Deciphering Crypto-Discourse: Articulations of Internet Freedom in Relation to the State

Isadora Hellegren
Department of Art History and Communication Studies
McGill University, Montreal

August 2016

A thesis submitted to McGill University in partial fulfillment of the requirements of the degree of Master of Arts in Communication Studies.

© Isadora Hellegren 2016

Abstract

The understanding of what constitutes “Internet freedom” varies between countries and cultures. In Internet governance debates, a myriad of actors is invested in defining the meaning of “freedom” in relation to Internet-specific technologies. A central component in meaning-making processes about Internet-specific technologies and their functions is the constant negotiation of online rights, such as personal privacy and freedom of expression. In the process of these and other contestations over what should or should not constitute Internet freedom, this study explores how a specific community of participants in the Internet governance debate, namely public-key cryptography advocates, has constructed a discourse in which “crypto” (encryption software) serves as an enabler of freedom.

While the design of “crypto” aims to render online communication illegible to anyone but its intended recipient(s), the representation of crypto serves as a battlefield in a larger discursive struggle to define the meaning of Internet freedom. This thesis investigates how crypto-advocates, and in particular Cypherpunks, have articulated *crypto-discourse*: a partially fixed construction of meaning that establishes a relationship between “crypto” and a negative conception of Internet freedom, in relation to the state. I argue that crypto-discourse excludes other possible positive meanings of Internet freedom. In so doing, the discourse removes responsibility from democratic states to secure online rights and freedoms for their citizens.

To decipher crypto-discourse, I turn to three interrelated concepts central to Laclau and Mouffe’s theory of discourse, namely, *social antagonisms*, *empty signifiers*, and *logics of difference and equivalence*. I map key discursive events pertaining to the articulation of “crypto” among interrelated discourse communities of cryptographers, hackers, online rights activists, and technology journalists during a period of forty years (1975 – 2015). I present the crypto-discourse timeline as comprised of three periods: the *origins* (1975 – 1990), *crystallization* (1990 – 2000), and *revitalization* of crypto-discourse (2000 – 2015). For each period, I analyze key discursive artifacts such as political manifestos produced by Cypherpunks and journalistic accounts produced by *Wired* magazine technology reporters using the discourse theoretical concepts. Lastly, I argue that this strategic articulation of crypto is suggestive of myth-making. The implications of this research call for a more contextualized debate about the role of democratic governments in upholding privacy rights and freedom of speech online.

Resumé

L'interprétation de ce qui constituent les libertés sur Internet varie selon les pays et les cultures. Dans les débats sur la gouvernance de l'Internet, une myriade d'acteurs est impliquée dans la définition de la notion des « libertés » par rapport aux technologies spécifiques à Internet. Un élément central dans le processus de création de sens par rapport aux technologies spécifiques à Internet et de leurs fonctionnalités est la négociation constante des droits en ligne, tels que la vie privée et la liberté d'expression. Dans ce débat, ainsi que d'autres contestations sur ce qui devrait ou ne devrait pas constituer les libertés sur Internet, cette étude explore comment les partisans de la cryptographie, une communauté spécifique participant au débat sur la gouvernance de l'Internet, a construit un discours dans lequel « la crypto » (logiciel de chiffrement) sert en tant que facilitateur de la liberté.

Alors que la « crypto », vise à rendre les données intelligibles, sauf au(x) destinataire(s) souhaité(s), la représentation de la « crypto » est en proie à une lutte discursive plus large qui contribue à définir le sens même de la liberté sur Internet. Ce mémoire traite des partisans de la « crypto », en particulier les Cypherpunks, et comment ils ont articulé un *cryptodiscours* : une construction de sens partiellement fixé qui établit une relation entre la « crypto » et une conception négative de la liberté sur Internet en relation avec l'État. J'avance que le cryptodiscours exclut d'autres sens positifs de la liberté sur Internet. Ainsi, le cryptodiscours réduit la responsabilité des États d'assurer les droits et libertés en ligne de leurs citoyens.

Afin de déchiffrer le cryptodiscours, j'utilise trois concepts centraux de la théorie du discours de Laclau et Mouffe, à savoir les antagonismes sociaux, les signifiants vides ainsi que les logiques équivalentes et différentielles. Je cartographie les évènements essentiels du discours relatifs à l'articulation de la « crypto » au sein des communautés de discours interdépendantes de cryptographes, de pirates informatiques, de militants des droits de l'Homme en ligne ainsi que de journalistes pendant une période de quarante ans (1975 - 2015). Je présente la trajectoire du cryptodiscours comme composée de trois périodes : *l'origine* du cryptodiscours (1975 – 1990), la *cristallisation* (1990 – 2000), et la *revitalisation* du cryptodiscours (2000 – 2015). J'analyse des artéfacts clés du discours incluant des manifestes politiques produits par les Cypherpunks ainsi que des récits journalistiques produits par des reporters du magazine technologique *Wired*. En terminant, je soutiens que cette articulation stratégique de « la crypto » est un processus suggestif de construction du mythe. Les implications de cette recherche appellent à un débat plus contextualisé a propos du rôle des gouvernements démocratiques dans le respect des droits de la vie privée et de la liberté d'expression en ligne. Je présente la trajectoire du cryptodiscours comme composée de trois périodes : l'origine du cryptodiscours (1975 – 1990), la cristallisation (1990 – 2000), et la revitalisation du cryptodiscours (2000 – 2015). Pour chaque période, j'analyse des artéfacts clés du discours incluant des manifestes politiques produits par les Cypherpunks ainsi que des récits journalistiques produits par des reporters du magazine technologique *Wired*. En terminant, je soutiens que cette articulation stratégique de « la crypto » est un processus suggestif de construction du mythe. Les implications de cette recherche appellent à un débat plus contextualisé à propos du rôle des gouvernements démocratiques dans le respect des droits de la vie privée et de la liberté d'expression en ligne.

Acknowledgements

First, I would like to express my sincerest gratitude to my supervisor Professor Becky Lentz for her guidance. Lentz' unwavering commitment to my progress has been invaluable to the completion of this thesis. Moreover, her expertise in regards to discourse theory has been indispensible to my scholarly progression. I am also grateful for the financial support that enabled my attendance in a workshop dedicated to qualitative and interpretive methods in social science research, held by Professor Dvora Yanow.

I would like to thank Professors Darin Barney, Gabriella Coleman, and Marc Raboy in the Department of Art History and Communication Studies at McGill University, as well as Professor Fenwick McKelvey at Concordia University, for offering compelling seminars that I have had the privilege to attend. Their individual insights and intellectual support have contributed in shaping this project in several ways. In addition, these seminars have provided inspiring learning environments where I have been able to increase and challenge my knowledge significantly throughout my time at McGill University. I would therefore like to extend this gratitude to my fellow peers in these seminars, from whom I have also gained new perspectives.

I am grateful to Media@McGill for arranging talks of great relevance to my research interest. I am especially thankful for the Media@McGill Travel Grant that made it possible for me to attend summer school at Central European University in Budapest, in 2015. I also wish to acknowledge professionals and scholars whom I had the opportunity to meet during the course in Advanced Topics in Internet Governance, Civil Society, and Policy Advocacy at CEU. Their expertise in a broad variety of related topics informed my research by emphasizing the complexity of the issues at hand. They were also a truly formidable group of people whom I am happy to have met and that I hope to meet again.

I wish to express my appreciation for the support that I have received from my fellow peers in the Peer Writing Group offered by Graphos and led by Professor Donetta Hines. These meetings have provided useful feedback and helped me clarify my writing. I also sincerely thank my friend Sharon George for her endearing support and correction of a draft.

Finally, I would like to thank my near and dear. I would not have been able to accomplish this endeavour without the love and steadfast encouragement from my partner in life, Patrice, who also contributed to this thesis by helping me translate my abstract into French. I also want to thank my mother in Sweden for her unconditional love that surpasses the dimensions of the Atlantic Ocean. In addition, I thank Ratacat for his positive influence on my sentiments towards this writing process.

Table of Contents

Chapter 1: Introduction....1

Research Context....2

Previous Research on Cypherpunks and Crypto-freedom 14

Conclusion and Preview of Chapters 21

Chapter 2: Research Design: Theory and Method 25

Articulations of Social Antagonisms....26

Empty Signifiers....28

Logics of Differences and Equivalences....32

Crypto-Discourse Timeline 39

Chapter 3: The Origins of Crypto-Discourse (1975 – 1990)....46

The Role of the U.S. Government in Articulating Crypto 47

The Role of Cryptographers in Challenging the State's Articulation of Crypto....49

The Role of a Counterculture in Articulating Technology....52

Conclusion....57

Chapter 4: The Crystallization of Crypto-Discourse (1990 – 2000) 58

The Role of the U.S. Government in Politicizing Crypto-Advocates....59

The Role of The Cypherpunks in Establishing A Partial Fixation of Meaning 65

The Role of Technology Journalism in Popularizing Crypto....72

Conclusion....75

Chapter 5: The Revitalization of Crypto-Discourse (2000 – 2015)....78

The Role of the U.S. Government in Articulating Crypto Globally 79

The Role of New Uses of Crypto in Extending the Articulation of Crypto....80

The Role of Journalistic Accounts in Revitalizing Crypto-Discourse 88

Conclusion....92

Chapter 6: Conclusion 95

Bibliography 102

Appendix 117

Figures

Figure 1 The relationship between social antagonisms, empty signifiers, and logics of difference and equivalence in discursive struggles to partially fix meaning. 33

Figure 2 Logics of difference and equivalence at work in an empty signifier. 34

Figure 3 Crypto-discourse timeline (1975 – 2015): The evolution of discourse communities and key discursive events listed in Table 1. 40

Figure 4 Logics of difference and equivalence at work in the empty signifier “crypto”. 71

Figure 5 The cover of *Wired* Magazine 1.02 May/June 1993..73

Figure 6 The cover of *Wired* Magazine 22.09 September 2014. 92

Tables

Table 1 Crypto-discourse timeline: Key discursive events per discourse community as illustrated in Figure 3 (1975 – 2015). 117

Chapter 1: Introduction

In February 2016, the United States' Federal Bureau of Investigation (FBI) and the multinational technology company Apple Inc. enter into a public dispute regarding access to data residing in a specific iPhone. A court order requires the tech giant to create software that enables access to the digitally protected content of the deceased San Bernardino mass shooter's iPhone 5c (Lee, 2016; Lichtblau & Benner, 2016; Pagliery, 2016). In response, Apple CEO Tim Cook publishes a customer letter publicly opposing the government's request. Instead of complying with the court order, Cook advocates for the need for strong encryption to protect personal information.

Apple's response to the court order quickly becomes a matter of discussion in several media outlets. Whistleblower Edward Snowden tweets that: "The @FBI is creating a world where citizens rely on #Apple to defend their rights [to privacy], rather than the other way around" (Snowden, 2016), presenting Apple as a privacy rights defender. The *Economist* portrays Tim Cook as a "CEO-statesman", "an evangelist, out to persuade the world of the righteousness of his chosen causes" (On The Stump, 2016), emphasizing the power that the CEO of a technology company such as Apple holds in shaping public policy. Noted law professor Yochai Benkler on the other hand, states that the legal conflict between Apple and the FBI is not even a question of privacy vs. security. Instead, he argues that "It is a conflict about legitimacy" (Benkler, 2016), pointing out a democratic deficit in the lack of trust in and accountability of the National Security Agency of the United States. An article in the student-run *Harvard Kennedy School Review* correspondingly argues that "Apple's choice to publish a letter framing this issue as an encryption one is populism plain and simple" (Zylberberg, 2016), calling attention to the wrongful representation of the request as one that concerns encryption software. These statements are but a few examples of the many voices that compete in defining the meaning of this dispute concerning law enforcement's ability to access personal data.

The FBI vs. Apple order did not, as Zylberberg points out, require Apple to weaken its encryption algorithm that renders personal data on iOS-devices inaccessible to unauthorized parties. The dispute nevertheless reminded technology reporters of a series of legal battles that took place in the early 1990s, namely the Crypto Wars (Barrett, 2016; Froomkin & McLauglin, 2016). In the Crypto Wars, online rights advocates and the United States Department of Justice disputed the legal status of encryption software in court. Struggles to define the meaning of encryption software do not, however, only take place in courtrooms. They also take place in academic journals, conferences, online spaces, and in technology magazines where the representation of encryption software serves as a battlefield in a larger discursive struggle to define the meaning of Internet freedom.

Research Context

"Freedom" is an elusive concept. The understanding of what constitutes freedom varies between countries and cultures. "Internet freedom" is an equally amorphous notion that lends itself well to multiple normative interpretations of what the Internet should represent. In Internet governance debates, myriad actors are invested in defining the meaning of "freedom" in relation to Internet-specific technologies. Computer scientists, hackers, online rights advocates, journalists, scholars, technology entrepreneurs, and policy makers are among the many stakeholders that participate in imagining and shaping the meaning of freedom in the future of the Internet.

Stakeholders participate in these debates in several ways. Some design the architecture of the Internet. Social actors such as computer scientists, software developers, and hackers structure how information is exchanged over the Internet by writing protocols and algorithms. Examples of such protocols and algorithms are the Internet Protocol (IP) that determines how data are delivered, the BitTorrent protocol that allows for peer-to-peer file sharing, and the RSA algorithm, designed to protect data in transmission. Other actors, such as policy-makers on national and international level, seek to seek to define what constitutes appropriate online practices through policy regulation. Additional efforts to shape the future of the Internet include media representations of Internet-specific technologies, practices, and their users. Depictions of for example encryption software as a terrorist tool for communication, online file sharing as criminal activity associated with piracy, and hackers as villains stealing personal credit-card information communicate what constitutes (and what does not constitute) desirable online behaviour. Internet governance debates focus both on the technical architecture of the Internet, and "expressions of mediation over societal values such as security, individual liberty, innovation policy, and intellectual property rights" (DeNardis, 2013, p. 2) related to this architecture.

The architects of the Internet are not only responsible for shaping Internet-specific technologies, but also for constructing meaning through them in various ways that influence how hackers, software developers, online rights advocates, policy makers and others visualize, design, and use these technologies. The form and functions of technologies may have material impacts on their environment and sometimes unforeseen consequences by changing the way people commute, work, or interact (Winner, 1986). Nevertheless, someone's design or use of a technology like computer software is never inherently positive or negative (Pinch & Bijker, 1984).

Attempts to establish the meaning of various technologies are contingent on their particular historical and cultural contexts (DeNardis, 2013; Feenberg, 1999; Slack, 1989). Furthermore, these attempts to establish meaning can have material impacts as our understanding of Internet-specific technologies shape related policy-making. A recent example of how a specific group of stakeholders produces meaning in relation to Internet-specific technologies includes Tarleton Gillespie's analysis of how a discursive community of engineers strategically constructs the term "end-to-end" as a "descriptor of the structure of the Internet" (Gillespie, 2006, p. 430). Gillespie's analysis of journal and conference publications from the 1970s to the 1990s shows how engineers in the United States have constructed the term in a manner that allows it to encompass a plurality of meanings that integrate different political agendas, like a "symbolic umbrella" (Gillespie, 2006, p. 447). What is more, Gillespie suggests that the versatility of the term "end-to-end" has effected debates about copyright law and peer-to-peer file sharing: "end-to-end-ness, not the actual design of the network but the iconographic principle it represents and the egalitarian connotations it implies, may have suggested that file-trading would be unstoppable" (Gillespie, 2006, p. 448). Gillespie proposes that the engineers' strategic construction of the term end-to-end has implications for engineering debates and consequently policy regarding the structure of the Internet. Understanding *how* various stakeholders construct specific understandings in regards to Internet-specific technologies is therefore significant to Internet governance debates.

