a true concern about the human condition and the rights of people of different groups and the demands of those different groups. So social activism is a natural product of an unjust society. And those individuals, who are devoted to facing this kind of system, must make people aware of the situation and search for possible better ways. Very often that does not happen immediately. But I think they are visionaries, because they believe and trust in humanity. (17)

Since the Internet has simplified information sharing, artists are now able to spontaneously group together to collaborate on these works of art (Deseriis 259). Collaboration among activists is not the only thing the Internet has stimulated: it is also a perfect opportunity to involve a larger audience to an art project and it gives activists the opportunity to, through social media, exchange with their audience (Deseriis 251).

Panda to Panda is part of a larger project: Seven on Seven. Seven on Seven is a project initiated by Rhizome, the new media wing of the New Museum in New York City. Each year, Rhizome matches seven artists with seven technologists. Each pair then travels to New York City, where they are given 24 hours to create an art project together, that will afterwards be presented during a conference. In 2015, one of the pairs Rhizome invited to participate were two dissidents: Ai Weiwei and Jacob Appelbaum (Hill, par. 1). Chinese activist and artist Ai Weiwei, sometimes called "the Andy Warhol of China", has been under the watch of the Chinese authorities since he started blogging about the government's wrongdoings in 2008. In 2011 he was detained for almost three months and was forced to give up his passport, which he has only very recently received back (Ramzy, par.1). Ai's art always has a dissenting character. He, for example, placed fresh flowers in the basket of his bike every single day during the three years in which he did not have a passport (Kedmey, par. 3). Because both Ai and Appelbaum are unable to travel to the United States, Appelbaum visited Ai's studio in Beijing, where they were given 48 instead of 24 hours to create their art piece. What Ai and Appelbaum subsequently created they have called *Panda to Panda*, and turned out to be more of a project than one single piece of art. *Panda to Panda* consists of twenty stuffed pandas, of which Ai and Appelbaum took out the stuffing and refilled with shredded documents that Glenn Greenwald and Laura Poitras received from Edward Snowden. In addition, a micro SD card with the documents on it was placed inside each panda. The project was documented by Ai, who shared the images with his followers on social media.

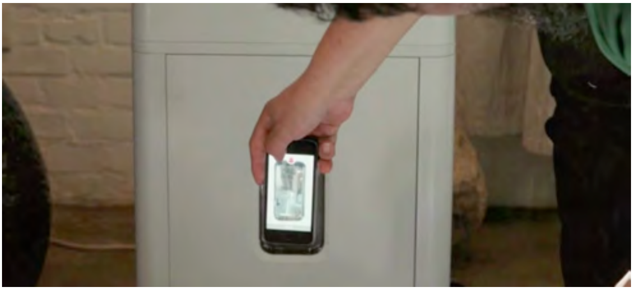


Fig. 5. Still from *The Art of Dissent*, Ai Weiwei films the shredding of the documents. *Nytimes.com*. The New York Times, 9 June 2015.

Laura Poitras was invited to film the process and eventually published the film in the online edition of *The New York Times*. In his *Seven on Seven* lecture about the project at the re:publica conference in Berlin, Appelbaum explains that after the pandas were shown at the Seven on Seven conference, he and Ai wanted to distribute them to as many places as possible. The pandas would then function as a "distributed backup" that would be difficult to destroy, since that would mean destroying all twenty pandas. One of these pandas was given to Harrison at the re:publica congress.

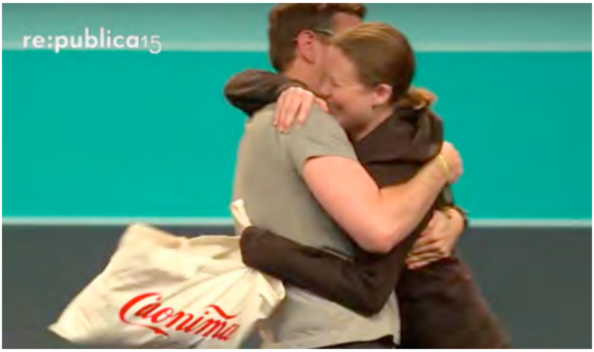


Fig. 6. Still from the video of the *Seven on Seven* lecture at the re:publica congress, Sarah Harrison is given a panda by Jacob Appelbaum. "re:publica 2015 – Jacob Appelbaum, Ai Weiwei, Laura Poitras: Seven on Seven." *Youtube*. Youtube, 9 June 2015.

Where the other pandas were distributed to and what the motivation for the title was, is also explained by Appelbaum during the re:publica conference:

> [...] and we sent them to a number of people using human networks, because resistance does not have to come just from the Internet, resistance comes from our hearts. And we can use our brains to do amazing things if we apply ourselves, and we wanted to make sure we would be able to share, so we called this project P2P or *Panda to Panda*. [...] so *Panda to Panda* is our attempt not only to thank the people who helped make this conversation possible, but also to make it impossible for people to stop us from having this conversation.

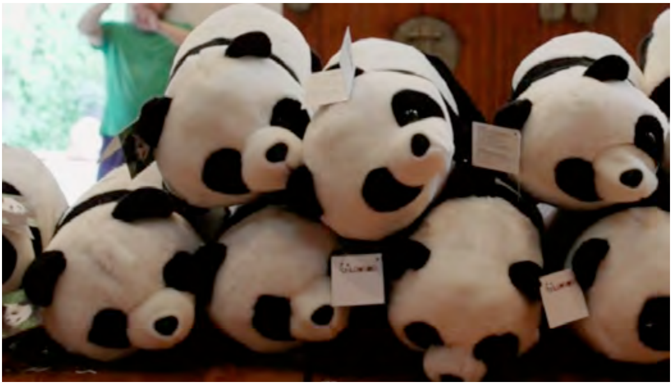


Fig. 7. Still from *The Art of Dissent*, the pandas with Ai Weiwei filming in the background. *Nytimes.com*. The New York Times, 9 June 2015.

Panda to Panda is an example of ethico-political subversion, in which authority is undermined in a number of ways. As mentioned, *Panda to Panda* turned out to be a project rather than a piece, and the project in its totality is a complaint against government surveillance and state power. As Ai, Appelbaum, and Poitras were working on the project, they have all been filming each other. Some of the material has been shared on social media. This made the documentation part of the project, but it also helped Ai and Appelbaum's followers to feel part of the project. In her *The New York Times* article on the project, Poitras writes they have "created a zone of hyper surveillance" (Poitras, par. 3). The constant filming emphasized and visualized the surveillance the trio is under: Ai, Appelbaum, and Poitras may all film each other, but in the meantime they are also watched by a number of surveillance cameras that the Chinese authorities have placed in front of Ai's studio. There is a constant awareness that they are always under watch anyway (Hill, par. 18).

The pandas, too, have a symbolic meaning. In *The New York Times* Poitras calls the title of the project "the synthesis of two terms created by dissident cultures" (Poitras, par. 5). Where Appelbaum likes to take direct action, Ai rather uses symbolism to make his point. And where Appelbaum aims to spread information, Ai tries to "find the hidden, deeper meaning in ordinary objects (Hill, par. 57). From Appelbaum's frame of reference, *Panda to Panda* is a variation on peer-to-peer communication, a means of communication in which there is no hierarchy and that allows all peers to interact in an equal way. This system is seen as "a philosophy of egalitarian human interaction on the Internet" (Poitras, par. 5). Appelbaum adds in a tweet that "the best peer-to-peer networks are humans", which he explained in his re:publica lecture as that he likes to see Internet in terms of human relationships (Connor, par. 9). From Ai's frame of reference, the pandas make a satirical reference to popular culture. In China, the secret police, the "government spies" that also surveil Ai, are often called pandas. According to Reed in *The Art of Protest. Culture and Activism from the Civil Rights Movement to the Streets of Seattle*, it is common that, like in *Panda to Panda*, elements of popular culture become mixed with movement cultures and are sometimes twisted by the movement (Reed 300-301). From both Ai and Appelbaum's reference, the shredding of the documents can be seen as a clear expression of resistance against the state oppression they both experience. Taking the original stuffing out of the pandas and re-stuffing them with documents of surveillance programs can also be explained as an internalization of censorship, as is pointed out in *Truthdig* (Shenkman, par. 10). By placing the data on a micro SD card in the pandas they can spread the information in the documents – they can "self-replicate" as Appelbaum says – something the privacy movement has always made an effort for (Hill, par. 58).

Poitras' short film, *The Art of Dissent*, adds an extra dimension to the project. At the Seven on Seven conference Poitras explained that the goal of her work is to "bridge the divide between our intellectual understanding and an emotional understanding of things like torture, occupation, and surveillance" ("Divorce Your Metadata", par. 11). This can be perceived from *The Art of Dissent*. A first version of the film was shown at the re:publica conference in Berlin and the final version appeared in *The New York Times*. In both versions, Appelbaum and Ai explain their harrowing experiences with surveillance and oppression (*The Art of Dissent*). This makes it very emotional and personal, and this can have a certain effect on members of the privacy movement. Because it is so personal, it may have an encouraging effect on those members. Although individuals do not sing together during a rally, as Reed mentions as an example, the personal character of Appelbaum and Ai's stories do make it easy for activists to identify with and experience a shared strength. The film has an implicit and yet very clear way of showing the privacy movement's ideas, values, and concerns to both insiders and outsiders to the movement. Through the personal stories of Ai and Appelbaum, *The Art of Dissent* shows on the one hand what the intelligence agencies do, and on the other hand critiques it by showing and shredding the documents. Furthermore, the film can function as documentation of the privacy movement's fight.