A central component in meaning-making processes about Internet-specific technologies and their functions is the constant negotiation of online rights, such as personal privacy and freedom of expression (DeNardis, 2013). *Crypto*, short for cryptography, refers to encryption software that renders online communication illegible to anyone but its intended recipient(s). The design of this computer software aims to keep communication private by concealing information from any third party trying to access it.[1] Different discourses in various contexts have long competed to establish the meaning of encryption. Actors have sought to construct the meaning of encryption by writing policy, writing cryptographic code, writing journalistic articles, and engaging in other practices to communicate understandings of the technology. For example, until the 1990s, the Unites States government classified encryption as war materiel, which made encryption algorithms illegal to export. Cryptographers, hackers, online rights advocates, and journalists alike have sought to challenge this meaning.

In 1991, cryptographer Phil Zimmermann developed the encryption software Pretty Good Privacy (PGP) and wanted to spread it to the public for political reasons. As the name Pretty

[1] Examples of widely used encryption software include by Phil Zimmermann's Pretty Good Privacy (PGP) in 1991, which is now the "global standard for e-mail encryption" (Bennett, 2008, p. 87) and its hybrid follow-up GNU

Good Privacy implies, as well as its hybrid follow-up GNU Privacy Guard (GPG), the developers closely associated encryption software with the right to privacy. In turn, hackers gathered online to develop and spread encryption software. Online rights advocates like the Electronic Frontier Foundation (EFF) fought a series of legal battles with the United States Department of Justice regarding the legal status of encryption. Technology journalists wrote about these events and popularized debates surrounding encryption software and their relationship to online rights. The various actors involved who politicized encryption software during the 1990s associated encryption technology with a right to online privacy.

The United Nations has more recently contributed to the debate about the relationship between Internet freedom and encryption software by presenting the technology as an essential tool to protect the human right to freedom of expression. The UN decided to extend human rights to the Internet as it declared that “the same [human] rights that people have offline must also be protected online” (United Nations, 2012, 2014). In addition, the United Nations Human Rights Council (UNHRC) has in recent years focused its attention towards questions regarding what constitutes the right to privacy and freedom of expression online (OHCHR, 2014). In 2015, UN Special Rapporteur on freedom of expression, David Kaye, presented a multi-stakeholder report on encryption, anonymity, and the human rights framework for online communication. He stated that encryption is essential to safeguard the human right to freedom of opinion and expression. In addition, nation states should not seek to implement so called “backdoors” or use other tactics that might weaken encryption and the protection of individuals’ online rights (United Nations, 2015). This report definitively establishes a direct relationship between encryption software and the human right to freedom of expression.

In the process of these and other contestations over what should or should not constitute Internet freedom, this thesis explores how a specific community of participants in the Internet governance debate, namely public-key cryptography advocates, has constructed a discourse in which encryption software serves as an enabler of freedom. Public-key cryptography (crypto) advocates encompass several communities that engage in different discursive practices. Cryptographers develop and publish encryption algorithms in academic journals and online. Hackers calling themselves Cypherpunks write code, but also promote the use and development of encryption through political manifestos and discussions on online mailing lists. Online rights advocates, such as the Electronic Frontier Foundation (EFF) work to resist government regulations on encryption software that seeks to either restrict access to the technology or weaken its functions. Technology journalists associated with *Wired* magazine write favourably about the cryptographers and hackers developing and spreading encryption software. While attempts to define the legal status of encryption software also deserve scrutiny, other attempts to advance an understanding of cryptography through discursive practices such as political manifestos and journalistic accounts receive far less attention. This thesis focuses specifically on the discursive work of the Cypherpunks and their political manifestos, which are at the core of what I refer to as "crypto-discourse", and technology journalists at *Wired* magazine who popularized the Cypherpunks' work through journalistic accounts.

Borrowing the concept of "crypto-freedom" from scholarship about hacker culture, I use the term *crypto-discourse* to refer to a partially fixed construction of meaning that establishes a relationship between crypto (encryption software) and a negative conception of freedom (Coleman & Golub, 2008).[2] By *negative* conception, I refer to an understanding of freedom that promotes individual freedom *from* state interference (Berlin, 1969; Laclau & Mouffe, 1985b; Tully, 2013). According to Isaiah Berlin's "Two Concepts of Liberty", "negative" liberty refers to "the liberty of non-interference", or non-coercion from an external actor, whereas "positive" liberty refers to a liberty of "self-mastery, self-realization, and self-government", and is subject to an external source of control, such as a state, which enables such freedom (Tully, 2013, pp. 24–25).[3] Various actors articulate the division of responsibilities within a given democratic society as positive and negative understandings of freedom in relation to the state (Laclau & Mouffe, 1985b). Members of the Cypherpunk community have actively advanced a meaning of crypto and freedom that positions the state as their adversary—an antagonist—in debates about online

[2] Gabriella Coleman and Alex Golub coined the term "crypto-freedom" in *Hacker Practice: Moral Genres and the Cultural Articulation of Liberalism* (2008). In this thesis, I build on their term crypto-freedom, which refers to a moral genre of hacker practices, to describe a discourse.

[3] An account that gives justice to the complexity of Berlin's concepts of liberty, as well as a discussion of the conceptual differences between the terms "liberty" and "freedom" is beyond the scope of this thesis. In this particular context I employ the terms interchangeably, as the objective of this study is not to unearth an underlying meaning.

privacy.[4] The Cypherpunks, a community devoted to the development and deployment of encryption software, gathered on the electronic *Cypherpunk Mailing List* in 1992 to discuss and develop crypto. Cypherpunks' strategies to advance crypto-freedom through purely technological means are of particular significance to other actors engaged in shaping the future of encryption policy. Yet the specific relationship between freedom and the state that Cypherpunks have articulated excludes other possible *positive* notions of Internet freedom in which the state has an *obligation* to ensure the protection of online rights.

Within this context of varying understandings of Internet freedom, the research question that guides this study of crypto-discourse is *how have crypto-advocates, and in particular members of the Cypherpunk community, articulated a discourse that defines Internet freedom in relation to the state?* The "*how*" in this question involves distinctive discursive practices over a period of forty years (1975 – 2015) through which Cypherpunks and technology reporters articulate crypto-discourse.

To be clear, in taking up Cypherpunks' crypto-discourse as my primary object of study, I am not critiquing the use and development of encryption software per se, as I contend that the functions of the technology do not hold an intrinsic (either positive or negative) value. Dissidents

[4] In this thesis, I do not distinguish between the concept of sovereign state and the concept of government due to their ontological statuses. I treat government as a physical representative of the concept of the state and use the terms interchangeably throughout the thesis.

can for example, if they have reason to fear prosecution by state authorities, require encryption software in order to denounce what they consider unjust acts carried out by oppressive regimes (Human Rights Foundation, 2013; United Nations, 2015).

Journalists may also require encryption software to protect sources who may be netizens, dissidents, or whistleblowers that threaten to expose the state's abuse of power. Glenn Greenwald, at the time reporter at the *Guardian*, and documentary film-maker Laura Poitras, used encryption in their communication with Edward Snowden as he disclosed confidential information about illicit mass surveillance practices in the United States and globally. In order to communicate safely, concerned dissidents may consequently depend on encryption software that does not reveal the content of their communication.

Others use encryption software to conceal the content of their communication for more nefarious ends. An example of such is the illegal exchange of child pornography through online hidden services on The Onion Router (Tor), an encryption based browser (Moore & Rid, 2016). The debate regarding the actual use and numbers of pedophiles versus the number of netizens with less maleficent intent using Tor hidden services continues to rage between crypto-advocates and government agencies (see Greenberg, 2015b). For these reasons, in my analysis of crypto-discourse, I do not take a normative stance regarding the deployment of encryption software. Instead, I seek to problematize how crypto-advocates advance a representation of encryption as an enabler of a *negative* conception of freedom. I contend that such a representation has normative implications for future policy regarding expectations on state authorities to uphold online rights.

In the chapters that follow, I argue that the discursive strategies employed by crypto-advocates, and in particular, by Cypherpunks, to articulate a relationship between encryption software and a negative conception of freedom (freedom *from* state interference) may overrun other possible, positive meanings of Internet freedom. Discursive strategies that articulate a negative conception of freedom may remove responsibility and accountability from democratic governments. Crypto-discourse presupposes individuals' responsibility to protect themselves and their online communication (through technological means) from undue interference from state authorities. This understanding does not emphasize the state's responsibility *not* to abuse its power in the form of mass or bulk surveillance of online communication. Nor does this negative conception of freedom call for mechanisms that would hold the state accountable if it did abuse its power as a democratically elected government. While strengthening individual rights to privacy, crypto-advocates' discursive strategies may actually serve to undermine efforts to construct a positive meaning of Internet freedom.

A positive meaning of Internet freedom based on democratic principles would require the state to *ensure* the protection of individual rights online. Such responsibility would also include installing appropriate independent verification mechanisms that would hold the state accountable for intrusions into online privacy. In this regard, I want to emphasize the contextual nature of interpretations of freedom. For example, the *Icelandic Modern Media Institute* (IMMI) was created in 2011 following the Icelandic parliamentary resolution, the *Icelandic Modern Media Initiative* ("About IMMI," n.d.). IMMI seeks to protect journalists and their sources by creating a legal data haven by combining selected freedom of expression and freedom of information laws, which are currently in place in other countries' legal systems, such as Sweden and Estonia

("About IMMI," n.d.; Hirsch, 2010). In this instance, IMMI represents an interpretation of a *positive* Internet freedom, as government action *enables* the protection of journalists whose role it is in liberal democracies to serve as watchdogs of government.

The Icelandic case of IMMI illustrates how the state seeks to ensure that mechanisms of power and control are in place to *uphold* democratic principles of transparency, accountability, and public participation, while also safeguarding personal data. Although the ideas of freedom of expression and information expressed by IMMI relate to those articulated in crypto-discourse, the positive understanding of freedom represented by IMMI is culturally and historically specific.[5] This contextual specificity is critically important in regards to understandings of freedom, as international organizations are increasingly harmonizing global communication policy in the name of counter-terrorist efforts (Braman, 2011).

A deeper understanding of strategies used by crypto-advocates such as the Cypherpunks to construct crypto-discourse should be significant to researchers in political science, policy studies, and science and technology studies, as well as to decision-makers in governments and

[5] IMMI founder Birgitta Jonsdottir is a member of the Icelandic Pirate Party. The politics of the Pirate parties are related to the use of peer-to-peer file sharing technology and originated in Sweden in 2006, a country which first legislated on Freedom of Information in 1766 (Beyer, 2014; Burkart, 2014). The file sharing protocol BitTorrent was created by Cypherpunk Bram Cohen (Greenberg, 2012b). Birgitta Jonsdottir works closely with Cypherpunk and WikiLeaks founder Julian Assange, and has previously been a WikiLeaks spokesperson.

international organizations working on the politics and policy of online rights and encryption software. In addition, Cypherpunks' strategies to advance a conception of Internet freedom should be of interest to researchers in political communication, discourse studies, and cultural studies who are seeking to understand how communities that develop software, such as the Cypherpunks, also participate in constructing a social imaginary about the future of the Internet.

By conceptualizing "crypto-freedom" in discourse-theoretical terms, this thesis advances an understanding of the particular functions of crypto-discourse as a social practice that shapes public policy. This study also catalyzes reflection on how a specific community of stakeholders (cryptographers, hackers, online privacy advocates, and technology journalists) actively work to construct a specific meaning of freedom—one that is free *from* government involvement in the protection of online communication—in relation to technology and the role of the state. An enhanced understanding of these stakeholders' meaning-making practices in regards to Internet specific technologies like public-key encryption is relevant to hackers, programmers, and policy-makers alike. All of these actors are involved in constructing the form, function, and meaning of the future of the Internet and its relation to the state. This understanding of how various actors construct meaning through Internet-specific technologies is also of importance to the everyday Internet user whose online rights and relationship to the state is at stake. Discourse theory provides conceptual tools that help advance this enhanced understanding.

Previous Research on Cypherpunks and Crypto-freedom

Scholars who have studied hacker communities such as the Cypherpunks and the discursive practices in which they engage have primarily looked at what unites them as communities and how they engage in negotiating meaning about technology, freedom, and the state. Practices related to Internet specific technology and shared social imaginaries prove essential to meaning-making processes for these communities.

Cultural anthropologists Gabriella Coleman and Alex Golub coined the term “crypto-freedom” to both identify and describe a form of hacker practice as a moral genre (Coleman and Golub, 2008). Drawing on Russian literary theorist Michael Bakhtin’s concepts of speech genres and heteroglossia (Bakhtin, 1981, 1986), they describe the heterogeneity of hacker practice by providing a topography of hacker moral genres; (1) crypto-freedom; (2) free and open source software and; (3) the hacker underground. With this topography and the support of events, technologies, characters, and socio-technical artifacts, the authors demonstrate the complexity of a genre’s formation. Genres are for example not fixed and they overlap, as hackers move between various moral expressions “changing moral registers the way a multilingual speaker switches from one language to another” (Coleman & Golub, 2008, p. 258). A hacker that writes encryption software may also believe that the source code that he or she is developing should be free to others to use and improve, according to practices of the moral genre of free and open source software. The Gnu Privacy Guard (GnuPG or GPG) for example is software that employs the Pretty Good Privacy (PGP) encryption standard. GPG is also “free” software, licensed under the GNU General Public License, allowing anyone to freely use, distribute, or modify the software as they see fit (Free Software Foundation, 2007). Hackers thus constantly engage in negotiating the meaning of freedom through different moral expressions: “Indeed, elaborating a sense of what freedom is and what it means to be free constitutes moral discourse for hackers” (Coleman & Golub, 2008, p. 256).

Coleman and Golub compare hacking to similarly varied and oftentimes contradictory expressions of American and Anglo-European liberalism. Their treatment of liberalism, not as an ideology or a philosophy, but as a heteroglossic practice that is under constant renegotiation, contributes to an understanding of liberal ideas, such as individualism, free speech, and privacy, as organic and contingent concepts that do not exist independently from each other, or from historical and cultural contexts. In addition, they use philosopher Charles Taylor’s notion of an “expressive self” (Taylor, 1989) to explain how liberal ideas are continuously articulated, renegotiated, and realized through these moral genres. The authors contend that liberal ideas are central to hacker ethics, and visible in every-day hacker practices and articulations. Coleman and Golub conclude that hacking is then, like liberalism, a “cultural sensibility with diverse and sometimes conflicting strands” and should be considered an ethically diverse process that converges with other social and political events (Coleman & Golub, 2008, p. 256).