Anything to Say? A Monument of Courage is a life-size bronze sculpture by American author Charles Glass and Italian artist Davide Dormino. The sculpture portrays three men: Julian Assange, Edward Snowden, and Bradley Manning (who has now chosen to live her life as Chelsea Manning). The three men are standing on three chairs, and a fourth chair is left empty. This fourth chair is meant for other individuals, to enable them to stand with the whistleblowers and freely express themselves ("Project"). *Anything to Say?* has its own Twitter account where followers can follow the realization, unveiling, and journey of the sculpture. The sculpture has never been placed in a typical museum context: it was unveiled at Alexanderplatz in Berlin in and has been traveling since.

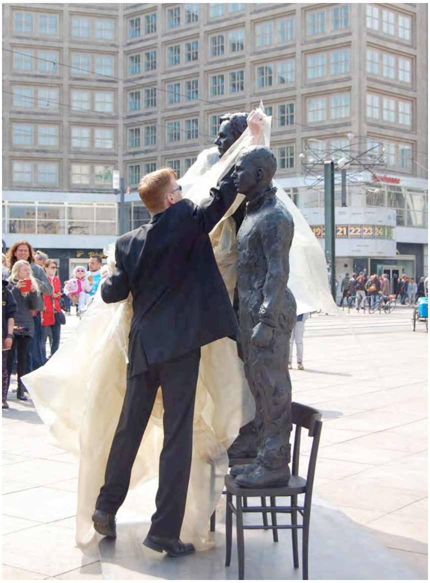


Fig. 8. Patrick Bradatsch unveils the sculpture at Alexanderplatz in Berlin (Loes Derks van de Ven).

Similar to *Panda to Panda*, an analysis of *Anything to Say?* demonstrates a number of ways in which art can strengthen the privacy movement. Words expressing thoughts on surveillance, oppression, and freedom of speech can be very powerful. By inviting the audience to speak as well as to listen to others, *Anything to Say?* succeeds in encouraging them and making them feel the strength of the group. Taking a stand on the fourth chair and expressing their thoughts does not come naturally to everyone, it takes a certain amount of courage, as the sculptures subtitle, *A Monument of Courage*, indicates. The sculpture encourages individuals to do the same as whistleblowers: step out of their comfort zone and become visible. This is reinforced on *Anything to Say?*'s Twitter account: "to get a better view you have to leave your comfort!". All three men are dressed in similar outfits. This emphasizes that the individual on the chair is on one level with the whistleblowers. This evokes a sense of equality and strength. Inviting the audience to speak makes them feel part of the artwork, and part of the group. Moreover, *Anything to Say?* does not only make the audience feel the strength of the group, it also makes individuals experience their own strength. When these individuals are part of the movement, expressing themselves confronts them with their own motives and commitment, as they are forced to overthink their own values regarding the subjects the privacy movement is concerned with. By welcoming everyone to stand on the empty chair the sculpture also bridges a gap between the audience members. Young or old, rich or poor, German or foreigner, part of the movement or not: the sculpture gives the audience a reason to connect. Furthermore, the sculpture carries out some of the beliefs of the privacy movement, and that informs individuals within as well as outside of the movement. Appelbaum and Harrison were present when the sculpture was unveiled, and Harrison's speech emphasized these beliefs.

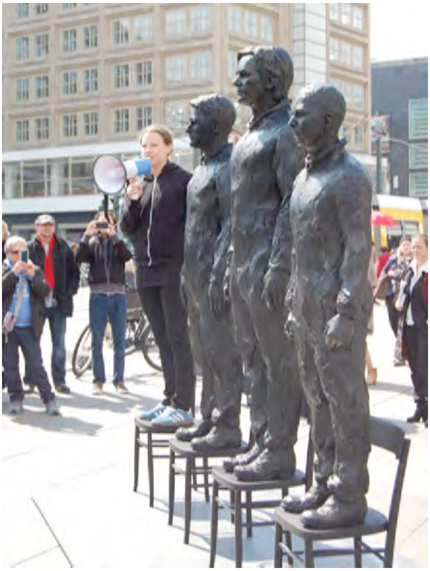
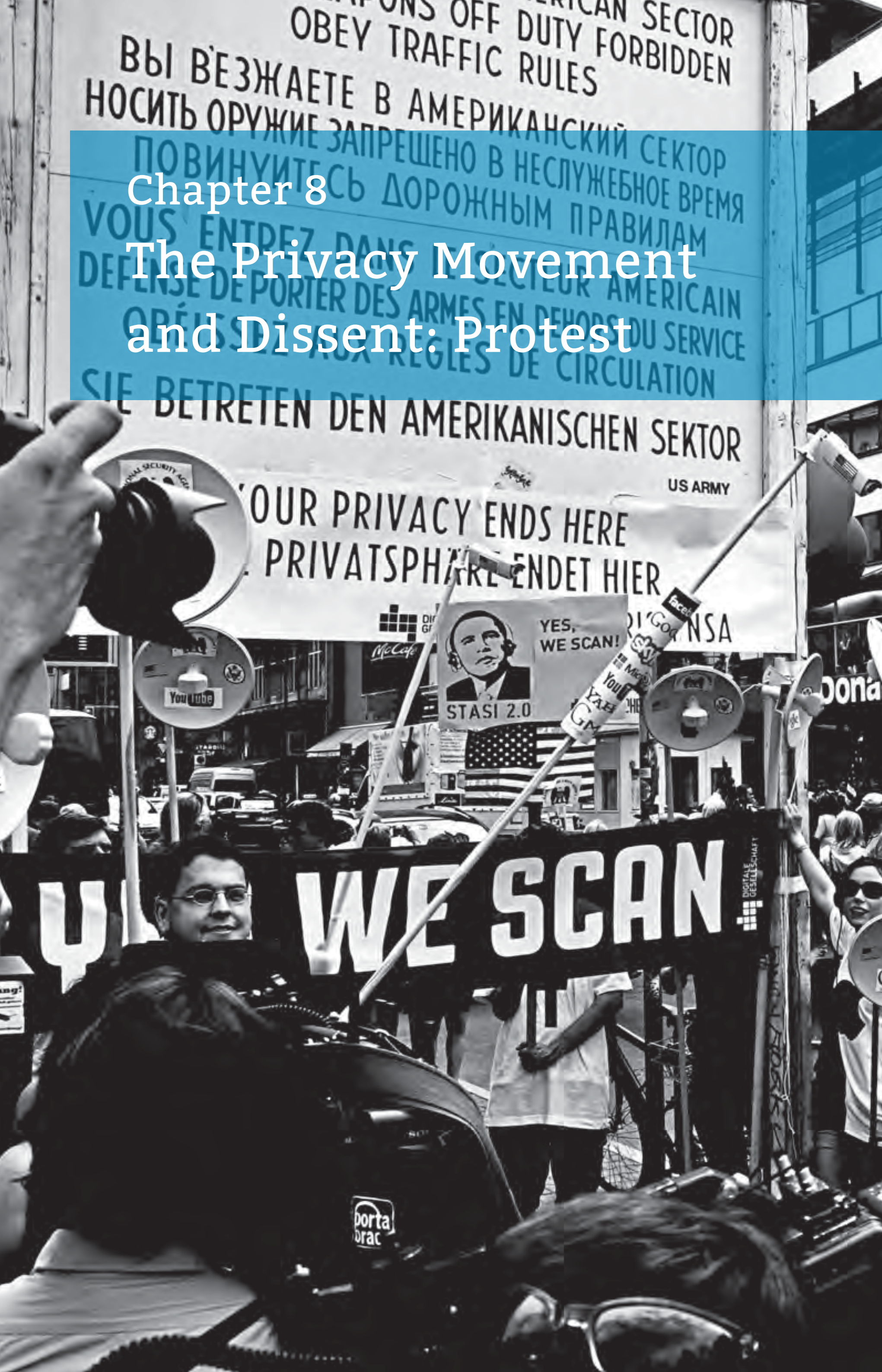


Fig 10. Sarah Harrison takes the fourth chair at the unveiling of *Anything to Say?* (Loes Derks van de Ven).

Anything to Say? does not only highlight the importance of the freedom of speech and the freedom of information, it also shows great respect for whistleblowers. It encourages the audience to show the same courage as Assange, Snowden and Manning have shown, but the sculpture in itself is also a sign of gratitude towards them. As Reed mentions, art does not only have to express certain movement values but can also be direct (Reed 299). This is also true for *Anything to Say?*: the sculpture in itself represents movement ideas and values, but by asking the audience to stand on the chair and express themselves it actually practices free speech and thereby practices one of the privacy movement's aims.

Activist art is a valuable way for the privacy movement to express what it stands for. Although there is only a relatively small group of activists within the movement that actually creates art, it has an impact on the entire movement. The analysis of *Panda to Panda* and *Anything to Say?* has shown that it encourages members within the movement and allows them to experience both their own and the group's strength. The personal character of the art reinforces this and the unity within the movement. The use of the Internet and social media helps both movement members and the general public to become involved in the projects.