By outlining the moral genre of “crypto-freedom”, Coleman and Golub illustrate how a negative understanding of freedom and a commitment to online privacy rights is rooted in the historical and cultural context of liberalism in the United States. The authors explain how Cypherpunks and other crypto-advocates in the United States who participated in creating the concept of crypto-freedom, are not politically bound to either left or right political ideologies. Instead, they share a negative understanding of freedom commensurate with Berlin’s conception of negative liberty (Berlin, 1969, 1969). This articulation of freedom, is present in various "material and semiotic artifacts" (Coleman & Golub, 2008, p. 270) and shows that Cypherpunks distrusted authority and agreed that government and corporations should not intrude on their personal privacy online (Coleman and Golub, p. 260). Besides this shared understanding of freedom in relation to authority, Coleman and Golub argue that what actually unites Cypherpunks as a discourse community, is a Cypherpunk's belief that this freedom should primarily be achieved through the development and use of encryption technology online (Coleman & Golub, 2008).[6]

Anthropologist Christopher Kelty similarly emphasizes the role of such a shared affinity with Internet specific technologies, as well as a shared social imaginary as elements that unite hackers. However, Kelty makes a deliberate choice not to use the term "hacker" in his work on free software and the people and practices surrounding it (Kelty, 2005, 2008). He contends that the term is "semantically overdetermined" (Kelty, 2008, p. 35). Overdetermination is a discursive concept that Kelty uses to claim that even if there are other definitions of the term "hackers", the term carries a negative connotation which suggests that hackers are "subversive and/or criminal" (Kelty, 2008, p. 35). Instead, Kelty chooses to use the term "geek" when referring to the social actors involved in his study, but he employs it in a way similar to Coleman and Golub to indicate

[6] Gabriella Coleman and Alex Golub do not refer to Cypherpunks as a discursive community but as participants of a moral genre.

"a mode of thinking and working, not an identity" (Kelty, 2008, p. 35). His major contribution to cultural studies of hacking is the notion of "recursive publics" to describe what unites geeks.

For Kelty, recursive publics are groups "constituted by a shared, profound concern for the technical and legal conditions of possibility for their own association" (Kelty, 2005, p. 135). In other words, these publics share a concern for their main mechanism for communication: the Internet and Internet specific technologies. Kelty focuses on issues related to practice, ideology, and imagination to find out how geeks relate to free and open software, and to each other. Also drawing on the work of Charles Taylor (Taylor, 2004), Kelty explains that hackers share a moral and technological imagination of the Internet as infrastructure and order. The means of communication, including the "creation, modification and maintenance of software, networks and legal documents" (Kelty, 2008, p. 8) are consequently as relevant to hacker practices and imaginaries as speech itself (Kelty, 2005). These publics are then, in Kelty's words, "the builders and imaginers of this space" (2008, p. 29). This notion of a shared social imaginary can also function as a political strategy among hacker communities.

According to others researching Internet-specific culture and technology, scholars McKelvey and Beyer, the discursive practices of digital pirates and their antagonistic relationship to the state serve as an example of how a shared social imaginary can be understood as political strategy to popularize "state-evading communication infrastructures" (McKelvey & Beyer, 2015, p. 891). McKelvey and Beyer outline crucial events in the history of digital piracy and its politics, including the development of file-sharing networks associated with online piracy such as the Napster application, BitTorrent protocol, and online torrent index The Pirate Bay (TPB). The authors conclude that the use of these technological infrastructures "evades the state's administrative gaze to observe and its judicial arms to control" (McKelvey & Beyer, 2015, p. 894). Moreover, the use of file-sharing networks also challenges existing laws on intellectual property and copyrights.

This antagonism between file-sharers and the state sometimes leads to legal prosecution. For example, the TPB administrators, Peter Sunde, Fredrik Neij, and Gottfrid Svartholm Warg have all been convicted of advocating copyright infringement. McKelvey and Beyer trace artifacts such as *The Cypherpunk Mailing List* that contain articulations of a political philosophy arising prior and parallel to state-evading file sharing technologies closely associated with ideals of decentralized forms of organization. The Cypherpunks, McKelvey and Beyer argue, "became particularly articulate in expressing the link between state evasion and computer networks" (McKelvey & Beyer, 2015, p. 895). In this way, the articulation of a relationship between crypto and a negative conception of freedom served as a political strategy to promote not only crypto, but also other state-evading communication infrastructures such as peer-to-peer technologies.

McKelvey and Beyer also highlight the use of pirate lore as a method to spread an anarchist understanding of crypto. Drawing on sea pirate imagery, the means by which communities of "activists, libertarians, and anarchists" (McKelvey & Beyer, 2015, p. 894) articulated the state as an antagonist include the *Cypherpunk Mailing List* and "The Crypto Anarchist Manifesto" (May, 1992). For instance, in response to the recording industries' attempt to conjure up an image of the 18th century pirates by using the jolly roger to declare online file sharing as a criminal act to combat copyright infringement, these hacker communities "reappropriated the image of a romanticized swashbuckling pirate" (McKelvey & Beyer, 2015, p. 895).

Another example of the use of piracy lore are the numerous discussions on the Cypherpunk Mailing List of anarchist Hakim Bey and his references to anarchist forms of association and state-evading practices as characteristics of the eighteenth century pirates. In his book *The Temporary Autonomous Zone* (T.A.Z.), Bey refers to stories of anarchist pirate utopias to describe contemporary online spaces as new forms of pirate spaces (Bey, 2001; McKelvey & Beyer, 2015). These pirate tales thus played a significant role in the construction of a social imaginary among Cypherpunks.

McKelvey and Beyer note that while pirate imagery inspired Cypherpunks, the freedom-oriented discourse of the Cypherpunks inspired contemporary digital piracy practices. Cypherpunks imagined communication infrastructure that did not yet exist, including forms of peer-to-peer technology as a means to avoid state surveillance (McKelvey & Beyer, 2015). Following several projects such as Napster and Mojo-Nation, former member of the Cypherpunk Mailing List, Bram Cohen, developed the decentralized file-sharing protocol BitTorrent (2001). Today, BitTorrent represents a large part of all Internet traffic. Similar to the Cypherpunks who popularized crypto by featuring the cover of *Wired* magazine, “digital pirates not only seek to create state-evading communication infrastructures, but their politics aspire to make these infrastructures as popular as possible” (McKelvey & Beyer, 2015, p. 891).

The Swedish art and activist collective The Pirate Bureau intended to spread a philosophy of free information sharing and created The Pirate Bay in 2003, which in 2014 was still the most popular BitTorrent search engine available (Van der Sar, 2014). The philosophy that accompanied the development of file-sharing technology also inspired the creation of a nonaffiliated political party in 2006, the Pirate Party, that later spread to countries all over the world (Beyer, 2014; Burkart, 2014; Schwarz et al., 2015).

The ways that pirates, geeks, and hackers identify as members of communities vary broadly. While some use one of these terms to refer to themselves, perhaps to proudly assert their piratehood associated with their political involvement (Beyer, 2014), others may only consider themselves or others to be pirates during the short moment when they participate in online piracy by illegally downloading a movie on the Internet (Andersson, 2011; Dahlberg, 2011; Schwarz et al., 2015). Others move between practices, rendering hacking a term that encompasses a multitude of various practices that cannot be reduced to a simple binary (Coleman & Golub, 2008). In addition, others who may engage in the same practices, reject hacking as a term based on negative connotations (Kelty, 2008). Although hackers are not united by a fixed identity, their identity formations are related to their common practices and consequently constructions of shared social imaginaries. For sake of consistency and clarity, I will hereafter use the term “hacker” throughout this thesis, to refer to members of communities that unite in their practices of developing and modifying internet-specific technologies.

Hackers’ technology-related practices are crucial to understanding what unites hackers as communities, either through Coleman and Golub’s topography of moral genres, Kelty’s recursive publics, or McKelvey and Beyer’s state-evading piracy practices. All of these practices are constitutive of how hackers engage in constructing a shared meaning of internet-specific technologies, freedom, and the state. Furthermore, Kelty considers technology-related practices to be forms of political action that “can both express and ‘implement’” ideas about the social and moral order of society” (Kelty, 2008, p. 8). Hacker practices are therefore discursive practices through which hackers construct a shared understanding of freedom (Coleman & Golub, 2008), a shared social imaginary of conditions of association (Kelty, 2008), and a political philosophy that functions to further spread the meaning and use of a specific technology, for example through the use of pirate imagery (McKelvey & Beyer, 2015).

Conclusion and Preview of Chapters

In this chapter, I have consulted research that addresses how hackers and related groups engage in meaning-making processes in order to foreground significant discursive practices that unite them as communities. This thesis builds on the work of the afore-mentioned researchers to further investigate from a discourse theoretical perspective how crypto-advocates, and in particular Cypherpunks, articulate visions of the future of the Internet in relation to the state. All of the scholars already mentioned emphasize the importance of hackers' relationship to Internet specific technologies such as encryption, shared cultural affinities, values, as well as the importance of visions of the future. Their scholarship outlines the historically and culturally specific conditions that structure the environment in which the actors studied produce and interpret meaning. For example, Coleman and Golub explain that the moral genre of crypto-freedom has a cultural and historical particularity and that it reflects values that are in various ways codified in the United States' national constitution (Coleman & Golub, 2008, p. 261). This work provides insight into the historical and cultural conditions pertinent to my analysis of crypto-discourse.

My analysis of crypto-discourse draws upon a particular area of discourse theory, namely, the work of Laclau and Mouffe (Laclau & Mouffe, 1985c), to add to our understanding of the functions of the meaning-making practices relating to encryption software. In the chapters that follow, I explore what discursive strategies crypto-advocates have used to articulate a relationship between encryption software and freedom. In addition, I illustrate how these strategies function to exclude other possible meanings of freedom that include the state. To do this, I investigate *how crypto-advocates, and in particular members of the Cypherpunk community, have articulated a discourse that defines Internet freedom in relation to the state.* This question is important to our understanding of how political actors use their articulation of encryption software to construct an understanding of the state as an antagonist in meaning-making processes pertaining to the future of the Internet. Such an articulation excludes other possible positive meanings of freedom in which the state must secure online rights and freedoms for its citizens.

In Chapter 2, I introduce my theoretical framework in which I draw on Laclau and Mouffe's conception of discourses as inherently political constructions. I introduce three concepts central to my exploration of how crypto-advocates have articulated crypto-discourse: *social antagonisms*; *empty signifiers*, and; *logics of differences and equivalences* (Jørgensen & Phillips, 2002; Laclau, 1996; Laclau & Mouffe, 1985c). I also outline the trajectory of crypto-discourse as comprised of three periods: *the origins*, *crystallization*, and *revitalization* of crypto-discourse.

In Chapter 3, I focus on the first period, the *origins* of crypto-discourse, to establish the historical context in which the interrelated concepts introduced in the previous chapter set the stage for the crystallization of crypto-discourse. I address the role of the United States government in the 1970s as the primary actor with power to define crypto in a time of war and a rising political opposition. I then discuss how cryptographers at MIT and Stanford establish a relationship between crypto and privacy through academic publications, consequently challenging the state's dominance over the definition of crypto. Furthermore, the chapter reviews the rise of a counterculture that includes discourse communities of journalists, communalists, and entrepreneurs in San Francisco who articulate a relationship between technology and freedom that excludes the state. These events serve to illustrate the emergence of crypto as an empty signifier within a larger discursive struggle for the future of Internet freedom.

In Chapter 4, I focus on the second and most distinct period of construction of crypto-discourse, namely its crystallization. The chapter identifies foundational moments in Cypherpunk history and the articulation of crypto-discourse that occur in direct response to government actions during the 1990s. Examples of such moments are the development and spread of Pretty Good Privacy (PGP) together with the formation and interrelated discursive strategies of the Electronic Frontier Foundation (EFF), the Cypherpunk movement, and *Wired* magazine. I further illustrate how crypto-advocates and in particular Cypherpunks employed the logics of difference and equivalence in their articulation of crypto as an empty signifier, through the passage of social antagonism that was set up during the previous period. This serves as segue to Chapter 5, which describes the last of the three periods in the evolution of crypto-discourse covered in this thesis, namely its revitalization.

Chapter 5 addresses how Cypherpunks and technology reporters at *Wired* magazine draw on and rearticulate the crystallized form of crypto-discourse from previous period to revitalize it in a global context. I begin by identifying the role of the U.S. government in reinforcing an anti-terrorist legal discourse that impacts global communication policy following the terrorist attacks on September 11, in 2001. I then discuss the formation of two organizations that offer new uses of encryption software, namely The Onion Router (Tor), emanating from MIT crypto-scientists, and WikiLeaks, established by Cypherpunk Julian Assange. Tor, WikiLeaks, and their applications of encryption challenge anew the state's claim to define crypto, by articulating a relationship between crypto and journalistic practices. I also discuss journalistic accounts from *Wired* reporters and WikiLeaks' Editor-in-Chief, Julian Assange featuring Cypherpunks, WikiLeaks, and Edward Snowden. These accounts reinforce previously articulated differences and equivalences by reinvigorating discursive work from the crystallization period of crypto-discourse. This final analysis leads me to my closing Chapter 6 where I discuss the relevance of these findings and their pertinence to future policy relating to the use of encryption software.

Chapter 2: Research Design: Theory and Method

In this chapter, I introduce my theoretical framework and the objects that I have selected for my analysis of crypto-discourse. In order to investigate how Cypherpunks with a negative understanding of freedom articulate a relationship between "crypto" and "freedom" and how this articulation functions as crypto-discourse, I draw on Laclau and Mouffe's conception of discourses as inherently political constructions (Laclau, 1996; Laclau & Mouffe, 1985c).

The chapter proceeds as follows. First, I present Laclau and Mouffe's conception of discourse to illustrate how I apply it as a way to decipher crypto-discourse. I then introduce three concepts central to my exploration of how crypto-advocates' use of crypto-discourse works in practice: *social antagonisms*; *empty signifiers*, and; *logics of differences and equivalences* (Jørgensen & Phillips, 2002; Laclau, 1996; Laclau & Mouffe, 1985c). I review these concepts to demonstrate their utility in my analysis of how crypto-advocates have constructed crypto-discourse. Then, I bring forward the discursive artifacts that constitute my objects of analysis. These include key artifacts produced by cryptographers, hackers, and technology reporters that articulate and popularize crypto-discourse during a period of forty years (1975 – 2015). I conclude this chapter with an illustration of how this period represents three pivotal moments in the evolution of the crypto-discourse, namely the *origins, crystallization,* and *revitalization* of crypto-discourse.

I adopt Laclau and Mouffe's conception of *discourse* as referring to partial, temporary, and contingent fixations of meaning that constitute social reality. Discourses are the results of *articulatory practices* that are inherently political struggles (Laclau & Mouffe, 1985a). Social actors engage in articulatory practices in attempts to construct partial fixations in meaning (Howarth, 2000; Laclau & Mouffe, 1985a). In order to construct partial fixations in meaning, social actors must exclude other possible meanings, as it is impossible to fully fixate meaning of the total. Social actors are consequently always involved in attempts to construct the social by seeking to make it appear natural, i.e. not constructed, but as something that holds meaning in and of itself.

By performing discourse analysis on what I refer to as crypto-discourse (a partially fixed construction of meaning that establishes a relationship between crypto (encryption software) and a negative conception of freedom), I seek to understand *how* crypto-advocates, and in particular Cypherpunks, have sought to construct social reality "so that it appears objective and natural" (Jørgensen & Phillips, 2002, p. 33). In order to decipher crypto-discourse, I turn to three interrelated concepts central to Laclau and Mouffe's theory of discourse namely social antagonisms, empty signifiers, and logics of difference and equivalence. In what follows, I summarize each of these concepts and indicate, for each, their relation to my study of *Cypherpunks'* articulation of crypto-discourse.

Articulations of Social Antagonisms

Social antagonisms, Laclau and Mouffe explain, are "the 'experience' of the limits of the social" (Laclau & Mouffe, 1985a, p. 105). Therefore, social antagonisms are central to discourse theory that seeks to uncover the historically contingent and political conditions and functions of meaning making process, rather than an inherent meaning, or "interpretations actors give to their practices" (Howarth, 2000, p. 11). From Laclau and Mouffe's discourse theoretical perspective, all meaning-making processes are political discursive struggles. In these struggles to determine meaning, actors articulate social antagonisms.

Articulations are "not the name of a *given* relational complex" (Laclau & Mouffe, 1985a, p. 93), but practices in which social actors construct relationships between each other, or between themselves and objects, by excluding other possible relationships. Antagonisms are therefore different from oppositions and contradictions, as both of these concepts refer to relationships between two totalities with already established identities. Instead, antagonisms presuppose that the relationship between two subject positions is obstructing the fulfillment of identity: "The presence of the "Other", prevents me from being totally myself" (Laclau & Mouffe, 1985a, p. 105). In other words, articulations of social antagonisms take place in discourses where social actors experience that their identities cannot be fulfilled due to this "Other".

I adapt these ideas in my analysis of crypto-discourse by examining how crypto-advocates construct obstacles to their identity (Howarth, 2000, p. 105). In constructing crypto-discourse, Cypherpunks articulate a social antagonism towards the state, excluding the state as a possible enabler of freedom. Through this process, the same actors construct identity, such as "Cypherpunk" and collective social imaginaries, such as "crypto-freedom". According to Cypherpunks, the state is the "Other" preventing them from being who they really are: from being free to act and communicate without state interference. Consequently, I argue that crypto-advocates such as the Cypherpunks "construct an 'enemy' who is deemed responsible for this 'failure'"(Howarth, 2000, p. 105).

Conceptualizing crypto-advocate and Cypherpunk practices as articulations of social antagonism helps us understand the functions of crypto-discourse. This construction of a social antagonism towards the state functions to unite crypto-advocates' various political aspirations, to construct their identity, and to construct an understanding of the future of the Internet where the meaning of freedom excludes the state.

Empty Signifiers

Another concept that Laclau and Mouffe develop in relation to social antagonism is the notion of an empty signifier. *Empty signifiers* are sites where we can see discursive struggles between competing discourses that seek to define meaning take place (Jørgensen & Phillips, 2002; Laclau, 1996; Marchart, 2012). Empty signifiers – not groups – hence constitute the minimal unit of analysis within both micro (cultural) and macro (political) level studies, as they hold together discourses (Marchart, 2012).[7] To understand how crypto-advocates have constructed crypto-discourse, I examine how they have emptied the signifier "crypto" of its

[7] Oliver Marchart develops this statement based on Laclau's theory of populist reason. He explains that "it is deeply flawed" to consider a group as the primary unit of analysis as this presupposes an assumption that there is "an underlying or fundamental reality beyond or before the process of discursive articulations" (Marchart, 2012, p. 8).

particular meaning as a specific technology, and then, how they filled it and consequently universalized their own particular meaning of freedom, while excluding other possible meanings.

Informed by linguist Ferdinand de Saussure's contributions to semiotics, Laclau and Mouffe employ the concepts of *signifier* to indicate an object or a concept – such as the word "crypto" – and *signified*, the object or concept to which the signifier refers – such as the functions and features of encryption software. Meaning-making agents establish meaning in *signs* – the sum of the signifier and the signified – by including some meanings and excluding other possible meanings. The determined meaning will always be relative to other possible meanings that are excluded in the process of signification.

The meaning of the sign "freedom" for instance, is relative to what actors such as the Cypherpunks determine is *not* freedom, through the exclusion of other possible meanings (Jørgensen & Phillips, 2002, p. 26). Some signs are more recurring and undetermined than others are, as many signs are centered on these recurrent signs and gain meaning only in relationship to them. These signs are called "nodal points" (Laclau & Mouffe, 1985b), or "floating" (Hall, 1996) and "empty" signifiers (Barthes, 1972), depending on the stage they are in within a process of articulation.[8]

[8] Stuart Hall conceptualizes "race" as a floating signifier, where race functions as a construction that perpetuates dominant power relations between people with different skin colour (Hall, 1996).

To describe the processual relationship between nodal points, floating, and empty signifiers, I draw on the following definitions. *Nodal points*, such as “freedom” and “democracy”, are “privileged signs” in relation to which a cluster of other signs gain their meaning (Jørgensen & Phillips, 2002, p. 36). Nodal points are also *floating signifiers*, because nodal points are especially prone to be at the heart of a discursive struggle for meaning (Jørgensen & Phillips, 2002, p. 28). In cases when a nodal point does become a site of struggle, it can become an empty signifier. *Empty signifiers* are signs that competing discursive articulations strategically seek to empty of their particular meaning to temporarily fill and fix with another, universal meaning, that excludes other possible meanings – in which case they would become nodal points.

The concept of empty signifiers lends itself well to understand Internet-related debates. While advancing intertextuality as a theoretical approach to study policy change, Becky Lentz (2013) provides an example of how definitions in policy debates over net neutrality serve as critical nodal points. Lentz states that the term “neutral” functions in a similar manner to an empty signifier in the historicity of the net neutrality debate. Lentz identifies “neutrality” as a “nodal textual artifact” (p. 579) and provides a close examination of the Federal Communications Commission’s (FCC) 2002 Declaratory Ruling. By tracing how the term has evolved throughout policy artifacts, Lentz situates the ruling “within a larger discursive struggle” (Lentz, 2013, p. 580) that is taking place in regulatory practices regarding telecommunications policy in the United States.

In another example, Joscha Wullweber (2015) accounts for a strategic transformation of the meaning of “nanotechnology” to identify the construction of definitions of the word over time. Wullweber describes how various actors, namely Research & Development (R&D) institutes such as the US National Nanotechnology Initiative (NNI) and the White House, have strategically transformed the empty signifier “nanotechnology” into a universal signifier in order to advance political agendas that align with interests of global economic competition (Wullweber, 2015). By analyzing policy development over a period of 15 years, Wullweber provides examples where actors exclude other possible meanings from the dominant definition. The author locates the very moment where the US National Nanotechnology Initiative (NNI) associates nanotechnology with the “universal interest of US society” (Wullweber, 2015, p. 85), in a press release from the White House. He also situates an instance when the NNI actively excludes the original particular meaning in favour of another more universal meaning that encompasses a multitude of possible meanings, such as nanobiotechnology and nanomedicine. In so doing, Wullweber guides the reader through key discursive moments in which social actors strategically reconstruct the meaning of nanotechnology.

Lentz’ and Wullweber’s studies illustrate the applicability of the concept of empty signifiers to understand the contingency of meaning-making processes in Internet-related debates. The authors show how social actors strategically seek to advance their own political objectives in meaning-making processes. Consequently, these studies emphasize the necessity of situating empty signifiers in their historical context to understand their evolution over time. This approach has informed my research design.

In this thesis, I conceptualize “crypto”, short for cryptography, as an empty signifier. Cryptography refers to the study of methods to send secret, or encrypted messages, and encryption to the methods that render communication illegible for anyone but its intended recipient. Encryption software then refers to the software that renders online communication illegible for any third party, or adversary, that would try to intercept it. Crypto, as an empty signifier, has taken on multiple possible meanings of “freedom”, which are beyond the features of the specific technology. Crypto-advocates have emptied crypto of its particular meaning and filled it with a meaning that unites different political objectives through the construction of a social antagonism.

To understand how Cypherpunks have constructed a crypto-discourse, I examine how they have emptied the signifier “crypto” of its particular meaning as a specific technology by seeking to fill it with a universal meaning of freedom. Through this process, the logics at play in empty signifiers reveal the circumstances of specific cases of identity formation, such as the construction of the Cypherpunk subject, and attempts to construct collective social imaginaries, such as a vision of the Internet freedom that excludes the state.

Logics of Differences and Equivalences

The logics at work in empty signifiers are particularly useful concepts to understand how Cypherpunks articulate a relationship between “crypto” and “freedom”. There are two logics at work in empty signifiers: (1) The *logic of difference*, which is expressed through processes of exclusion of other possible meanings, and (2) the *logic of equivalence,* which unites various struggles that may differ in their objectives. The logics of difference and equivalence that are at work in the empty signifier function simultaneously through the passage of antagonism (Figure 1).

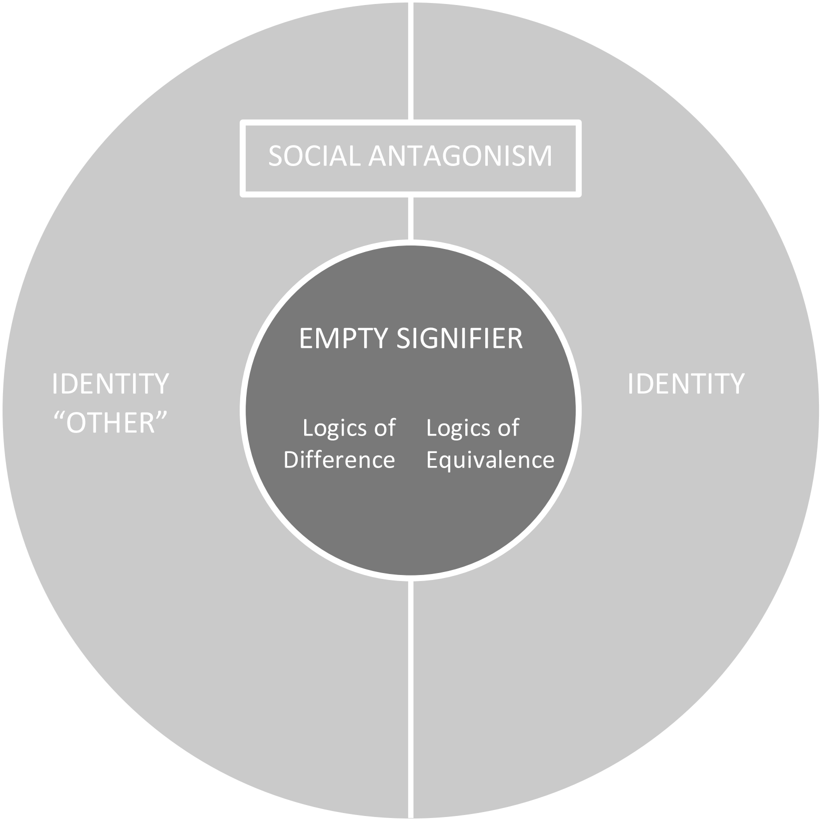

Figure 1 The relationship between social antagonisms, empty signifiers, and logics of difference and equivalence in discursive struggles to partially fix meaning.

Figure 1 illustrates the relationship between social antagonism, empty signifiers, and logics of difference and equivalence. The empty signifier is a site of struggle based on social antagonism in which the logics of difference and equivalence are at play. Through the passage of antagonism, actors construct identity through a shared political objective that they determine in relation to the "Other", whom they experience prevents their identity from being fulfilled. A full circle of identity is not possible, as all meaning-making processes are discursive struggles and it is impossible to fully fixate meaning of the total. As social actors engage in articulatory practices that construct social antagonisms, the logics of difference and equivalence are simultaneously at work in the empty signifier.

Figure 2 shows *how* the logics of difference and equivalence work simultaneously in an empty signifier through the construction of chains of equivalence.

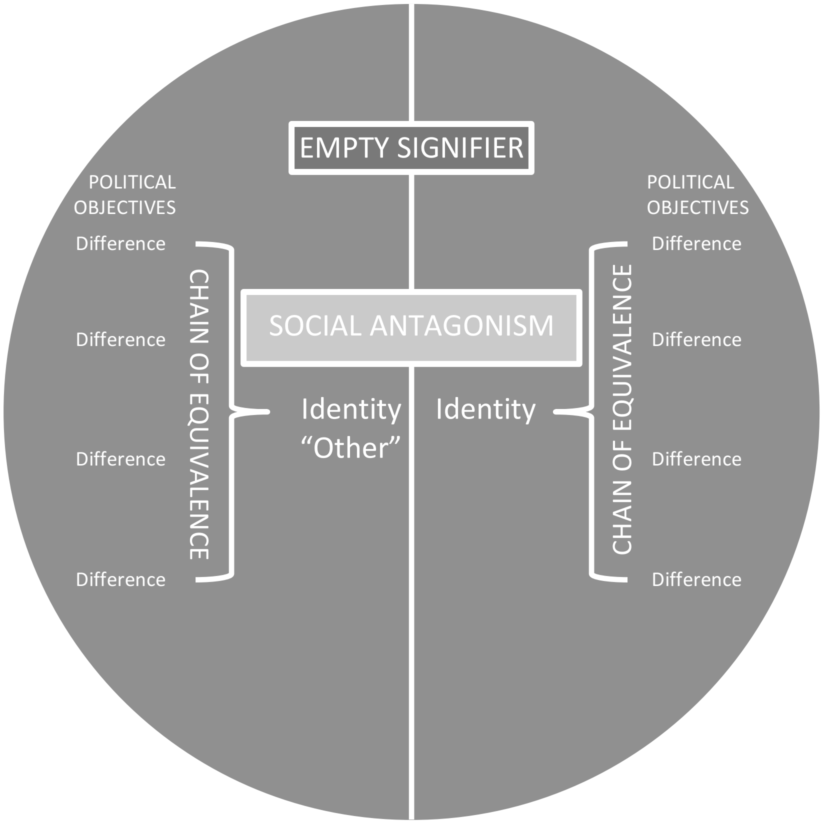

Figure 2 Logics of difference and equivalence at work in an empty signifier.

A *chain of equivalence* is a series of differential political objectives represented through one term, such as "crypto", behind which they become equal. The logic of difference excludes other possible meanings from the empty signifier while the logic of equivalence make differential political objectives (indicated in figure 2 as “difference”) appear equivalent when opposed to a significant difference, an antagonist (indicated in figure 2 as “Other”), such as a suppressive government (Laclau, 1996). Differential objectives thus only appear equivalent – form chains of equivalence – when opposed to an “Other”, who represents an obstacle to the fulfillment of the differential political objectives. The delineation of an “Other” thus unites differential political objectives through the construction of chains of equivalence.

Chains of equivalence and social antagonisms function to construct partial and contingent social identities, such as “pirate”, “hacker”, and “Cypherpunk”, as well as to universalize a political objective, such as “crypto-freedom”. In this thesis, I focus primarily on the latter. In order to articulate a universal objective, such as a negative freedom enabled by the use of encryption software, articulations must strategically exclude other possible meanings, such as a positive freedom enabled by the state (Marchart, 2012). The empty signifier “crypto” is thus the result of articulations of such chains of equivalence and exclusions of meaning.

An example of research that employs the logics of difference and equivalence to deconstruct a discourse is available in Norval’s (1996) work on Apartheid discourse. Norval draws on what she refers to as the logics of exclusion and inclusion to describe and explain the rise and dominance of the Apartheid project, a politically implemented system of segregation in South Africa during the second half of the twentieth century (Norval, 1996). Identity construction of the South African subject during the rise and prominence of Apartheid occurred through discursive processes of exclusion, drawing limits that separated the South African society into different groups and constructed “others”.