Chapter 8
The Privacy Movement and Dissent: Protest


OBEY TRAFFIC RULES
DUTY FORBIDDEN
AMERICAN SECTOR
ВЫ ВЪЕЗЖАЕТЕ В АМЕРИКАНСКИЙ СЕКТОР
НОСИТЬ ОРУЖИЕ ЗАПРЕЩЕНО В НЕСЛУЖЕБНОЕ ВРЕМЯ
ПОВИНУЙТЕСЬ ДОРОЖНЫМ ПРАВИЛАМ
VOUS ENTREZ DANS LE SECTEUR AMERICAIN
DEFENSE DE PORTER DES ARMES EN DEHORS DU SERVICE
OBÉISSEZ AUX REGLES DE CIRCULATION
SIE BETRETEN DEN AMERIKANISCHEN SEKTOR
US ARMY
YOUR PRIVACY ENDS HERE
PRIVATSPHÄRE ENDET HIER
NSA
YES, WE SCAN!
STASI 2.0
WE SCAN
DIGITALE GESELLSCHAFT
YouTube
McCafé

The Privacy Movement and Dissent: Protest

Protest is the last of three ways in which the privacy movement expresses dissent. Protest is a form of action that is strongly tied to social movements, especially to the innovative ones like the privacy movement (Della Porta and Diani 168). Similar to other aspects of social movements, the digital age has also altered its protest. For the privacy movement the change is so comprehensive that it has become difficult to define what the role of the Internet exactly is; the boundaries between the online and offline sphere have faded. This chapter will first explore protest of social movements in general, both online and offline. Subsequently, it will zoom in on the types of protest used by the privacy movement, and what the role of the fading boundaries between the online and offline spheres on those protests is.

When political unrest changed social movements in the 1960s and 1970s, it also changed the way in which citizens legitimately exercise influence on decision-makers. Many of the means of protest in itself, such as "boycotts, barricades, petitions, and demonstrations", have not changed much since the 1700s, Della Porta and Diani claim (Della Porta and Diani 170). They were, however, not seen as a legitimate way to take part in politics. This changed from the 1970s onwards, when "signing petitions, lawful demonstrations, boycotts, withholding of rent or tax, occupations, sit-ins, blocking traffic, and wildcat strikes" also became a legitimate part of the protest repertoire (Della Porta and Diani 166).

Modern day protest is defined as "non-routinized ways of affecting political, social, and cultural processes" by Della Porta and Diani, who add that protests should be seen as "sites of contestation in which bodies, symbols, identities, practices and discourses are used to pursue or prevent changes in institutionalized power relations" (Della Porta and Diani 165). Influencing the political, social, and cultural processes always happens in a similar manner, and starts with a group of actors that are "interested in political decisions" (167). This group brings forth a group of leaders that initiates and leads actions and maintains contact with other, external groups. The mass media subsequently spreads the group's message. The message is, perhaps contrary to expectations, not directly aimed at decision-makers but at a group of individuals that is called "the reference public of the decision-makers" (167). When the reference public is convinced, they will likely use their resources to convince those who do have access to the decision-making process (167). This cycle influences the choice of the form the protest takes. The contact the leaders maintain with external groups is valuable, the strategies the leaders choose needs to appeal to the mass media in order to have the movement's message spread, and the influence of the reference public needs to be maximized in order to maximize the attention from decision-makers (Della Porta and Diani 178-179). Bearing all these factors in mind influences what type of protest is eventually chosen. In addition, the leaders must also keep in mind that the protest repertoire of a movement has an effect on the activists within the movement. It represents their values and creates solidarity and a collective identity among them, which in its turn is necessary to incite activists to action (179).

Three forms of action can be distinguished based on the pattern it follows: the logic of numbers, the logic of damage, and the logic of bearing witness. According to Della Porta and Diani, the logic of numbers assigns importance to the number of activists protesting, for example at demonstrations and marches, which will be returned to further on in this chapter. The logic of damage focuses on the violence that accompanies protests, which is not very relevant for the privacy movement. The logic of bearing witness, however, suits the privacy movement best. This form of action, which came up in the 1970s, has two main features that match the philosophy behind the privacy movement's protest. One feature is that instead of focusing on convincing decision-makers and the public, the protest focuses on the "strong commitment to an objective deemed vital for humanity's future", for example (online) human rights and the future of the Internet in the case of the privacy movement (Della Porta and Diani 176). This commitment is also the drive behind this form of protest, instead of some official authority or internal power. In the kind of protest that then results from this philosophy is a certain risk involved, which activists are willing to accept in order to demonstrate their beliefs (176). Della Porta and Diani mention Greenpeace actions or blocking nuclear sites as examples of riskful actions activists are willing to take. Although they come from the same philosophy, these actions are much more severe than the ways in which the privacy movement protests. However, the risk that is attached to it is equally serious. Expressing their beliefs and their commitment can leave them in a quite a predicament. Another feature of the bearing witness logic is that it has a certain "sensitivity [towards] other alternative values and cultures" and that it uses "conferences, journals, concerts, and documentaries" as means of education (177). In the case of the privacy movement, this shows for example through the conferences the activists attend and lecture at, the books and films that are published, and educational meetings such as

CryptoParties that are organized. All these activities attempt to change the public's view on the world, and the public is constantly addressed and encouraged to take action. Although political change certainly is a motive in the philosophy behind the logic of bearing witness, this change has to come from the public and not solely from political decision-makers. It is always a combination of a change in "political structures" and a change in "individual consciousness" (177).

The influence the arrival of the Internet has had on protest is twofold. On the one hand, the Internet has complemented already existing, offline forms of protest, such as street demonstrations. Because the Internet allows communication to spread fast and among large groups of people, it has made mobilization and organization easier for offline forms of protests and has given it the ability to go beyond borders (Van Aelst and Van Laer 1146). On the other hand, the Internet has also generated new forms of protest, which are often associated with hacktivism (Van Aelst and Van Laer 1147). Although the Internet has certainly not made offline forms of protest redundant, it has changed its character in such a manner that it becomes difficult to determine where the offline world stops and the online world begins. In "Internet and Social Movement Action Repertoires. Opportunities and Limitations", Belgian professors Peter van Aelst and Jeroen van Laer mention that some researchers find the online and offline world so "heavily interdependent" that the distinction between the two should no longer exist (1147).This view is also applicable to the privacy movement. The distinction between their online and offline protest forms is not very clear; every form of protest that shows characteristics of offline protest, shows equally as many characteristics of online protest. The online and offline world seamlessly merge into one another.

When keeping the focus on protest in the digital age, online activism can be divided into three areas, according to Sandor Vegh in *Cyberactivism: Online Activism in Theory and Practice*. These areas are based on the goal the initiative has. This can be either awareness/advocacy, which aims at sending and receiving information; organization/mobilization, which is focused on appealing to action; or action/reaction, which focuses on initiating or reacting to action (Vegh 73). Awareness/advocacy is the area that is closest to the goal of the privacy movement's protests. Similar to the aforementioned logic of bearing witness, the exchange of information is used to create public awareness in order to draw attention to the cause. Internet is used by activists to inform the public on events that are, according to Vegh, "not reported, underreported, or misreported in the mainstream mass media" (73). This is especially so when human rights are violated. Since the privacy movement is indeed concerned with human rights, it is thus logical that it uses the Internet to share information, although the information that is shared is, in addition to under- and misreported, also often classified or concealed. By reporting the wrongdoings, activists hope to achieve "public condemnation" and "subsequent action"(Vegh 72). The sharing and exchange of information has an additional advantage: it creates a connection between the public and the activists. The network that is then created enables easy mobilization and organization of protest. Vegh remarks that the Internet can be used as a way to inform the public because the channels that are traditionally used are often in the hands of those who's interests are opposite of the activists' interests. Up to a certain extend, this is also still true for the privacy movement. However, the fading boundary between the online and the offline world makes offline and online sharing equally difficult. The Internet is increasingly becoming a traditional channel. And like traditional channels, the Internet, too, is partly controlled by those who do not necessarily share the privacy movement's beliefs. The advocacy aspect of the awareness/advocacy area is concerned with the "organization of the movement and carrying out action" (73). It can either be "a strictly defined group, a civic advocacy group, a lobbying body, or a loosely defined group" that is responsible for this (73). The Internet then provides a communication channel that does not take up much of the activists' time and financial means (73). Awareness/advocacy is not the only area that the privacy movement's protests fit into. It also employs activities that fit into the organization/mobilization area, since it calls for both online and offline action. And, moreover, by developing, using, and promoting tools that target the censoring and controlling of the Internet, it also employs activities that fit into the action/reaction area (74-75). However, these activities are better explained through Van Aelst and Van Laer's distinction between actions that are either Internet-supported or Internet-based, and that have either a low threshold or a high threshold.

Protests in the digital age can be distinguished into two dimensions, namely one that determines if the actions are Internet-supported or Internet-based and one that determines the height of the threshold. This distinction proves to be useful to explain the ways in which the privacy movement protests in addition to the aforementioned educational activities. Protests that are Internet-supported are traditional means of protest that the Internet has made easier to coordinate and organize, whereas protests that are Internet-based can only happen because of the existence of the Internet. Here, too, Van Aelst and Van Laer mention that the distinction between the two is starting to blur, as even digitally correct hacktivists sometimes protest on the street (1148-1149). The second dimension involves the height of the threshold for people to become involved in the protest; a high threshold means that participating entails a high risk and level of commitment, while a low threshold means a low risk and level of commitment (1150).