The logics of inclusion were simultaneously at play as they served to construct a shared social imaginary. Norval illustrates the functions of these logics with an in-depth analysis of the articulation of “Afrikanerdom”. Apartheid supporters articulated a social imaginary in the vacuum left after events that unsettled the common understanding of reality which had previously dominated South Africa during the nineteen thirties and forties. An example is how the churches and intellectuals at Potchefstroom University articulated a Calvinist Christian nationalism, using conceptualizations of freedom and equality that would inform a new worldview. Norval also analyzes statements and arguments of political propaganda, and she concludes that the nationalist president Diederichs’ conceptualization of nationhood was an important universalizing influence that would facilitate the creation of a “mythical space” that Apartheid discourse could occupy (Norval, 1996, p. 81). Norval thus outlines how articulations of social antagonism, empty signifiers, and logics of difference and equivalence were at work in Apartheid discourse.

Drawing on theory and method in Norval’s work, I employ logics of difference and equivalence to observe how empty signifiers operate in crypto-discourse. Coleman and Golub point out that Cypherpunks’ “pessimism regarding the intrusive nature of government” and “suspicion of the industrial military complex falls as easily within the libertarian Right as it does a certain anti-military Left-pacifism […] As a result, crypto-freedom practices, groups and events include people with divergent political viewpoints” (Coleman & Golub, 2008, p. 260). The logic of difference hence functions to conceptually separate the Cypherpunks from their antagonist, the State, by excluding the state from the meaning of crypto. The logic of equivalence works simultaneously to unite varying political objectives of Cypherpunks and make them appear equivalent when confronted with the constructed antagonist, the state.

The logics of difference and equivalence allow me to distinguish particular discursive strategies that Cypherpunks use in crypto-discourse. Methmann's study on climate discourse (2010), for example, argues that international organizations in charge of climate protection, strategically engage in a hegemonic discourse that is characterized by a "consistent inconsistency" (Methmann, 2010, p. 346). He contends that by writing and implementing policy in the name of the empty signifier "climate protection", organizations such as the World Trade Organization (WTO), International Monetary Fund (IMF), the World Bank, and the Organization for Economic Cooperation and Development (OECD), exclude meanings of "climate change" and "global warming" from the climate discourse.

In similar fashion, Andreja Vezovnik (2013) outlines what she refers to as linguistic operations in her analysis of the representative discourse of the "Erased" in Slovenia. The Erased refers to individuals who were deprived of their Slovenian citizenship in 1992 when the Slovenian Ministry of Interior Affairs removed their names from the Register of Permanent Residence. Vezovnik argues that NGOs, academics, critical journalists, and others have strategically articulated the representational discourse of the Erased. This discourse, she continues, is "firmly grounded" (p. 608) in the empty signifiers of "human rights" and "democracy". Vezovnik thus shows how the actors in her study make use of logics of difference and equivalence in empty signifiers in a manner that removes agency from the Erased.

Other constructors of discourse may be displacing responsibility from themselves or others (Methmann, 2010; Offe, 2009). Similar to how Methmann explains that actors in charge of climate protection successfully deflect their responsibility using discursive strategies, Offe (2009) puts forward that the term "governance" is a strategic construction that removes responsibility from international organizations, nation-states, or any other actors presumably involved in governance processes. Offe (2009) argues that the term “governance” functions as a concept that is used to “bridge and blur the differences” between theoretical distinctions that are usually employed in social sciences, such as between structures and processes, between public and private, and between political and economical activity (Offe, 2009, p. 553). Offe’s three main criticisms towards governance as a theory deconstruct the concept by demonstrating its limits, its inconsistencies, and its depoliticizing effects. Instead, governance is associated mainly with positive words, which Offe argues, “suggest[s] that ideological, premature and undifferentiating harmonization is one function of the concept and its discursive use” (p. 551).

All of these scholars identify instances where actors empty the signifier at hand of its particular meaning in order then to fill it with a more universal meaning that excludes other possible meanings. In this process, actors form a shared partial identity and a shared universal objective. The discursive strategies that actors employ can function to disempower groups or to remove responsibility and accountability from actors involved. In this way, logics of difference and equivalence prove helpful in outlining discursive strategies that allow these articulations to appear objective, or true.

The above-mentioned studies also provide insights for how I frame my research process in this project. Similar to Lentz and Wullweber, I apply the concept of an empty signifier to an Internet-related discourse. I locate the social antagonism in which crypto (as an empty signifier) emerges as a response to events and ideas that take place and circulate primarily in California, USA, in the 1970s. I subsequently trace transformations of crypto over a period of forty years (1975 – 2015). In order to do this, I employ the logics of difference and equivalence to analyze key discursive artifacts in which crypto-advocates, and in particular Cypherpunks, attempt to construct social reality through crypto-discourse.

Crypto-Discourse Timeline

In my analysis of crypto-discourse, I map key discursive events pertaining to the articulation of “crypto”—in relation to freedom—among interrelated discourse communities of cryptographers, hackers, online rights activists, and technology journalists during a period of forty years (1975 – 2015). Based on interrelations between different discourse communities and discursive events during specific times, I distinguish in Figure 3 an evolution of crypto-discourse over three distinct periods: the *origins* (1975 – 1990), the *crystallization* (1990 – 2000), and the *revitalization* (2000 – 2015).

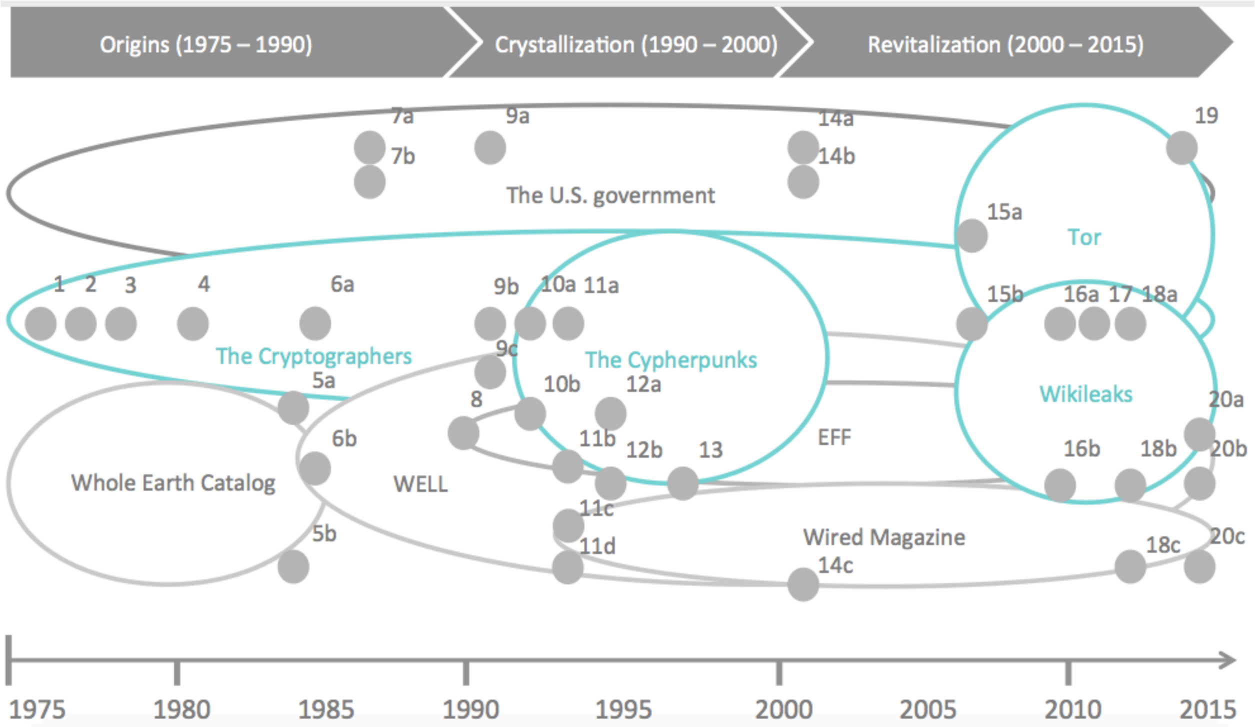

Figure 3 Crypto-discourse timeline (1975 – 2015): The evolution of discourse communities and key discursive events listed in Table 1.

The timeline in Figure 3 illustrates overlapping discourse communities that form and evolve from 1975 to 2015 in relation to key discursive events (see Table 1 Appendix for list of discursive events) which members of these communities have produced during this period. The timeline portrays the different communities with the help of four different colours; *dark grey* represents the State (U.S. government); *medium grey* represents online rights activists (Electronic Frontier Foundation (EFF)); and *light grey* represents technology journalists (Whole Earth Catalog, WELL, and *Wired* magazine). The grey dots indicate key discursive events in vicinity to the discourse communities in which they take place.

Discourse communities, like hacker moral genres or recursive publics described in Chapter 1, are bound together through their discursive practices that govern the rules and conditions for meaning-making processes within them (Coleman & Golub, 2008; Kelty, 2008; Swales, 1990). Throughout the history of crypto-discourse, cryptographers (MIT, Stanford), hackers (Cypherpunks), online rights advocates (EFF), technology journalists (*Wired)*, and other crypto-advocates have used different practices to instil meaning in the concept of public-key encryption software. These actors have developed algorithms, presented at conferences, written political manifestos, and written journalistic accounts to name a few of the discursive practices that unite them in various discourse communities.

Members of a discourse community may, however, engage in different practices at different times. A cryptographer can for example publish an encryption algorithm in an academic journal that will be read by other scientists in the same discourse community, and later file a lawsuit regarding the legal status of that algorithm. Similarly, a hacker who mainly writes code may also engage in journalistic practices in order to spread that code. The circles that separate discourse communities in Figure 3 are therefore not definitive. In hacker communities, technology-related practices are nevertheless central to their construction of a shared social reality internet-specific technologies, freedom, and the state (Coleman & Golub, 2008; Kelty, 2005; McKelvey & Beyer, 2015). Some practices are therefore more prominent and hence descriptive of a community, than others.

In this thesis, I focus particular attention on the discursive work of Cypherpunks as well as technology journalists at *Wired* magazine (blue and light grey circles in Figure 3) and how their discursive practices have sought to establish meaning in the empty signifier “crypto”. The Cypherpunks only formally formed in 1992 (number 10b in Figure 3), but several events led up to their formation as a discourse community and others reinvigorated their discourse at later stages. As I have noted from previous research on the subject (Coleman & Golub, 2008; McKelvey & Beyer, 2015), the empty signifier crypto is present in several artifacts, notably political manifestos and journalistic accounts that have been influential in and outside of the Cypherpunk discourse community.

The figure outlines some of the discursive artifacts produced by cryptographers, Cypherpunks, online rights advocates, and technology journalists in relation to major events pertinent to the history of crypto-discourse, such as technology and policy development, as well as community formations. The timeline begins with a publication that introduced public-key cryptography to the academic cryptographic community in 1976 (number 1 in Figure 3). This period constitutes the *origins* of crypto-discourse, as cryptographers began to challenge the state's definition of encryption software. In the early 1990s, the empty signifier crypto emerges as a site of struggle between competing discourses and new discourse communities form out of the cryptographic community and the countercultural Whole Earth network (see number 8, 10b, and 11c in Figure 3). This period represents the *crystallization* of crypto-discourse as Cypherpunks and technology reporters employ the logics of difference and equivalence in political manifestos and magazine articles and books to construct a negative understanding of freedom (see number 10a, 11a, 13, and 14c in Figure 3). The timeline ends with an issue of technology and culture magazine *Wired* that features whistleblower Edward Snowden in 2014 (number 20a in Figure 3). During this last period, crypto-advocates *revitalize* crypto-discourse from the crystallization period in a new global context. As the struggle over the meaning of encryption software expands, the discursive practices previously exemplary of the variety of communities overlap notably. During and after the Snowden leaks for example (number 19, 20a, and 20b in Figure 3), Edward Snowden uses encryption software to disclose state secrets in order to reveal state mass surveillance among a number of countries worldwide. In so doing, the former CIA contractor engages in practices that intersect with State, online rights advocates', hackers and cryptographers', and technology journalists' discursive practices. This timeline thus provides a brief overview of the complexity and contingency of crypto-discourse.

My primary objects of analysis include political statements written by self-acclaimed Cypherpunks that articulate a relationship between "crypto" and an understanding of freedom that they define in relation to the state (number 10a, 11a, 12a, and 18b in Figure 3). The Cypherpunks who wrote these statements intended to communicate their political objectives of the group. The statements include but are not limited to Tim C. May's "The Crypto-Anarchist Manifesto" (1992), and Eric Hughes' "A Cypherpunk's Manifesto" (1993), which they published on the *Cypherpunk Mailing List*. The time and location for publication of these manifestos is significant for their relevance as examples of primary objects of analysis in this study, since the Cypherpunk Mailing List served as the main means of communication for Cypherpunks when they formed as a discursive community. The manifestos have been widely distributed in the mailing list, over the Internet, and been republished in book collections (Ludlow, 1996, 2001). I have therefore selected these artifacts among others as key products of the discursive practices central to their discourse community. In order to understand how crypto-discourse expanded beyond the Cypherpunk community, I turn to technology journalism.

No account of crypto-discourse would be complete without turning to the role of acclaimed technology journalists (included in Whole Earth network, WELL, and *Wired* discourse communities in Figure 3), especially Steven Levy, and his role in constructing crypto-discourse

(Levy, 1993, 1994b, 2001). The second category of objects includes covers, articles, and books produced by Steven Levy and other *Wired* reporters that feature prominent crypto-advocates (number 5b, 11d, 14c, 18c, and 20c in Figure 3). These journalistic accounts popularize and perpetuate crypto-discourse through articulations related to the production and circulation of the primary artifacts. Among the accounts are *Wired* magazine article *Crypto Rebels* (11d) from 1993 and the accompanying front cover featuring the three founders of the Cypherpunks: Tim May, Eric Hughes, and John Gilmore (11b). This article spread crypto-discourse to a large readership and popularized it (McKelvey & Beyer, 2015). The book *Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age* (number 14 in Figure 3) from 2001 also constitutes an important artifact of crypto-discourse due to its representation of crypto and crypto-advocates. I have selected these journalistic artifacts because of their direct relationship to the crypto-movement, their capacity to reach out to a large readership and their participation in constructing and sustaining crypto-discourse. Through this diverse, but by no means exhaustive collection of discursive artifacts, I identify discursive strategies at work that crystallize crypto-discourse in the 1990s. Due to the contingent nature of discourse however, I also analyze these artifacts in relation to other contextual discursive events over time.

* * *

In this chapter, I have introduced my theoretical framework and the crypto-discourse timeline. Based on key discursive events, I have presented the evolution of crypto-discourse as comprised of three periods: the *origins, crystallization,* and *revitalization* of crypto-discourse. In the following chapters, I situate these key discursive events in their historical and cultural contexts in order to illustrate their centrality to crypto-discourse. Throughout the chapters, I turn to the concepts of articulations of social antagonism, empty signifiers, and logics difference and equivalence to decipher the discursive strategies at work during the origins, crystallization, and revitalization of crypto-discourse.

Chapter 3: The Origins of Crypto-Discourse (1975 – 1990)

In the previous chapter, I outlined three key concepts that I apply to my analysis of the trajectory of crypto-discourse as comprised of three periods: the origins, crystallization, and revitalization of crypto-discourse. These concepts are articulations of social antagonisms, empty signifiers, and logics of differences and equivalences. In this chapter, I focus on the first period: the origins of crypto-discourse. This period establishes the historical context in which these three interrelated concepts set the stage for the crystallization of crypto-discourse described in Chapter 4.