Many of the privacy movement's protest actions are Internet-supported with a low threshold. According to Van Aelst and Van Laer, asking for a donation of money, legal protest demonstrations, and influencing consumer behavior qualify as Internet-supported actions with a low threshold. The privacy movement uses all three means of protest regularly, although in the case of the privacy movement the influencing of consumer behavior better suits Internet-based action with a low threshold. Organizations within the privacy movement often ask for a donation to support a whistleblower. The Courage Foundation, for example, asks for a donation for the legal defense of Edward Snowden, hacktivist Jeremy Hammond, and a number of other whistleblowers of which some need to stay anonymous. Occasionally, the foundation also opens emergency funds, as it for example recently did for British activist and alleged hacker Lauri Love ("Who We Support"). Recently, *The Intercept* and the Freedom of the Press Foundation cooperated to establish a fund for the legal defense of Chelsea Manning. Within two weeks the fund raised well over $156,000 of the necessary $200,000 ("Donate to Chelsea"). Furthermore, WikiLeaks also asks its supporters to make a donation in order to be able to continue to share news. According to Van Aelst and Van Laer, the Internet has given an impulse to donations: in the analogue age the costs to coordinate such actions would outweigh the donations it raised, but in the digital age this has become much easier. Worth noting is that in case of the privacy movement, the threshold for donating money may be slightly higher than Van Aelst and Van Laer describe in their article, as whistleblowing is a politically sensitive subject. At the end of 2010, Bank of America, Visa, MasterCard, PayPal, and Western Union decided to stop transferring money to WikiLeaks ("Banking Blockade"). The banking blockade WikiLeaks faces has increased awareness on the fact that governments are willing to enforce their power with the help of financial institutions. This leads one to suspect that governments and financial institutions are also willing and able to track from whom the organization receives donations. This increases the risk for contributors; donating via the anonymous digital currency Bitcoin is an option all aforementioned organizations offer.

Another Internet-supported form of action with a low threshold is legal demonstrations. For demonstrations, the logic of numbers that Della Porta and Diani describe is useful. The number of activists and supporters that attend a demonstration shows strength; it lets decision-makers know how large the activists' support system is and that a large part of the public does not support their decision. Moreover, a large group of protesters warn decision-makers know that they are at risk of losing voters if they do not adjust their policy (Della Porta and Diani 171). Here, the Internet has been an enhancing factor. It has made spreading and exchanging information about the goal and practical details of a demonstration much easier, which can increase the number of participants. Furthermore, the Internet can make every call to mobilization become transnational. When issues raise international concern, the Internet allows "domestically grounded activists" to connect to that issue and "[spur] local, large scale protest events" (Van Aelst and Van Laer 1153).

Many demonstrations were held by organizations within the privacy movement, especially in the months after the first publication of the Snowden documents. That the Internet helps to spread information fast is shown by the Digitale Gesellschaft's Yes We Scan demonstration, which was held at Checkpoint Charlie only two weeks after the first publications, when President Obama visited Berlin (Khazan). The demonstration was relatively small, and the Internet benefited it in a way Della Porta and Diani have not described: it had generated quite some attention from the (online) press, which helped to spread the activists' message. A larger demonstration was held a few months later in Washington, D.C. It was organized by Stop Watching Us, a group that describes itself as "a coalition of more than 100 public advocacy organizations and companies from across the political spectrum" ("About the Rally"). On the 12th anniversary of the PATRIOT Act, thousands of protesters gathered on the National Mall in Washington, D.C. to take part in the Rally Against Mass Surveillance. Stop Watching Us has made extensive use of the Internet, providing participants with all the information they could possibly need to successfully participate. The website also encourages those who do not live in the United States to find a satellite protest, which were for example held in eight different German cities. For those who were interested but unable to join the protest, the event was live streamed

("About the Rally"). Another example of how the Internet can rapidly spread information and the effect that has on protest is the Netzpolitik demonstration held in Berlin on August 1, 2015. The announcement that Netzpolitik, a German organization concerned with digital rights and culture, made that two of their reporters and one source had been charged with treason kicked up a storm among privacy activists. The announcement was made on 30 July, 2015, and soon the first tweets about a demonstration started to appear. No more than two days later, on August 1, 2015, thousands of people gathered on the streets of Berlin to protest for the freedom of the press ("Demo am 1. August"). Moreover, within a matter of days a number of leading privacy activists had showed their support for Netzpolitik, including tweets by Glenn Greenwald and the Courage foundation and a guest blog for Netzpolitik by Appelbaum about "Landesverrat" ("Glenn Greenwald (ggreenwald)"; "The Courage Foundation (couragefound)"; Appelbaum, "Jacob"). The fact that so many of the protests took place shorty after the first publications of the documents and Netzpolitik's announcement is not a coincidence. Della Porta and Diani describe this as part of a protest cycle. When the conflict heightens it is normal for protest to intensify, like an "ebb and flow in collective mobilization" (Della Porta and Diani 188-189). Times in which there is relatively little protest are followed by times of "intense mobilization that encompass large sections of societies, and quite often affect many societies simultaneously" (188).

Similar to the donation of money, it might also be worth considering how low the threshold for demonstrating really is for activists of the privacy movement. What the activists demonstrate against is, as mentioned, a sensitive subject.

The debate on government surveillance has not reached its conclusion yet; government opinions and policies are continuously changing, just like the technical means used for surveillance. In the analogue age it was difficult for governments to form a clear image of who exactly took part in a demonstration. Modern technology, however, does allow governments to get a good insight in this. That governments actually use these techniques becomes clear from an example Schneier uses in *Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World*. After participating in a protest, protesters in the Ukraine received a text message from their government that stated, "Dear Subscriber, you have been registered as a participant in a mass disturbance." (Schneier, *Data and Goliath* 2) Something similar happened in Michigan, U.S.A., in 2010. After a labor protest the local police asked for information about every cellphone that had been near the protest (2). Thus, the height of the risk that is involved in these sorts of protest is worth reconsidering.

Internet-based protests with a low threshold are less relevant to the privacy movement than those that are Internet-supported and have a low threshold. Van Aelst and Van Laer include the use of email bombs, virtual sit-ins, and online petitions in this category. Online petitioning is the only Internet-based action with a low threshold that the privacy movement uses. Although Van Aelst and Van Laer mention a research by Della Porta and Mosca from 2005 that concludes that online petitions are "the most widespread form of action that was used online", the privacy movement does not often make use of this form of action (Van Aelst and Van Laer 1156). Since the summer of 2013, there have only been a few large petitions. One petition was started through the online

We the People program of the White House, requested pardon for Snowden, and has recently been closed and rejected by the United States government ("We Petition"). Another petition was initiated by Stop Watching Us. It can still be signed, requests United States congress to give full insight in the NSA's surveillance programs, and is accompanied by a letter addressed to United States Congress ("Stop Watching Us"). In addition, Free Chelsea Manning initiated a petition that asks President Obama for the pardon of Chelsea Manning ("Free Chelsea Manning").

Similar to Internet-based protests with a low threshold, the privacy movement also does not take many Internet-supported actions with a high threshold. Van Aelst and Van Laer mention transnational demonstrations, transnational meetings, and sit-ins and occupations as this type of protest. Sit-ins and occupations are a rather radical form of protest that is not often used by activists from the privacy movement. Transnational demonstrations are linked to legal demonstrations as an Internet-supported action with a low threshold. Although the privacy movement has organized quite a few demonstrations over the past two years, not many of them were transnational. Only one, the Stop Watching Us demonstration, referred to satellite protests in another country. Only one other, a demonstration to protest against Germany's involvement with the NSA in July 2013, was simultaneously held in a number of German cities. Taking part in transnational meetings is the only form of Internet-supported protest with a high threshold that the privacy movement regularly uses. Van Aelst and Van Laer explain transnational meetings through the Global Justice Movement, which, for example, organizes various global, national, and local forums. The privacy movement does not organize any transnational meetings itself. There are, however, many (international) congresses that focus on digital issues, for example the Chaos Communication Congress and re:publica. These congresses always cover privacy and surveillance related subjects, and members of the privacy movement are almost always invited to lecture on this subject. The ways in which the Internet can be advantageous to transnational meetings is almost infinite: it can simplify the registration of participants, it can easily keep those participants updated on the latest news involving the event, it can widely communicate the planning of the event, and it can facilitate the organization's internal communication (Van Aelst and Van Laer 1154-1155).

In addition to Internet-supported action with a low threshold, Internet-based action with a high threshold is the protest form the privacy movement uses the most. Internet-based actions with a high threshold entail, according to Van Aelst and Van Laer, protest websites, alternative media, culture jamming and hacktivism. Protest websites are websites of social movements that "promote social causes and chiefly mobilizes support" (1158). Although the privacy movement is not involved in many of these websites, there are for example edwardsnowden.com and chelseamanning.org. These protest websites are dedicated to whistleblowers and explain the importance of their work and what supporters can help them with.

Alternative media websites use the Internet to publish their dissenting opinion on political and cultural subjects. Because the mass media either does not always publish on those subjects or does not share the activist's views, the Internet makes it possible to circumvent mass media and minimizes the effort to spread the information to a large audience. One example of alternative media the privacy movement uses is *The Intercept*, an online newspaper co-founded by Glenn Greenwald, Laura Poitras, and Jeremy Scahill. This newspaper aims, according to its website, to "[produce] fearless, adversarial journalism" and focuses on stories that provide transparency about government and corporate institutions' behavior ("Editorial Mission & Staff"). Whereas the Internet has made it easier for *The Intercept* to reach the public, media organization WikiLeaks cannot exist without the Internet. This second example of alternative media is fully dependent on the Internet. WikiLeaks aims to publish news that it deems necessary for the general public to know of ("What is WikiLeaks?"). As it usually supports its news with documents, it is even more dependent on whistleblowers to provide WikiLeaks with information. Submitting this information goes through a completely secure online system. Without the Internet, sharing this information would be much more difficult, since the information would physically have to reach WikiLeaks. This would entail a much larger risk for whistleblowers and would likely mean a decline in sources.

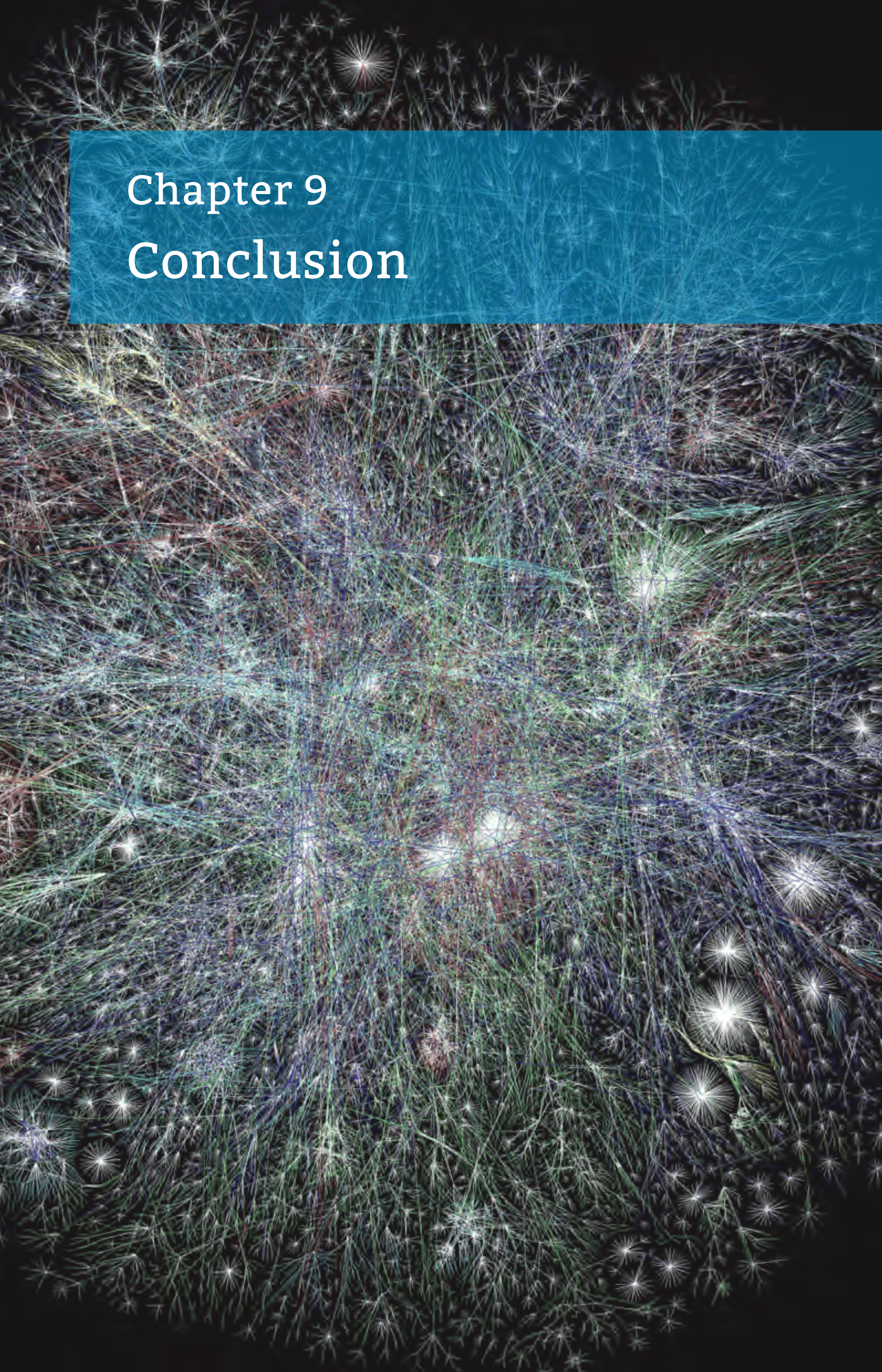
Culture jamming is a form of protest that the privacy does not use, at least not in its standard form. It is defined as protest that "changes the meaning of corporate advertising through artistic techniques that alter corporate logos visually and by giving marketing logos a new meaning" (1159). This is usually done through "appropriation, collage, ironic inversion, and juxtaposition", and it uses tactics such as "billboard pirating, physical and virtual graffiti, website alteration, [and] spoof sites" (1159). Although the privacy movement does not make use of any of these techniques, there is one example worth mentioning that can be seen as a new form of a spoof site, which is a clone of an already existing website that is meant to parody or provoke the organization behind the original program (1159). Activists within the privacy movement are often very active on social media, and specifically on Twitter. When at the end of 2013 the public relations department of the NSA launched its own Twitter account, there soon came a response in the form of a spoof account: @NSA_PR, or NSA Public Relations in full. The owners of the account have altered the original NSA logo by providing the American eagle with an evil grin and has come up with its own marketing slogan: "we care, we're here to listen" ("NSA Public Relations (NSA_PR)"). The account, of which the initiators are unknown, often responds to recent surveillance and security issues in a humorous way. When WikiLeaks published documents about the NSA's interception of French leaders, NSA Public Relations for example posted, "Parlez-vous Français?" And when the USA Freedom Act was enacted, the account posted, "Please direct all media inquiries regarding today's passage of #FreedomAct to someone who cares. Thank you." Moreover, the account also often responds to Glenn Greenwald's view on the NSA's surveillance activities, for example when it tweeted, "Hiring: Director of Strategic Communications. Responsibilities include: replying "Nuh uh" to @ggreenwald" on Twitter".

Van Aelst and Van Laer name hacktivism as the last form of Internet-based protest with a high threshold. They define hacktivism as "confrontational activities like DoS attacks via automated email floods, website defacements altering the source code of targeted websites, or the use of malicious software like viruses and worms" (1159). These activities are not commonly used within the privacy movement, and do not match the less aggressive techniques it does use. This does, however, not mean that the privacy movement does not use hacktivism as means of protest, but rather that it performs a digitally correct form of hacktivism. Hacktivism is often explained through the Electronic Disturbance Theater's Floodnet, which is used for virtual sit-ins by slowing down the server and reduce the network capacity (1160). Floodnet is an example of direct action hacktivism, something digitally correct hacktivists do not agree with because they believe in free flows of information (Jordan and Taylor 91). Digitally correct hacktivism designs programs that help confirm and accomplish their political aims (98). Chapter two already mentioned Peek-a-booty as being such a program. Of the many programs that exist, two of the most well-known and widely used programs for this kind of protest are the Tor Project web browser and Pretty Good Privacy. The Tor Project aims to "improve [...] privacy and security on the Internet" ("Tor: overview"). When a Tor user wants to go to a website, the Tor browser connects to a website via a number of intermediate servers instead of connecting to its destination directly. This process shields off the Tor user's identity and can help to reach websites that a government has forbidden ("Tor: overview"). WikiLeaks, for example, uses Tor to help sources upload their materials anonymously to its website. Pretty Good Privacy, better known as PGP, is a program that allows email-users to encrypt their emails. This means that the email is secured in such a way that it is impossible for anyone to open the message except for the receiver, who needs to have a private key with which only he can retrieve the original content ("Pretty Good

Privacy"). Both programs are designed to secure the user's privacy. Whereas it is debatable whether direct action hacktivism is legal or not, the use of the Tor browser and email encryption are legal. The anonymity the programs provide does, however, seriously hamper the work of intelligence agencies. Both the Tor Project and PGP are not new; they were developed long before Edward Snowden made his revelations. They are, however, always under development. Some activists have, for example, started to use other programs for encryption, such as the Free Software Foundation's GNU Privacy Guard (GPG). Activists within the privacy movement are often closely involved in the development of these, and similar programs, and always make the best of their chance to stress the importance of these programs. In addition to hacktivism, the promotion of these privacy tools also influences consumer behavior, which is originally a form of Internet-supported protest with a low threshold. Van Aelst and Van Laer name initiating a website that shows eco-friendly products as an example. The privacy movement does not use these "traditional ways" of influencing consumer behavior often, although the digital rights organization the Electronic Frontier Foundation has designed a scorecard of secure messaging programs ("Secure Messaging Scorecard"). However, by promoting privacy tools such as the Tor browser or PGP it does influence the Internet user's consumer behavior online. And by using certain programs and boycotting others, for example by using the Tor browser instead of Internet Explorer or the Safari browser, users show their political viewpoints.

In general, the digital age has had an enormous influence on how social movements protest. The boundary between the offline and online world has become vague, if not entirely disappeared. Despite those changes, the process of influencing decision makers has stayed the same, just like the philosophy behind the protest and the moment in which the protest takes place. Moreover, the privacy movement also still uses manners of protest that were already used long before society entered the digital age, although the rise of the Internet has altered those protests in such a way that using them without also using the Internet is unimaginable. In addition to Internet-supported protests, the rise of the Internet has also created protests that are Internet-based. Striking is that the way in which the privacy movement uses these types of protest and the risk that is attached to them differs from the standard, for both Internet-supported and Internet-based protests. Organizations do, for example, ask for donations or organize demonstrations, but the risks attached to it are different than what literature describes. The same is true for the risks attached to demonstrating. And although it does not use standard ways of culture jamming and hacktivism, it has developed its own forms. This shows that the way in which the privacy movement protests sometimes differs from what is described. Partly, this can be explained through the degree to which the Internet and technology is interwoven with the privacy movement. The human rights issues the privacy movement is concerned with may not be attached to either the online or offline sphere, the shape in which the issues become apparent is usually inextricably intertwined with technology. Furthermore, technology advances in an extremely rapid pace, which makes it challenging for literature to keep up with those changes.

Chapter 9
Conclusion



Conclusion

In the previous eight chapters, this thesis has provided an understanding of how the group that initially helped Snowden fits into a larger movement of privacy activists. This has been done through a number of elements that are characteristic to the privacy movement: composition, leadership, meeting places, and three types of dissent.