The chapter proceeds as follows. First, I address the role of the United States government in the 1970s as the primary actor with power to define crypto. At this time in history, the U.S. government considered crypto to be munitions and it was illegal to export it. I situate the state as the creator of the Internet within the historical context of the Cold War, the Vietnam War, and rising political opposition to the government's actions in relation to these wars. I present this historical and political perspective of the role of the U.S. government in order to illustrate the context in which crypto-advocates articulate a social antagonism towards the state.

Next, I describe the discursive work of MIT and Stanford cryptographers who develop cryptographic methods that further secure online communication third party access. Through publications in scientific journals, these cryptographers articulate crypto in relationship to privacy. In so doing, while simultaneously making their cryptographic methods available for a wider scientific community, they challenge the state's dominance over the definition of crypto. This articulation represents the move that will allow crypto to become an empty signifier.

Third, I cover the rise of a counterculture, exemplified in particular by the Whole Earth ‘Lectronic Link (WELL), a discourse community of journalists, communalists, and entrepreneurs in San Francisco who turned to technology as a means to achieve societal change. Through their publications in a Bulletin Board System (BBS), an online messaging board, the WELL articulated a relationship between technology and freedom that excluded the state. Technology reporter Steven Levy significantly added to this articulation through his writing on hackers. This articulation became crucial to the production of crypto-discourse as members of the hacker community (including cryptographers) and the Whole Earth network met and merged.

I conclude the chapter with an overview of how the aforementioned events and practices led to the genesis of crypto as an empty signifier within a larger discursive struggle for the future of Internet freedom. This conclusion serves as segue to the second of the three periods in the evolution of crypto-discourse covered in Chapter 4.

The Role of the U.S. Government in Articulating Crypto

The United States government had the historical upper hand when it came to defining the meaning of crypto. The concept of encryption as a process to render communication illegible for a third party precedes the notion of a sovereign state; Internet-specific encryption, however, does not. Before the 1970s, encryption was used by the military-industrial complex and was defined by the U.S. government as war materiel. During this period, the United States was involved in the Cold and the Vietnam Wars.

The Cold War era was a significant period for the state to create a public understanding of new technologies that it developed primarily in relation to the war. Edwards describes the Cold War era in the U.S. to be characterized by a “closed world discourse” (Edwards, 1997). The closed world discourse was closed he argues, as it was capable of encompassing all political struggles taking place in that context. Because the potential horrors of the Cold War were too abstract to grasp, they could only be understood in the minds of people through their “metaphorical and cultural dimensions” (Edwards, 1997, p. 14). Consequently, discursive practices and strategies in the form of metaphors, simulations, and fictions reflecting the dangers of nuclear weapons, the power of centralized control, and computers “had, in an important sense, more political significance and more cultural impact than the [nuclear] weapons that could not be used” (Edwards, 1997, p. 14). Similarly, Barbrook emphasizes the importance of world exhibitions in spreading public social imaginaries of the future intricately entangled with Cold War technology. Through conferences such as the World Expo in New York in 1964, the U.S. government and corporations such as IBM presented technology related to the Cold war as progressive inventions.[9] According to Barbrook, “the weaponry of genocide [nuclear reactors, rockets, and computers] “had been successfully repackaged into people-friendly products”

[9] IBM, the largest computer mainframe manufacturer at the time, received funding from the U.S. government to develop computers in military purposes (Barbrook, 2007).

(Barbrook, 2007, p. 34) in relation to space travel and artificial intelligence. In this context, the U.S. government developed the predecessor to the Internet, ARPNET, for military purposes.

The State, as a state in war, held the power to define the meaning of the Internet and Internet-specific technology. This included cryptographic algorithms (ciphers), which are mathematical instructions used in encryption systems, such as symmetric encryption, that intend to conceal communication exchanged over the Internet. *Symmetric encryption* describes an encryption system in which two parties share an encryption algorithm and a key to communicate. Through this method, the two parties commonly described by cryptographers as “Alice and Bob” (Schneier, 1996), can encrypt messages between one another using the same key to decrypt them. If a third party gets access to the symmetric key, the communication would no longer be kept secret. This constitutes a problem, or a weakness, as the purpose of encryption is to conceal communication. When cryptographers offered a solution to this problem in 1975, they also offered opposition to the state’s previously unchallenged position as the sole actor to define the meaning of crypto.

The Role of Cryptographers in Challenging the State’s Articulation of Crypto

Cryptographers at prestigious U.S. universities challenged the state’s dominant position in defining encryption, when they made their research available to a broader scientific community through conferences and academic journals. Stanford University cryptographers Whitfield Diffie and Martin Hellman proposed a theoretical solution to the old cryptographic problem of symmetric key management, namely public-key (asymmetric) encryption. *Public-key encryption* proposes two sets of keys instead of one, one public and one private key, one to encrypt and one to decrypt. Diffie and Hellman presented their proposed solution at the *National Computer Conference* and by publishing *New Directions in Cryptography* in an engineering journal (number 1 in Figure 3), introducing it to the scientific community in 1976 (Diffie & Hellman, 1976a, 1976b; Schneier, 1996). Diffie and Hellman also defined the problem that they addressed as an issue not of security, but: “the best known cryptographic problem is that of privacy” (Diffie & Hellman, 1976a, p. 29). In 1978, MIT computer scientists Ron Rivest, Adi Shamir, and Leonard Adleman published *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,* an article that described the RSA algorithm, making the concept of public-key encryption possible to implement (number 3 in Figure 3). In their publication Rivest, Shamir, and Adleman state:

> The era of “electronic mail” [10] may soon be upon us; we must ensure that two important properties of the current “paper mail” system are preserved: (a) messages are *private*, and (b) messages can be *signed*. We demonstrate in this paper how to build these capabilities into an electronic mail system. (Rivest, Shamir, & Adleman, 1978, p. 120)

Rivest, Shamir, & Adleman articulate a relationship between encryption and privacy by likening online communication to the postal service, designating privacy as a property of that system. In so doing, they extended the notion of security, as used in military contexts to include privacy, a concept that pertains to individual freedoms or rights codified in law. This articulation offered a new interpretation of encryption to a larger community of researchers.

The cryptographers did not only make public-key encryption algorithms available within their discourse communities of fellow computer scientists and cryptographers, but also made the concepts accessible to a broader public through a popular technology magazine. Martin Gardner, known for his ability to explain mathematical problems to a general audience, spread the word about this cryptographic system by explaining it in his column “Mathematical Games” in the popular technology magazine *Scientific American*, in 1977 (number 2 in Figure 3). Gardner described the algorithm as: “A new kind of cipher that would take millions of years to break” (Gardner, 1977), making it appear indestructible. These publications did not only seek to define encryption, but also helped popularize it. An increased popular interest in encryption constituted the beginning of a larger challenge to the state’s definition of encryption as war materiel.

One cryptographer in particular politicized the meaning of crypto by presenting it as a means to divulge personal identity in direct opposition to the state. An active supporter of the 1980s Crypto conferences, David Chaum politicized crypto and articulated a social antagonism towards the state as he proposed systems of anonymity to “make big brother obsolete” (Chaum, 1981, 1985) (number 4 and 6a in Figure 3).[10] In what would become widely influential writings among hackers and cryptographers, Chaum established a relationship between anonymity,

[10] The first International Cryptology Conference, “Crypto”, took place in California, in 1981. Berkeley cryptographer David Chaum set up the non-profit International Association for Cryptologic Research (IACR) at the second Crypto conference (“History of IACR Conferences and Workshops,” n.d.).

privacy, and security. Through journal articles such as *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms* (1981) and *Security Without Identification: Transaction Systems to Make Big Brother Obsolete* (1985), Chaum introduced anonymous transaction systems that would lay the conceptual foundations of decentralized digital payment systems such as cryptocurrencies. These anonymous transaction systems, he argued, would prevent corporations and the government from collecting and misusing information about individual behaviour. This way, these systems could enhance personal privacy and security through anonymity. Chaum hence positioned the state as the third party: the adversary from which private communication must be protected. By referring to government and large corporations as Big Brother, Chaum further portrayed the state as the antagonist. In addition, Chaum provokingly suggested that with the help of these systems, Big brother would no longer be needed, threatening the very legitimacy of the state's existence. With Chaum's contributions, the cryptographers now offered an alternative conceptualization of crypto in which the technology should be used to protect personal communication, instead of state secrets.

The Role of a Counterculture in Articulating Technology

During the origins of crypto-discourse, many American citizens began to express discontent with their government's actions in the ongoing Vietnam War. This discontent had become even stronger a few years earlier following military analyst Daniel Ellsberg's leaks of the so-called "Pentagon Papers": top-secret documents that revealed government wrongdoings in relation to the war. In response to the public's dwindling faith in the state apparatus, a countercultural movement that sought to oppose the hierarchical and rigid structures of the cold war military complexes took shape (National Archives, n.d.).

The Whole Earth network portrayed technology as a countercultural force in and of itself (Turner, 2006). Stewart Brand founded the *Whole Earth Catalog* in the 1960s in San Francisco that featured technology reviews. The magazine functioned to form a local discourse community during a time when large numbers of Americans turned to the countryside to form communes. Members of the network did not seek to achieve social change through traditional political means. Instead, they turned towards technology, commerce, "and the transformation of consciousness as the primary sources of social change" (Turner, 2006, p. 4). The Whole Earth network united in their celebration of high technology and a decentralized whole system of collaboration inspired by cybernetics (Turner, 2005). According to technology journalist Steven Levy, hackers also united through these shared values.

In 1984, technology journalist Steven Levy published *Hackers: Heroes of the Computer Revolution* (number 5b in Figure 3) that reverberated throughout the Whole Earth network and among the cryptographers. This largely influential book described early hacker culture at MIT, later Californian hacking cultures and a "Hacker Ethic", which constituted a set of "concepts, beliefs, and mores" that Levy considered shared among hackers (Levy, 1984, p. 27). This ethic includes the ideal of computers as machines that are not only able to teach you about the world, but can ultimately make your life better. The concept also encompasses a belief that access to both computers and information should be unlimited: "all information should be free" (Levy, 1984, p. 28). In addition, the ethic includes the encouragement to "Mistrust Authority – Promote Decentralization" (Levy, 1984, p. 29), to name a few of the tenets.

Through his book, Levy accomplishes several things. First, he articulates a representation of the hacker as a hero, a protagonist presupposing an antagonist. Levy depicts hackers as revolutionaries and liberators, “who lived the magic in the computer and worked to liberate the magic so it could benefit us all” (Levy, 1984, p. x). He also elevates the role of computers as the (magical) tool that enables the heroes to accomplish their “revolution” against authority. Government, corporations, and all institutions representative of bureaucracy represent obstacles hindering hackers from living out their “exploratory impulse” (Levy, 1984, p. 29). Bureaucracy is built upon “arbitrary rules” (Levy, 1984, p. 29), contrary to the “real” rules, which is the logic upon which computers operate. Levy thus articulates, through his accounts of hackers and their Ethic, a relationship between freedom (from arbitrary man-made rules of bureaucracy) and computers (logical, mathematical, and magical tools that enable freedom).

Although many that called themselves hackers did not agree with all of these tenets (Brand, 1985), Levy’s book has been widely influential. For example, the book was the inspiration for hackers from the Homebrew Computer Club, Steven Levy, members of the Whole Earth network such as Stewart Brand and Kevin Kelly (future founder of *Wired* magazine) and entrepreneurs of the San Francisco tech community to organize the Hackers’ Conference in 1984 (Brand, 1985; Malcolmson, 2016). The Hackers’ Conference (number 5a in Figure 3) serves as an illustration of how influential Steven Levy’s journalistic book was in bringing members of the communities together. Consequently, his representation, not limited to hackers, but also computers, and freedom, became a central topic of discussion. In one of the discussions about Levy’s Hacker Ethic, Stewart Brand modified the tenet that “information should be free”, to instead argue that “information wants to be free” (Brand, 1985), attributing to information a will of its own, a form of necessity. This representation of information recurred at several occasions in the following period of crypto-discourse and was later revoked by the Cypherpunks. Although the attendees at the Hackers' Conference disputed Levy's statements, his books brought members of hacker communities and the Whole Earth network together.

In 1985, the Whole Earth network's members gathered on the Whole Earth 'Lectronic Link (WELL), one of the first Bulletin Board Systems (BBS) that would host an online community (number 6b in Figure 3). The WELL included entrepreneurs, journalists, and hackers and from left and right, and many of them had participated in the Hackers' Conference (Turner, 2006). The design of the list followed "a countercultural conception of community and a cybernetic vision of control" (Turner, 2006, p. 143). The articulated relationship between self-governance (freedom from the form of centralized control represented by the state) and computers resonated with the expressed values that had brought together the Whole Earth network and the computer enthusiasts present at the Hackers' Conference. The WELL, as a computer conferencing system, allowed its users to start discussion topics as they wished and to respond to each other's posts in a decentralized manner.[11]

The creation of this computer conferencing system coincided both with the broadening of accessibility to what would constitute the Internet, as well as with restrictions on what was legal to do on the Internet. In 1986, The National Science Foundation connected their network, the

[11] Designed by Larry Brilliant, Network Technologies International (Turner, 2006).

NSFnet, with ARPANET (Malcolmson, 2016). This became the Internet, connecting university and research networks together, broadening the scope of who used the "network of networks" beyond the U.S. government (National Science Foundation, n.d.). Although mainly accessible to academics, non-academic tech savvy hackers also explored the possibilities of the Internet. At the same time, the U.S. government extended the definitions of what constituted illegal online activity in the Computer Fraud and Abuse Act (CFAA) (number 7b in Figure 3). This act criminalized much hacker activity, including accessing computers and networks without authorization (Wong, Silvers, & Opsahl, 2003). These restrictions received much attention on the WELL.

A factor that contributed to the popularity of the WELL and its content was the celebrity status of some of its members. John Perry Barlow was the lyricist of the band the Grateful Dead and his fans followed him to the WELL. Barlow shared his story of how the FBI, in their attempt to police computer fraud, increasingly went after hackers using new technology such as bulletin board systems (Sterling, 1992). In so doing, Barlow brought the network's attention to a rising tension between those who wanted to have a "free" Internet – one free from the barriers put up by government, and the government itself, which had directed its forces towards what it defined as new forms of crime: computer crime. In the 1990s, this battle would transform into a series of legal battles using crypto as their battlefield.

Conclusion

In this chapter, I have shown how the Cold War and the United States' war in Vietnam are of historical relevance to the origins of crypto-discourse as each event influenced cryptographers' and countercultural movements' articulation of the state as a social antagonist. Furthermore, I have delineated key articles published in scientific journals that articulate new encryption solutions in relation to privacy as a problem rather than security. I have also included a column in popular technology magazine *Scientific American* as it renders encryption algorithms accessible to the public outside of the academic realm. Lastly, I have introduced the Whole Earth Network as a discourse community along with the journalistic work of Steven Levy, which brought together hackers from the scientific community, hackers outside of it, and the Whole Earth network. Furthermore, I have illustrated how this journalistic work advanced a vision of technology as an enabler of freedom, excluding the state from its definition. These articulations of social antagonism provide the conditions in which crypto can emerge as an empty signifier.

In the next chapter, I present the period of crystallization of crypto-discourse by reviewing the events and discursive work that solidifies crypto-discourse during the early 1990s. This discourse is primarily articulated by a particular crypto-community, the Cypherpunks, that arises out of politicized cryptographers, and by the technology magazine *Wired*, that emerged out of the WELL.