Social movement theory has formed an important basis of the understanding of the privacy movement. Della Porta and Diani's definition of a social movement has been leading. One of their criteria is that the actors are involved in conflictual relations with a clearly identified opponent. The privacy movement's ideas about government transparency, privacy, and a free Internet conflict with governments and intelligence services' surveillance activities. The movement's ideals relate to an equal relationship between a government and its citizens, in which citizens are given the freedom to be fully informed and the privacy necessary to speak freely. These ideas have roots in the 1960s Right to Know Movement and hacktivism. The other two criteria are the presence of dense, informal networks and a distinct collective identity. The privacy movement meets those two criteria, in which leadership and a physical meeting place play an important role.

Although leadership within the privacy movement is untraditional and decentralized, Appelbaum, Greenwald, Harrison, and Poitras have formed a small group that has taken on the function of movement leaders. Instead of being based on traditional aspects, their leadership is based on the way in which they move across movement organizations and the fact that they are perceived as representatives of the movement. Their leadership may not be traditional or fixed, they do play an important role in the movement: by making connections between people and organizations they benefit cooperation within the movement, and the social network they form draws new members to the movement.

A collective identity is established when activists have the opportunity to regularly meet, for example at certain events or certain locations. Here, the influence of the Internet plays a smaller role than perhaps expected. Although the Internet can have an advantageous effect on social movements, real social contact remains necessary. The presence of a physical meeting place leads to the rise of a movement scene, where social movements, subculture, and counterculture intersect and a collective identity is shaped. Similar to leadership within the privacy movement, its collective identity is also variable and flexible. Combined with its history and digital culture, the presence of leaders, movement members, and organizations make Berlin an ideal place for many activists within the privacy movement to meet and form a collective identity.

The way in which dissent is expressed can be distinguished into three categories: whistleblowing, activist art, and protest. Each has its own characteristics and its own function within the movement. The whole of these three forms of dissent combined gives a representative oversight of how the privacy movement disseminates their ideals and goals.

Whistleblowers have an exceptional function for and place within the privacy movement: they provide activists with information that is otherwise difficult to obtain, they often move from whistleblower to movement member, and their deeds are respected and applauded by other members of the movement.

Activist art has a number of ways in which it can influence and benefit a social movement, and the case study of *Panda to Panda* and *Anything to Say?* has shown the influence of art on the privacy movement. It enables other activists within the movement to experience the movement's strength, and encourages them to also share their personal experiences, which allows them to experience their membership. Through art, the movement is also able to convey its ideas and goals. The Internet, and especially social media, is an enhancing factor in this process.

In protest, the boundaries between the online and the offline spheres are fading, especially in the case of the privacy movement. The online and offline worlds are intertwined to such a degree that there is hardly a distinction perceptible between them. Most of the privacy movement's protests are either Internet-supported with a low threshold, such as asking for donations of money and street demonstrations, or Internet-based actions with a high threshold, such as protest websites and hacktivism.

A number of conclusions can be drawn from these findings. First, the privacy movement has a number of distinct characteristics that make it challenging to define as a whole. The movement exists out of a complicated web of links between individuals and organizations that function independently, but cooperate and share board members at the same time. Moreover, the group of individuals concerned with privacy and surveillance related issues is large. What the movement's membership criteria are and who actually is a member is not always clear-cut. The broader the view, the more difficult it becomes to define those criteria. Although there are definitely collective ideas and goals within the privacy movement, and thus a collective identity, this is also not always fixed and easy to define. While these features make it difficult to define this group of privacy activists, social movement theory has shown that new social movements can indeed have those characteristics. While the movement has a group of individuals that act as movement leaders, they do not fit into traditional descriptions of leadership. They are also not the only individuals within the movement that fulfill the role of a movement leader, but they are the ones that are very visible and vocal, and therefore able to forge links among other activists and organizations. Leadership, like membership and collective identities, can be fluid and variable instead of stabile and fixed. Here, existing literature is thus sufficient to determine that the privacy movement matches the main criteria that define a social movement.

Second, looking at Berlin as a meeting place for activists of the privacy movement has shown the advantageous effect of "real" meeting places for a social movement in the digital age. It is surprising that the privacy movement exactly complies with what the current literature describes; the Internet certainly has benefits but real life contact remains necessary. Despite the fact that the core of the discussion the privacy movement joins is about human rights in general instead of merely about online rights, the movement is inextricably intertwined with technology and the Internet. This may lead to the expectation that "real" meeting places are no longer necessary. However, in Berlin the privacy movement has found a place to gather. The city shares a similar attitude towards surveillance, and its vibrant digital culture brings forth many initiatives and events that allow privacy activists to easily fit in and form a collective identity. In this respect, too, it is possible to explain characteristics of the privacy movement through existing literature.

Third, the privacy movement also has a characteristic that existing literature sometimes fails to adequately describe: the way in which it expresses dissent. Whistleblowing, activist art, and protest are all three described in literature as accepted ways to express dissent. The way in which it deviates becomes most apparent in whistleblowing and protest. The importance the privacy movement attributes to whistleblowing is unique to this movement. While there is indeed some literature available that describes whistleblowing as dissent, there is no literature that describes its relation to social movements. The way the privacy movement depends on whistleblowers for information, but at the same time also deeply respects their deeds and admits them to the movement is not advanced in analyses of other social movements.

Furthermore, descriptions do not entirely fit the types of protests the privacy movement uses. This can be attributed to both the rapid development the Internet and technology undergo and the nature of the issues the privacy movement is concerned with. The donation of money, for example, is described as a type of protest that is Internet-supported. However, the analysis of current requests for donations shows that the Internet has completely taken over this type of protest. Every aspect of the fund-raising process takes place online. The same is true for street demonstrations. The actual protest does take place in the "real" world, but this is so intertwined with the Internet that the demonstration itself is the only element that happens offline, and even that is supported by the Internet through the online sharing of images and stories of the protest. For both of these types of protest the risk is higher than the literature describes because of the combination of advanced surveillance techniques and the political sensitiveness of the subject. Literature regarding Internet-based protests is also not entirely adequate to describe the types of Internet-based protests of the privacy movement. Particularly the definition of protest websites and hacktivism are no longer sufficient. The movement has accustomed the content of its websites to its own needs by mostly dedicating it to whistleblowers. Moreover, the programs the movement develops are generally not confrontational and meant to actually break systems, but are meant to enforce the movement's ideas of the freedom of information through programs that hamper intelligence agencies' work.

What these aforementioned elements of composition, leadership, meeting spaces, whistleblowing, art, and protest share is that Appelbaum, Greenwald, Harrison, and Poitras are involved in all of them. After the publication of the Snowden documents, this group has started to fulfill a leading role within a group of already active privacy activists. They are the focal points of a large web in which they share contacts and activities that they are involved in. Moreover, they also share Berlin as a central place where they, together with other privacy activists, often meet. They each have their own areas in which they work with whistleblowers, but their activities often intersect. In addition, Greenwald and Poitras have co-founded the alternative media outlet *The Intercept*. Appelbaum and Poitras sometimes collaborate on art projects, but Greenwald was also featured in *CITIZENFOUR* and Harrison received one of the twenty pandas from *Panda to Panda*. And when *Anything to Say?* was unveiled, Appelbaum was present and Harrison gave a speech. Moreover, when two reporters and a source of Netzpolitik were charged with treason, Appelbaum, Greenwald, and Harrison's The Courage Foundation all drew attention to the case. Through this web of intersecting contacts and activities, Appelbaum, Greenwald, Harrison, and Poitras do not only form a powerful group themselves, but they also build bridges between other individuals and organizations.

In conclusion, it can be stated that in some aspects the existing literature is adequate to understand the privacy movement, and in some aspects it is not. The latter can be attributed to the advancement of technology in general and of the Internet in particular, the degree to which the use of the Internet is interwoven to the privacy movement, and the fact that there has been only little research done on this particular movement yet. Therefore, this thesis provides a global and general insight into the privacy movement, and can serve as a starting point for further, more specific research. The privacy movement in its entirety is larger than described here and originates from long before Snowden made his revelations, albeit in a different form. Because of the magnitude and diversity of the movement, it can be valuable to research it through one perspective, for example through journalism, law, or technology. Although Berlin is the place where the group that initially helped Snowden gathers, it is not the only place that has a very thriving digital culture. Other cities, such as Barcelona for example, could also have been a research subject. Moreover, Berlin's digital culture is large and diverse enough to dedicate an entire thesis to. Furthermore, the types of dissent the privacy movement expresses can be researched more in depth than possible in one master's thesis. The privacy movement's expressions of dissent are deviant and interesting enough to each become a separate master's thesis.

Works Cited

"About." *Anniemachon.ch*. Annie Machon, n.d. Web. 13 July 2015.

"About Courage." *Couragefound.org*. The Courage Foundation, n.d. Web. 13 July 2015.

"About Freedom of the Press Foundation." *Freedom.press*. Freedom of the Press Foundation, n.d. Web. 13 July 2015.

"About the Rally." *Rally.stopwatching.us*. Stop Watching Us, n.d. Web. 29 July 2015.

"About Us." *Firstlook.org*. First Look Media, 2014. Web. 20 July 2015.

Andelman, David A. "The Art of Dissent. A Chat with Ai Weiwei." *World Policy Journal* 29.3 (2012): 15-21. Web. 20 July 2015.

Anything to Say? (AnythingtoSay_). "To get a better view you have to leave your comfort!" 5 June 2015, 2:25 p.m. Tweet.