Chapter 4: The Crystallization of Crypto-Discourse (1990 – 2000)

In the previous chapter, I explained the origins of crypto-discourse and established the historical context in which the interrelated concepts—articulations of social antagonisms, empty signifiers, and logics of differences and equivalences—introduced in Chapter 2 set the stage for the crystallization of crypto-discourse. In this chapter, I focus on the second and most distinct period of crypto-discourse, namely its crystallization. My purpose is to demonstrate how crypto-advocates, and in particular Cypherpunks, employed the logics of difference and equivalence in their articulations of crypto as an empty signifier through the passage of social antagonism that was set up during the origins of crypto-discourse.

This chapter proceeds as follows. First, I describe how a series of computer enthusiasts stemming from the cryptographic community and the Whole Earth Network politicized cryptography in a direct response to government actions. Political actions include Phil Zimmermann's dedication to developing and spreading Pretty Good Privacy (PGP) encryption to the public, the formation of the online civil liberties organization the Electronic Frontier Foundation (EFF), and the formation of the Cypherpunk movement during the so-called Crypto Wars. These wars were comprised of a series of legal battles regarding the status of encryption software. All of these events: the development and spread of PGP, the formation of EFF, and the formation of the Cypherpunk movement are interrelated as discursive strategies that draw on the social antagonism that the cryptographers and WELL members constructed.

Next, I focus on specific instances of the discursive work of the Cypherpunks that includes the Cypherpunk electronic Mailing List and their political manifestos published on the listserv. I show how through these artifacts, the Cypherpunks articulated their varying political objectives and identity through the logics of difference and equivalence, in direct relation to the empty signifier *crypto*. I illustrate the functions of the logics of difference and equivalence in establishing chains of equivalence in the empty signifier in Figure 4.

Lastly, I describe the discursive work of *Wired* magazine, also a product of WELL (described in Chapter 3), and how it popularizes crypto-discourse. I feature the three founding members of the Cypherpunks on cover of the second issue of *Wired* in 1993: John Gilmore, Eric Hughes, and Tim C. May. This publication, together with later journalistic accounts by *Wired* reporter Steven Levy, and the Cypherpunk Mailing List, constitutes foundational moments in Cypherpunk history and the articulation of crypto-discourse. Each event illustrates how Cypherpunks constructed a shared social imaginary of the future of the Internet.

I conclude this chapter with a short summary of how these discursive events, together with the EFF's challenge to the legal status of crypto, coalesced into the crystallization of crypto-discourse during the 1990s. This serves as segue to the last of the three periods in the evolution of crypto-discourse covered in this thesis, namely its revitalization.

The Role of the U.S. Government in Politicizing Crypto-Advocates

Parallel to government efforts to establish a connection between encryption software and computer crime, concerned computer users from the cryptographic community and the Whole Earth network mobilized ideologically behind cryptography as a means to achieve political and societal change. During the 1990s, the conceptualization of crypto became a battlefield, and the term emerged as a site of struggle between discourses competing to fill the empty signifier with meaning. The social antagonism that the cryptographic community and the Whole Earth Network constructed in relation to government actions during the origins of crypto-discourse set the stage for the crystallization of crypto-discourse. This politicization of cryptographers, online rights advocates, and hackers has been referred to by technology journalist Steven Levy as the rise of "cryptoactivism" (Levy, 2001, p. 205).

Cryptographers politicized crypto in the early 1990s. The Pentagon Papers and Martin Gardner's column in popular technology magazine *Scientific American* (number 2 in Figure 3) were both factors that would motivate Phil Zimmermann to develop encryption software (Levy, 2001). Phil Zimmermann had followed the Pentagon whistleblower and anti-nuclear activist Daniel Ellsberg, and his work which denounced the actions of the United States government in the Vietnam war (Greenberg, 2012, p. 127). What prompted Zimmermann to actively engage was proposed government regulations on online communications.

In 1991, Zimmermann developed encryption software and with the help of other crypto-advocates, popularized it to the public in a direct response to government regulatory propositions. Zimmermann learned through a statement on a bulletin board system (BBS) about the U.S. proposed amendment to a counter-terrorist Senate Bill 266 (number 9a in Figure 3). The bill would require software manufacturers and communication providers to allow access to plaintext (decrypted) communication, if required by law enforcement. In direct response, Zimmermann developed public-key encryption software entitled Pretty Good Privacy (PGP) in 1991 (number

9b in Figure 3). The name “Pretty Good Privacy”, inspired by a radio program (Levy, 2001, p. 195), established an understanding of the software as an enabler of privacy.

Zimmermann and other cryptographers circulated PGP widely through bulletin board systems and other forums, as well as by contacting journalists. Crypto-advocate Kelly Goen communicated the release of PGP and the motivation behind it to Jim Warren, a computer scientist, activist, and columnist at San Francisco technology magazine *MicroTimes* (Levy, 2001). Levy explains how Zimmermann and other crypto-enthusiasts with whom he had shared his software with, had a clear strategy in mind to spread encryption through technology journalism: “if thousands of copies of PGP were in use, Senate Bill 266 would be rendered irrelevant” (Levy, 2001, p. 197). The U.S. government started investigating Zimmermann for “violations of the U.S. Arms Export Control Act” (Bennett, 2008, p. 87) but PGP had already spread widely over the Internet. Zimmermann even suggested that these investigations may have contributed to popularizing PGP: “Oddly enough, the US Government may have inadvertently contributed to PGP's spread, by making it more popular because of my case” (Zimmermann, 1995). In addition, Zimmermann circumvented government restrictions by publishing the source code in a book, which he could then export under the protection of the First Amendment. As the cryptographers developed and spread the PGP software and source code, the articulations of antagonism between the state and the cryptographers continued through a series of legal battles, in which online rights advocates politicized crypto.

Members of the Whole Earth network described by cyberpunk fiction author Bruce Sterling, as the “Civil Libertarians” (Sterling, 1992) also politicized as a response to government actions. The U.S. government’s attempts to prevent computer crime during the late 1980s resulted in a crackdown on hackers and technology developers (Sterling, 1992) due to what founder of Lotus Development Corporation Mitchell Kapor, calls a “serious misunderstanding of computer-based communication and its implications for civil liberties” (Kapor, 1991, p. 158). Kapor, together with his fellow Whole Earth members John Perry Barlow lyricist for the Grateful Dead, and John Gilmore, software developer from Sun Microsystems, felt targeted by the government’s actions and founded the civil liberties organization the Electronic Frontier Foundation (EFF) in 1990 (number 8 in Figure 3). As the government sought to further regulate crypto through the implementation of so called “backdoors”, which would give the intelligence agencies a key to access the encrypted information, EFF mobilized around encryption technology in particular. EFF fought for civil liberties online in the 1990s’ Crypto Wars.

The Crypto Wars, a term only later used by civil liberty organizations such as the EFF, refers to a series of legal battles between the United States Department of Justice and civil liberty organizations, primarily the EFF, regarding the status of encryption technology.[12] During the

[12] In 1995, the Electronic Frontier Foundation sued the Department of Justice on behalf of Berkley PhD student Dan Bernstein, who “wished to publish an encryption algorithm he developed, the source code for a program to run the algorithm, and a mathematical paper describing and explaining the algorithm” (Dame-Boyle, 2015). This algorithm contained a code that would make a stronger cipher than the one being used by the NSA and was therefore considered a weapon. The *Bernstein v. Department of Justice* case resulted in a court rule deciding that code is as a form of speech that was protected under the First Amendment and changed the future possibilities for encryption technologies as well as established the recognition of online rights as opposed to offline rights.

battles that lasted almost an entire decade, encryption source code went from being classified as munitions, to speech protected by the First Amendment (Bennett, 2008) and the U.S. did not prosecute Zimmermann. These "Civil Libertarians" challenged the state's claim to define the meaning of encryption as they articulated the technology as a form of free speech that should be protected under the First Amendment. In other words, they successfully articulated a chain of equivalence between crypto and free speech that differentiated from articulations made by the state. Besides legal disputes, online rights advocates also advanced their articulations of crypto through other practices, such as conference presentations.

Technology reporter Jim Warren, who had received word about PGP through the cryptographers, articulated the concerns of cryptographers and hackers when he organized the *First Conference of Computers, Freedom, and Privacy* (1991) (number 9c in Figure 3). The conference brought together members from the crypto community, the Whole Earth Network, companies such as Apple and civil rights organizations including the EFF. At this conference, participants discussed a variety of topics relating to the constitution, computer networks, and the conceptualization of online freedoms and rights (Warren, Thorwaldson, & Koball, 1991). WELL-member, EFF-founder, and software developer John Gilmore were among the attendees.

John Gilmore gave a speech calling for the participants of the conference to start building technological systems with strong encryption in order to achieve "real" freedom (Gilmore, 1991). Gilmore's free society is one in which individuals have technologically enforced financial privacy in the form of anonymity systems by using strong encryption. This freedom would also include free trade and accountability towards each other on an individual basis (as opposed to towards the public).

Gilmore used a number of strategies in his articulation of what constitutes a desirable society with such a freedom. In his articulation, Gilmore excludes the possibility of trust in government. He argues that any government that would seek to get more power would not be able to resist the temptation to collect and use information about the citizens that it is supposed to serve. This exclusion is further reinforced when trust in government is juxtaposed to trust in mathematics: "I want a guarantee -- with physics and mathematics, not with laws -- that we can give ourselves things like real privacy" (Gilmore, 1991). Recalling Levy's hacker ethic, this articulation similarly equates technology with freedom. He further strengthens this understanding of freedom by presenting it as the "real" freedom, with "real" privacy, endorsed by mathematics. In so doing, he excludes human made "fake" laws like "laws that say you can't listen to cellular phone calls" (Gilmore, 1991) that consequently would represent a supposedly "unreal" freedom. He also clearly depicts government, and in particular the National Security Agency, as the obstacle as he explains that "the NSA is currently holding us hostage" (Gilmore, 1991). In addition, Gilmore presents aspects of his vision of freedom–privacy, financial privacy, and anonymity–as individual "rights". He thus refers to these aspects as principles that everyone should be entitled to by law, whether manmade or physical, although such rights are defined by the former.

In sum, Gilmore articulated with the help of the logics of equivalence, a relationship between technologically assured online financial privacy, anonymity, individual rights, and freedom. He simultaneously employed the logics of difference to exclude government and man made laws that would ensure the protection of privacy, from this chain of equivalence. As cryptographers and online rights advocates politicized crypto in relation to the release of Pretty

Good Privacy (PGP) to the public in 1991 (v 1.0), a group of individuals including Gilmore, took it upon themselves to establish the meaning of the term “crypto”, namely the Cypherpunks.

The Role of The Cypherpunks in Establishing A Partial Fixation of Meaning

During the crystallization period, the Cypherpunks and technology reporter Steven Levy sediment a partial fixation of meaning by using several discursive strategies. They employ the logics of difference and equivalence by excluding some meanings, and including others in political manifestos, technology magazine articles, and a book. Furthermore, they advance crypto-discourse by popularizing it, which is in alignment with their shared political objective.

The discursive work of the Cypherpunk community constitutes a crystallizing moment in crypto-discourse. Using the logics of difference and equivalence, the Cypherpunk community articulated their varying political objectives and shared identity in direct relation to the empty signifier crypto. The Cypherpunks, “an informal group dedicated to public education and dissemination of encryption” (Gilmore, n.d.), formed in 1992 in California, as a response to what they experienced as a threat to their online privacy. Tim C. May, Eric Hughes, and John Gilmore gathered cryptographers, WELL-members, and other encryption software enthusiasts in a house in Berkeley to discuss, but more importantly, to develop crypto (Coleman & Golub, 2008).

During that first meeting, Jude Milhon proposed the name “Cypherpunks” for the group (Levy, 2001).[13] Milhon went under the name St. Jude in her writings for the Internet culture magazine *Mondo 2000,* which covered cyberpunk topics “with stories about virtual sex, smart drugs, cryptology, and nanocyborgs” (Boulware, 1995). “Cypherpunk”, is a direct spin-off of “cyberpunk”. The term is used to describe a fictional literature genre, generally characterized by dystopic and highly technological settings in a future controlled by multi-national corporations. “Cyber”, in cyberpunk, derives from the scientific research branch of cybernetics, and “punk” signifying the anti-establishment subculture (Clute, Langford, Nicholls, & Sleight, 2012). While “cypher” was a new term and the result of mixing “cyber” with “cipher” (the term used to describe encrypted messages), the “punk” remained, signifying the attitude and the antagonism of the group towards authority.

This articulation of antagonism towards authority and in particular towards the state is most visible through artifacts that the Cypherpunks published and circulated on an online mailing list. After the initial meeting at Eric Hughes’ house, John Gilmore created and hosted the *Cypherpunk Mailing List* (Gilmore, n.d.). Originally comprising a handful of members, the list

[13] Although Jude Milhon is a central figure in the WELL, Cypherpunks, and *Wired*, she is among the few women mentioned and is only briefly mentioned in the literature that tells stories of the Cypherpunks (see Greenberg, 2012b; Levy, 2001).

eventually grew to accommodate thousands of members that would continue to contribute to the list until the early 2000s (Greenberg, 2012).

The Cypherpunk Mailing List (number 10b Figure 3) served several functions. It united cryptographers, online rights advocates, and hackers alike that sought to debate the politics and develop the codes of crypto. In 1993, Berkeley mathematician and founding member Eric Hughes explained in "A Cypherpunk's Manifesto" (number 11a in Figure 3) posted to the list, that "Cypherpunks write code" (Hughes, 1993), thus defining the group by their practice. However, list members did not only write code but actively participated in constructing what meaning the code should carry.

The Cypherpunk mailing list served as a space where Cypherpunks could articulate their ideas about crypto and the future. Whereas some members took these ideas to engage in legal battles regarding the status of encryption, others imagined concepts such as cryptocurrencies long before the creation of Bitcoin.[14] Discussions on the list also inspired members to later develop technologies such as the file sharing protocol BitTorrent associated with online piracy, and go on to create initiatives such as the whistleblower organization WikiLeaks.[15]

[14] Bitcoin is an open source digital currency and a decentralized payment system.

[15] Bram Cohen had been a contributor to the list and developed BitTorrent in the beginning 2000s (Greenberg, 2012b).

Prominent crypto-advocates took to their hearts to articulate an understanding of crypto as an enabler of freedom in order to spread the crypto-word. The founding members of the Cypherpunk list wrote political manifestos such as “The Crypto Anarchist Manifesto” (May, 1992), “A Cypherpunk Manifesto” (Hughes, 1993), as well as an elaborate Cypherpunk FAQ entitled the “Cyphernomicon” (May, 1994).

The “Crypto Anarchist Manifesto” (number 10a in Figure 3) has circulated the Internet and come to signify the practices of the entire movement. Physicist and former Intel employee Tim C. May was like his fellow founders, a libertarian. According to Levy, May’s vision was "an end to nation-states" (Levy, 2001, p. 207). May had also taken to cryptographer Chaum’s writings from 1985 that politicized crypto by suggesting anonymous systems, as he articulated crypto-anarchy. May had already written and shared similar versions of what would be the “Crypto Anarchist Manifesto” at Crypto and Hacker conferences (May, 1992). He read it at the first physical Cypherpunk meeting at Hughes' house in Berkeley, in 1992. Then he published it in the *Cypherpunk Mailing List*, from where it has been widely distributed on the Internet.