Appelbaum, Jacob. *An Archive of Jacob Appelbaum's Post-Katrina Blog*. Wordpress, Sept. 2005. Web. 25 July 2015.

Appelbaum, Jacob. "Jacob Appelbaum zum #Landesverrat: The nightmare is the punishment – Der Alptraum ist die Strafe." *Netzpolitik.org*. Netzpolitik, 6 Aug. 2015. Web. 8 Aug. 2015.

Appelbaum, Jacob. Personal interview. 4 May 2015.

Appelbaum, Jacob, Renata Avilla, Harry Halpin, B. Traven. "Putting the "Revolution" back in Internet Revolution: Programmers and Social Movements." 7 May 2015. Lecture.

Appelbaum, Jacob. "Seven on Seven." re:publica, Berlin. 7 May 2015. Lecture.

Appelbaum, Jacob. "Surveillance and You." Security in Times of Surveillance. Eindhoven Institute for the Protection of Systems and Information, Eindhoven University of Technology, Eindhoven. 28 Apr. 2014. Lecture.

Appelbaum, Jacob. *Talks 2005-2013*. Greyscale Press, 2013. Print.

Appelbaum, Jacob. "To Protect and Infect, Part 2." 30th Chaos Communication Congress, Chaos Computer Club, Berlin. 29 Dec. 2013. Lecture.

Assange, Julian. *Cypherpunks. Freedom and the Future of the Internet*. New York, 2012. Print.

Ayers, Michael D., and Martha McCaughey, ed. *Cyberactivism. Online Activism in Theory and Practice*. New York: Routledge, 2003. Print.

Ball, James. "NSA Explainer." *The Guardian*. The Guardian, 14 Oct. 2013. Web. 7 Mar. 2015.

Bamford, James. "The NSA and Me." *The Intercept*. First Look Media, 2015. Web. 1 Aug. 2015.

"Banking Blockade." *Wikileaks.org*. Wikileaks, 28 June 2011. Web. 28 July 2015.

"Berlin is Divided." *History.com*. History Channel, 2009. Web. 27 July 2015.

"Bio: William Binney and J. Kirk Wiebe." *Whistleblower.org*. Government Accountability Project, 2015. Web. 13 July 2015.

Bundesrepublik Deutschland. Deutscher Bundestag. *Basic Law for the Federal Republic of Germany*. Berlin, 2012. Web. 27 July 2015.

"c-base Official Handout." *c-base.org*. c-base. Web. 27 July 2015.

"c-base." *Wiki.hackerspaces.org*. Hackerspace Wiki, n.d. Web. 27 July 2015.

Cadwalladr, Carole. "Berlin's digital exiles: where tech activists go to escape the NSA." *The Guardian*. The Guardian, 9 Nov. 2014. Web. 7 Mar. 2015.

Castells, Manuel. *Networks of Outrage and Hope. Social Movements in the Internet Age*. Cambridge: Polity Press, 2012. Print.

Channel 4. "Alternative Christmas Message 2013. Online video clip. *Channel 4*. Channel 4, 25 Dec. 2013. Web. 25 July 2015.

CITIZENFOUR. Dir. Laura Poitras. Perf. Edward Snowden, Glenn Greenwald, and Ewen MacAskill. Praxis Films, 2014. Film.

"Civil Disobedience." *Stanford Encyclopedia of Philosophy*. N.p., 2013. Web. 13 July 2015.

Connor, Michael. "Eight Big Ideas from Seven on Seven." *Rhizome.org*. Rhizome, 4 May 2015. Web. 8 Aug. 2015.

"Constitutional History of Germany." *Constitutionnet.org*. International IDEA, 2014. Web. 27 July 2015.

Corbett, Sara. "How a Snowdenista Kept the NSA Leaker Hidden in a Moscow Airport." *Vogue*. Vogue, 19 Feb. 2015. Web. 5 Apr. 2015.

DDR Museum. Berlin: DDR Museum, 2006. Plaque.

De Cauter, Lieven. *Art and Activism in the Age of Globalization*. Ed. Lieven de Cauter, Ruben de Roo, and Karel Vanhaesebrouck. Rotterdam: NAi Publishers, 2011. Print.

De Cauter, Lieven, Ruben de Roo, and Karel Vanhaesebrouck, eds. *Art and Activism in the Age of Globalization*. Rotterdam: NAi Publishers, 2011. Print.

De Graaf, Beatrice, and Schinkel, Willem. "Het recht op veiligheid schept een permanente noodtoestand." *NRC*. NRC, 31 Dec. 2010. Web. 7 Mar. 2015.

"De Jacht op Edward Snowden." KRO. NPO2, 25 Jan. 2015. Television.

De Koning, Bart. *Alles onder controle*. Amsterdam: Balans, 2008. Print.

Della Porta, Donatella, and Mario Diani. *Social movements. An Introduction*. Malden: Blackwell Publishing, 2006. Print.

De Maria, William. "Whistleblowers and Organizational Protesters. Crossing Imaginary Borders." *Current Sociology* 56.6 (2008): 865-883. Web. 3 July 2015.

"Demo am 1. August: Für Grundrechte und Pressefreiheit – Gegen die Einschüchterung von netzpolitik.org und seiner Quellen." *Netzpolitik.org*. Netzpolitik, 31 July 2015. Web. 31 July 2015.

Deseriis, Marco. *Art and Activism in the Age of Globalization*. Ed. Lieven de Cauter, Ruben de Roo, and Karel Vanhaesebrouck. Rotterdam: NAi Publishers, 2011. Print.

De Zwart, Hans. “Uitreiking Winston Award Q&A met Edward Snowden.” Big Brother Awards. 14 Dec. 2014. Lecture.

Diani, Mario. *Social Movements and Networks. Relational Approaches to Collective Action*. Diani, Mario, and Doug McAdam, eds. New York: Oxford, 2003. Print.

“Divorce Your Metadata. A Conversation Between Laura Poitras and Kate Crawford.” *Rhizome.org*. Rhizome, 2015. Web. 8 Aug. 2015.

“Donate to Chelsea Manning’s Legal Defense.” *Freedom.press*. Freedom of the Press Foundation, n.d. Web. 28 July 2015.

“East Germany Created.” *History.com*. History Channel, 2010. Web. 27 July 2015.

“Editorial Mission & Staff.” *Theintercept.com*. First Look Media, n.d. Web. 8 Aug. 2015.

European Parliament. Directorate-General for Internal Policies of the European Parliament. *National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility With EU Law*. By Prof. Didier Bigo, et al. Oct. 2013. Web. 27 July 2015.

“Events.” *Ccc.de*. Chaos Computer Club, n.d. Web. 27 July 2015.

“Films.” *Praxisfilms*. Praxis Films, 2015. Web. 25 July 2015.

Fleischhauer, Jan. “What’s the Fuss about US Surveillance?” *Der Spiegel*. Der Spiegel, 5 July 2013. Web. 27 July 2015.

“Free Chelsea Manning.” *Chelseamanning.org*. Free Chelsea Manning, n.d. Web. 29 July 2015.

“Free Snowden. In Support of Edward Snowden.” *Freesnowden.com*. The Courage Foundation, n.d. Web. 8 Aug. 2015.

“Glenn Greenwald (ggreenwald).” Twitter Account. *Twitter*, n.d. Web. 8 Aug. 2015.

“Glenn Greenwald.” *Salon.com*. Salon Media Group, 2015. Web. 20 July 2015.

Goris, Gie. *Art and Activism in the Age of Globalization*. Ed. Lieven de Cauter, Ruben de Roo, and Karel Vanhaesebrouck. Rotterdam: NAi Publishers, 2011. Print.

Greenwald, Glenn. "30C3 Keynote." 30th Chaos Communication Congress. Chaos Computer Club, Berlin. 28 Dec. 2013. Lecture.

Greenwald, Glenn, Ewen MacAskill, and Laura Poitras. "Edward Snowden: the whistleblower behind the NSA surveillance revelations." *The Guardian*. 11 June 2013. Web. 7 July 2015.

Greenwald, Glenn. *No Place To Hide. Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Metropolitan Books, 2014. Print.

Greenwald, Glenn. "NSA Collecting Phone Records of Millions of Verizon Customers Daily." *The Guardian*. The Guardian, 6 June 2013. Web. 17 July 2015.

Gurnow, Michael. *The Edward Snowden Affair: Exposing the Politics and Media Behind the NSA Scandal*. United States: Cardinal Publishers Group, 2014. Print.

Gutbub, Marie. "Cryptoparty Introduction Video." Online video clip. *Vimeo*. Vimeo, Feb. 2015. Web. 22 May 2015.

"Happy Birthday Edward Snowden!" *Snowdenbday.tumblr.com*. Tumblr, 18 May 2015. Web. 7 Aug. 2015.

Harris, Shane. *The Watchers. The Rise of America's Surveillance State*. New York: The Penguin Press, 2010. Print.

Haunss, Sebastian, and Darcy K. Leach. *Culture, Social Movements, and Protest*. Ed. Hank Johnston. Burlington: Ashgate Publishing Company, 2009. PDF.

Hill, Kashmir. "Three Days in Beijing with Three of the World's Most Famous Dissidents." *Fusion*. Fusion, 27 Apr. 2015. Web. 28 Apr. 2015.

Hornung, Gerrit, and Christoph Schnabel. "Data protection in Germany I: The population census decision and the right to informational self-determination." *Computer Law & Security Report* 25.1 (2009): 84-88. Web. 27 July 2015.

"Join Us in Urging President Obama to Pardon Chelsea Manning." *Chelseamanning.org*. Free Chelsea Manning, n.d. Web. 29 July 2015.

Jordan, Tim, and Paul Taylor. *Hacktivism and Cyberwar. Rebels with a Cause*. London: Routledge, 2005. Print.

Jubb, Peter B. "Whistleblowing: A Restrictive Definition and Interpretation" *Journal of Business Ethics* 21 (1999): 77-94. Web. 3 June 2015.

Kedmey, Karen. "Passport-Carrying Ai Weiwei Mounts His First Solo Shows in China." *Artsy*. Artsy, 27 July 2015. Web. 27 July 2015.

Khazan, Olga. "'Yes We Scan': Germans Protest at Checkpoint Charlie as Obama Arrives in Berlin." *The Atlantic*. The Atlantic, 18 June 2013. Web. 28 July 2015.

Machon, Annie. "Launch Event Code Red". Code Red, Berlin. 23 Apr. 2015. Lecture.

Machon, Annie. Personal interview. 5 May 2015.

Machon, Annie. "The War on Concepts." re:publica, Berlin. 5 May 2015. Lecture.

McCoy, Alfred W. "Surveillance Blowback. The Making of the U.S. Surveillance State, 1898-2020." *The Nation*. The Nation, 16 July 2013. Web. 15 July 2015.

"Modus Operandi." *Codered.is*. Code Red, 2015. Web. 11 May 2015.

"Noob." Oxford Dictionaries. Oxford: Oxford University Press, 2015. Web. 7 Aug. 2015.

NSA Public Relations (NSA_PR). "Hiring: Director of Strategic Communications. Responsibilities include: replying "Nuh uh" to @ggreenwald on Twitter." 25 July 2014, 09:14 p.m. Tweet.

NSA Public Relations (NSA_PR). "Parlez-vous Français?" 24 June 2015, 12:16 a.m. Tweet.

NSA Public Relations (NSA_PR). "Please direct all media inquiries regarding today's passage of #FreedomAct to someone who cares. Thank you." 2 June 2015, 10:45 p.m. Tweet.

"NSA Public Relations (NSA_PR)." Twitter Account. *Twitter*, n.d. Web. 8 Aug. 2015.

Orwell, George. *1984*. Adelaide: Ebooks@Adelaide, 2013. iBooks file.

Postill, John. "Freedom Technologists and the New Protest Movements: A Theory of Protest Formulas." *Convergence: The International Journal of Research into New Media Technologies* 20.4 (2014): 402-418. Web. 25 June 2015.

Poitras, Laura. "The Art of Dissent." *The New York Times*. The New York Times, 9 June 2015. Web. 20 July 2015.

"Privacy Laws in Germany - Developments Over Three Decades." *Iitr.de*. Institut für IT-Recht, 23 May 2013. Web. 27 July 2015.

"Pretty Good Privacy (PGP)." *Searchsecurity.techtarget.com*. Tech Target, 2015. Web. 8 Aug. 2015.

"Profile: Sarah Harrison." *WikiLeaks.org*. WikiLeaks, 2013. Web. 25 July 2015.

"Project." *Anythingtosay.com*. Anything to Say?, 2015. Web. 20 July 2015.

Ramzy, Austin. "Ai Weiwei, Chinese Artist and Provocateur, Is Given Back His Passport." *The New York Times*. The New York Times, 22 July 2015. Web. 22 July 15 2015.

Reed, T. V. *The Art of Protest. Culture and Activism from the Civil Rights Movement to the Streets of Seattle*. Minneapolis: University of Minnesota Press, 2005. Print.

Reitman, Janet. "Snowden and Greenwald: The Men Who Leaked the Secrets." *Rolling Stone*. Rolling Stone, 4 Dec. 2013. Web. 20 July 2015.

Roth, Anne. “Launch Event Code Red”. Code Red, c-base, Berlin. 23 Apr. 2015. Lecture.

Ryge, Leif. Personal interview. 4 May 2015.

Schmeidel, John C. *Stasi. Shield and Sword of the Party*. New York: Routledge, 2008. Print.

Schneider, Ruth. “We’ve Entered Revolutionary Times. Jacob Appelbaum: New Berliner, Exiled Hactivist, Passionate Idealist.” *Exberliner*. Sept. 2014: 8-11. Print.

Schneier, Bruce. *Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C*. New York: John Wiley & Sons, 1996. Print.

Schneier, Bruce. *Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World*. New York: W. W. Norton & Company, 2015. Print.

Scheuerman, William E. “Whistleblowing As Civil Disobedience: The Case of Edward Snowden.” *Philosophy and Social Criticism* 40.7 (2014): 609-628. Web. 3 July 2015.

Scott, Katherine A. *Reining in the State. Civil Society and Congress in the Vietnam and Watergate Eras*. Lawrence: University Press of Kansas, 2013. Print.

“Secure Messaging Scorecard.” *Eff.org*. Electronic Frontier Foundation, n.d. Web. 8 Aug. 2015.

Shenkman, Carey. “Techno-Art of the Moment, Featuring Laura Poitras, Ai Weiwei and the Mona Lisa.” *Truthdig*. Truthdig, 5 May 2015. Web. 20 July 2015.

Simonds, Wendy. “Presidential Address: The Art of Activism.” *Social Problems* 60.1 (2013): 1-26. Web. 20 July 2015.

Snowden, Edward J. “The World Says No to Surveillance.” *The New York Times*. The New York Times, 4 June 2015. Web. 4 June 2015.

Snowden, Edward J. “Uitreiking Winston Award Q&A met Edward Snowden.” Big Brother Awards. 14 Dec. 2014. Lecture.

Spiegel Staff. "Inside TAO: Documents Reveal Top NSA Hacking Unit." *Der Spiegel*. Der Spiegel, 29 Dec. 2013. Web. 7 Mar. 2015.

Stasi Museum. Berlin: Haus 1, 2015. Plaque.

"Statement by Edward Snowden to Human Rights Groups at Moscow's Sheremetyevo Airport." *Wikileaks.org*. WikiLeaks, 12 July 2013. Web. 13 July 2015.

"Stop Watching Us." *Optin.stopwatching.us*. Stop Watching Us, n.d. Web. 9 Aug. 2015.

SuddenlySnowden, Edward J. Snowden. "Just days left to kill mass surveillance under Section 215 of the Patriot Act. We are Edward Snowden and the ACLU's Jameel Jaffer. AUA." *Reddit*. Reddit. Web. 1 Aug. 2015.

The Art of Dissent. Dir. Laura Poitras. Perf. Ai, Weiwei and Jacob Appelbaum. Praxis Films, 2015. Film.

"The Courage Foundation (couragefound)." Twitter Account. *Twitter*, n.d. Web. 8 Aug. 2015.

"The Five Eyes." *Privacyinternational.org*. Privacy International, n.d. Web. 11 Aug. 2015.

"The Watergate Story." *Washingtonpost.com*. The Washington Post. Web. 25 June 2015.

"Tor: Overview." *Torproject.org*. Tor, n.d. Web. 8 Aug. 2015.

United Nations. Human Rights Council. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. New York: United Nations, 2015. Web. 26 May 2015.

"Untersuchungsausschuss ("NSA")." *Bundestag.de*. Deutcher Bundestag Web. 13 July 2015.

Van Aelst, Peter, and Jeroen van Laer. "Internet and Social Movement Action Repertoires. Opportunities and Limitations." *Information, Communication & Society* 13:8 (2010): 1146-1171. Web. 28 July 2015.

Vasseur, Flore. "The Woman Who Hacked Hollywood." *Medium.com*. Backchannel, 8 Apr. 2015. Web.

Vegh, Sandor. *Cyberactivism. Online Activism in Theory and Practice*. Ed. Ayers, Michael D., and Martha McCaughey. New York: Routledge, 2003. Print.

Wagenknecht, Addie, and Jillian York. "Art and Hacking in the Post-Snowden Age." re:publica, Berlin. 5 May 2015. Lecture.

"We Petition the Obama Administration to: Pardon Edward Snowden." *Petitions.whitehouse.gov*. The White House, 9 June 2013. Web. 28 July 2015.

"What is CryptoParty?" *Cryptoparty.in*. CryptoParty, 2015. Web. 27 July 2015.

"What is Open Source." *Opensource.com*. Red Hat, 2015. Web. 1 Aug. 2015.

"What is Wikileaks?" *Wikileaks.org*. WikiLeaks, 28 June 2011. Web. 8 Aug. 2015

"Who We Support." *Couragefound.org*. The Courage Foundation, n.d. Web. 28 July 2015.

Wilde, Sara. "From Stasi to NSA… And Back?" *Exberliner*. Sept. 2014: 20-21. Print.

Meeting the Privacy Movement
Dissent in the Digital Age

In the summer of 2013, whistleblower Edward Snowden leaked classified documents of the United States intelligence organization NSA to the press. The documents, of which the magnitude and scope were unprecedented, shocked many and caused an outrage among privacy activists worldwide.

At the time of the first publications a small group of individuals, consisting of security researcher Jacob Appelbaum, journalist Glenn Greenwald, WikiLeaks editor Sarah Harrison, and documentary filmmaker Laura Poitras, stood by Snowden's side. This group became part of a larger group of privacy activists, in which they started to take on the role of movement leaders. They are now focal points in a large web of privacy activists and organizations that as a whole forms the privacy movement, which shares Berlin as a central meeting place. The movement has three distinct ways in which it expresses dissent: whistleblowing, art, and protest.

Meeting the Privacy Movement. Dissent in the Digital Age identifies four elements that are characteristic to this movement: composition, leadership, meeting places, and dissent. With the help of social movement theory and these four elements it is explained how the group that initially helped Snowden fits into a larger group of privacy activists.