May introduces anarchy to crypto in the format of a manifesto. The manifesto also advances the understanding of crypto as a productive force of its own. May describes an anticipated “social and economic revolution” brought about by encryption. The manifesto begins with a reference to the “Communist Manifesto” (Marx & Engels, 2008) and opens with: “A specter is haunting the modern world, the specter of crypto anarchy” (May, 1992). This use of historical materialism that forwards technological development as a force beyond human control excludes responsibility from social actors to determine its direction and use. Any attempt to hinder the development of crypto anarchy is therefore meaningless:

> The State will of course try to slow or halt the spread of this technology, citing national concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be valid; crypto anarchy will allow national secrets to be trade freely and will allow illicit and stolen material to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion […]. But this will not halt the spread of crypto anarchy. (May, 1992).

In this manner, May takes the argument of national concern and removes it, excludes it from a possible meaning of crypto, as it will not matter that it is a valid concern. This form of technological determinism removes the possibility of an understanding of the state fulfilling a responsible role as it removes the purpose of the state meaningfully ensuring that it does not abuse its power. This strategy constructs an understanding that crypto anarchy is inevitable.

In "A Cypherpunk's Manifesto" (number 11a in Figure 3)*,* Hughes employs a similar strategy as May, when he represents the development of crypto as inevitable. He invokes Stewart Brand's statement from the Hackers' Conference in 1984 that "information wants to be free" (Brand, 1985, p. 49) when he speaks of "… the realities of information. Information does not just want to be free, it longs to be free" (Hughes, 1993). In addition, he explicitly excludes the possibility of the state as a grantor of privacy stating that, “we know that someone has to write software to defend privacy, and since we can’t get privacy unless we all do, we’re going to write it” (Hughes, 1993).

Both May and Hughes employ a strategy similar to Levy’s representation of hackers when he referred to them as liberators of the magic trapped in computers (Levy, 1984). Their strategy is also compatible with what critical science and technology scholar Söderberg suggests is hackers’ strategic use of material determinism to forward their political objectives. Söderberg exemplifies this claim through an analysis of open source advocate Eric Raymond’s essay *The Cathedral and the Bazaar,* in order to identify contradictions within hacker statements and hacker practice (Söderberg, 2013). These discursive strategies serve to construct an understanding of an inherent meaning in crypto, naturalizing the understanding of encryption as the enabler of a particular form of freedom – the “real” form of freedom that Gilmore presented.

Figure 4 illustrates how Cypherpunks employ the logics of difference and equivalence in their construction of crypto-discourse.

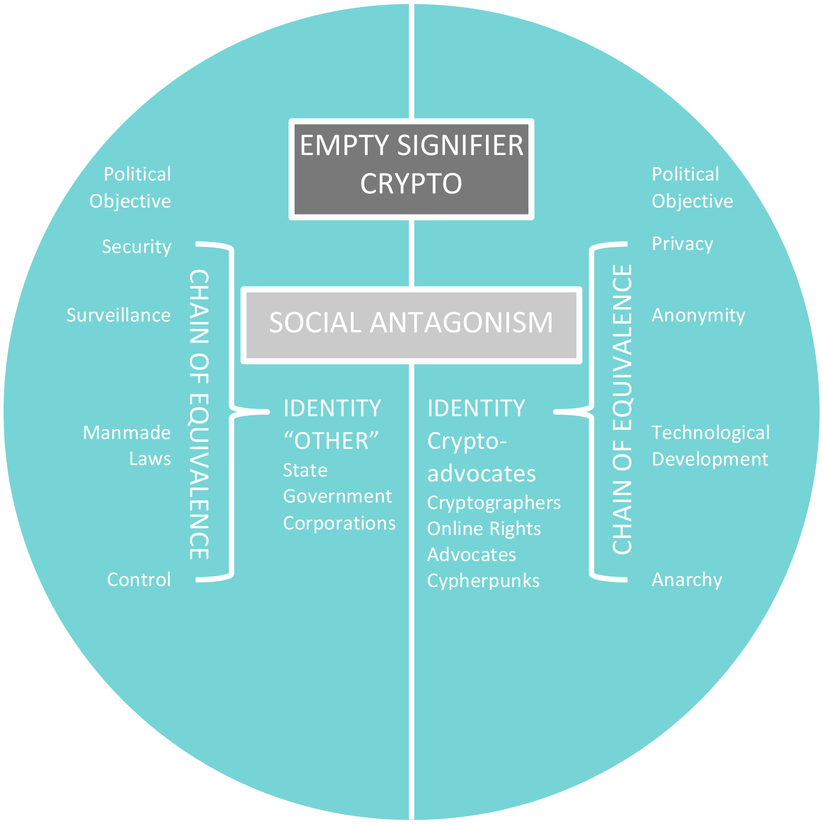

Figure 4 Logics of difference and equivalence at work in the empty signifier "crypto".

Through their shared practices of writing and sharing code and political manifestos on a mailing list, Cypherpunks articulate crypto in relation to several political objectives that form a chain of equivalence. These include privacy, freedom of speech, financial anonymity, anarchy, the common good, safety, and technological development, to name a few. They also articulate crypto in relation to obstacles to it, for example the state, control, security, surveillance, regulations on encryption, and large faceless organizations. These articulated obstacles form an opposing chain of equivalence through the logics of difference. Through these chains of equivalence, Cypherpunks construct partial identity of crypto-advocates as well as of the "Other", which includes the state. The political manifestos constitute key discursive events in this articulation of crypto-discourse, although they remained at first within a smaller community of Cypherpunks and other crypto-enthusiasts. The discourse became more firmly sedimented when technology journalists made it popular through journalistic accounts that represent crypto through the Cypherpunks.

The Role of Technology Journalism in Popularizing Crypto

Technology journalism played a significant role in crystallizing crypto-discourse. Indeed, the very success of crypto-discourse, as per the Cypherpunks and PGP developer Phil Zimmermann, depended on the spread of encryption technology. Technology and culture magazine *Wired* launched in San Francisco in 1993. The founders of the magazine came from the same discourse community as many of the Cypherpunk and EFF members, namely, the Whole Earth network described in the previous chapter. Several members of the community have contributed to the magazine by writing articles (e.g. Brand, 1993), and technology reporters such as Levy have published articles several articles popularizing Steven Levy's representation of the Cypherpunks and their articulation of crypto (Figure 5).

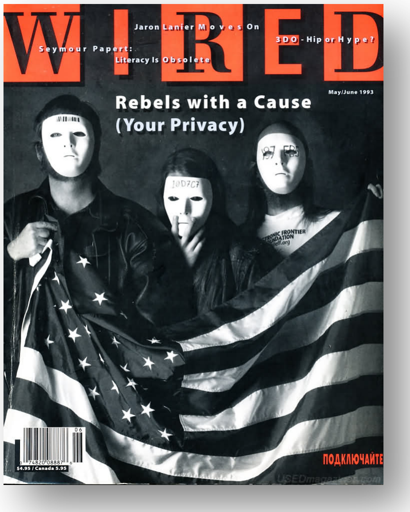

Figure 5 The cover of *Wired* Magazine 1.02 May/June 1993.

The cover is featuring the founders of The Cypherpunks: Tim C. May, Eric Hughes, and John Gilmore.

A key discursive artifact in the crystallization of crypto-discourse is the second issue of *Wired* magazine (see Figure 5; number 11d in Figure 3) in which Levy had an article entitled “Crypto Rebels” (Levy, 1993). The cover of this issue featured the three founding members of the *Cypherpunk Mailing List*: John Gilmore, Eric Hughes, and Tim May. On the cover, these three men are pictured in front of the flag of the United States, wearing masks with PGP keys inscribed on them. In the article that accompanies the cover, Levy uses the empty signifier crypto to portray Cypherpunks as “rebels”, similar to how he depicted hackers as heroes in 1984 (Levy, 1984, 1993). Levy sets up the social antagonism towards authority immediately: “It’s the FBIs, NSAs, and Equifaxes of the world versus a swelling movement of Cypherpunks, civil libertarians, and millionaire hackers. At stake: Whether privacy will exist in the 21st century” (Levy, 1993). He also portrays the Cypherpunks as saviours, as they are not only here to liberate technology, but to save “your” privacy, as stated on the cover. Through that statement, the magazine incites the readers to be concerned about their personal privacy, as an infringement on their rights and freedoms. Hence, the magazine portrays Cypherpunks, as opposed to the national security state, as those who will fight for the people. The rebel is then presented as the hero that stands up against the antagonist government.

This representation of Cypherpunks adds a second layer of signification to crypto. The *Wired* issue not only represents crypto, the process of encryption, as a tool that enables a particular form of freedom, but also represents Cypherpunks as its liberators. By adding the U.S. national flag, the cover establishes a connection between anonymity (the masks), encryption (the written PGP keys on the masks), and the United States, invoking patriotism. The Cypherpunks are not only standing up against the antagonist, they are defending their nation. Other details, such as the print of the Electronic Frontier Foundation on one of the member’s t-shirts, presumably Gilmore’s, associate the movement with civil liberties. In this cover, the Cypherpunks became synonymous with crypto, privacy, anonymity, free speech, American, and Internet freedom.

Through this publication, the Cypherpunks had a considerable cultural impact (McKelvey & Beyer, 2015). Levy spread awareness of the Cypherpunks to a broader public, in a manner that popularized the movement. Rebels and punks are celebrated in popular culture and resonate well with fans of cyberpunk fiction. Following this publication, Levy has written numerous articles on crypto for *Wired*, including *Cypher Wars* (1994b) and *E-Money (That’s What I Want)* (1994a). He has also reported for other magazines such as The New York Times Sunday Magazine and

Macworld, which he has drawn from, to compile his book, *Crypto: How the Code Rebels Beat the Government, Saving Privacy in the Digital Age* (Levy, 2001).

Although published in 2001, *Crypto: How the Code Rebels Beat the Government, Saving Privacy in the Digital Age* (Levy, 2001) (number 14c in Figure 3) is another key artifact in the crystallization period of crypto-discourse that employs all three of Laclau and Mouffe's concepts. The book assembles the story of the cryptographers, the civil libertarians, and Cypherpunks behind the empty signifier crypto in one popular journalistic account. The book strategically unites rebels, heroes, advocates, activists, enthusiasts, war, and a number of other epithets with crypto. By naming all of them code rebels, heroes, and saviours of privacy, Levy depicts the government as the antagonist (and looser) in a war where crypto is the battlefield. Drawing on more war imagery, he describes for example crypto anarchy as "a powerful intellectual weaponry" (Levy, 2001, p. 210). Using a language associated with war, this book thus sediments the chains of equivalence that have been articulated in the discursive work of the Cypherpunks and Levy's previous accounts of crypto.

Conclusion

In this chapter, I have presented the crystallization of crypto-discourse during the 1990s. I have described the emergence of crypto as an empty signifier. I have also demonstrated how crypto-advocates, and in particular Cypherpunks and technology journalists, have strategically employed the logics of difference and equivalence in their articulation of crypto, through the passage of the social antagonism that they had articulated during the origins of crypto-discourse.

First I described how cryptographers, such as Phil Zimmermann, and members of the WELL, such as the founders of the EFF, politicized as a response to government actions, drawing on the social antagonism laid out in the previous chapter. Then, I introduced the discursive work of the Cypherpunks and technology reporter Steven Levy. I illustrated through selected artifacts that are representative of foundational moments in crypto-discourse, how Cypherpunks and Levy have articulated and popularized political objectives and identity through the empty signifier crypto. This analysis shows how Cypherpunks constructed a shared vision of the future of Internet freedom that was popularized through the discursive work of *Wired* magazine.

Zimmermann's development and spread of PGP, combined with EFF's challenges to the legal definition of crypto, Cypherpunk political manifestos, and *Wired* magazine cover and articles thus coalesced during this period into the crystallization of crypto-discourse. In this partial fixation of meaning, the Cypherpunks established a relationship between encryption software and a negative conception of freedom that excluded the state. Cypherpunks employed the logics of difference and equivalence in their particular articulation of crypto, which I illustrate in Figure 4. By establishing chains of equivalence, the Cypherpunks and *Wired* universalized this particular articulation as the differential political objectives presented by crypto-advocates became equivalent to each other in the social antagonism towards the state.

In the next chapter, I present the revitalization period of crypto-discourse. During the 2000s, the articulation of crypto as an empty signifier occurred in a new context. State actions seek to define crypto in a global context, new uses of crypto expand the chains of equivalence, and journalistic accounts revitalize crypto-discourse from the 1990s.

Chapter 5: The Revitalization of Crypto-Discourse (2000 – 2015)

In the previous two chapters, I delineated the origins and the crystallization of crypto-discourse. In this final chapter, I address the revitalization of crypto-discourse, a period during which crypto as an empty signifier resurfaces as the site of struggle between competing discourses.

The chapter proceeds as follows. First, I briefly review the role of the U.S. government in reinforcing an anti-terrorist legal discourse that impacts global communication policy following the terrorist attacks on September 11, in 2001. The state thus reclaims its right to define the empty signifier crypto globally as it seeks to establish a relationship between online communication technology and terrorist activity. I then discuss the formation of two organizations, The Onion Router (emanating from MIT crypto-scientists) and WikiLeaks (established by Cypherpunk Julian Assange), which offer new uses of encryption software. I also consider the implication of significant information leaks, such as WikiLeaks (2010) and the Snowden leaks (2013) of confidential information about the U.S. government's activities and how these leaks were facilitated by the use of encryption. Tor and WikiLeaks, and their applications of encryption, challenge anew the state's claim to define crypto, by articulating a relationship between crypto and journalistic practices.

I then discuss writings of WikiLeaks' Editor-in-Chief, Julian Assange and journalistic accounts by *Wired* reporters Andy Greenberg featuring Cypherpunks, WikiLeaks, and Edward Snowden. These accounts reinforce the previously articulated chains of difference and equivalence by reinvigorating discursive work from the crystallization period of crypto-discourse.

I conclude this last chapter of the crypto-saga with a review of how all of these events revitalize crypto-discourse in a global context. During the revitalization period, Cypherpunks and technology reporters draw on and rearticulate the crystallized form of crypto-discourse from previous period employing in a similar manner the discursive concepts of social antagonism, empty signifiers, and logics of difference and equivalence. This leads me to my closing chapter, where I discuss the relevance of these findings and their pertinence to future policy about encryption software and its relationship to Internet freedom.

The Role of the U.S. Government in Articulating Crypto Globally

Following the terrorist attacks on September 11, in 2001, the U.S. government attempted to restore its position as the actor that defines crypto and established a relationship between online communication technology and global terrorist activity. Through laws such as the U.S. Patriot Act (number 14a in Figure 3), the Bush administration, together with the United Nations, constructed an anti-terrorist legal discourse – The War on Terror - that affected global communication policy. The government constructed this discourse by treating terrorism as warfare, criminal activity, and armed rebellion simultaneously (Braman, 2011).

In addition, the U.S. government, together with the U.K. government, presented a draft resolution of anti-terrorist measures to the UN that “with almost no alterations, was adopted almost immediately by a unanimous vote” (Braman, 2011, p. 490). By treating terrorism as a global issue, the U.S. and U.K. governments impelled actors of the international community, through the mechanisms of the United Nations, to follow suit immediately. This form of harmonization of communication policy disregards national differences in legal and political systems, such as varying perceptions of the meaning of privacy and the role of government (Dinev, Bellotto, Hart, Russo, & Serra, 2006, as cited in Braman, 2011). This way, the UN globalized a particular articulation of communication policy crafted by the U.S. and the U.K. governments.

The UN Resolution (1373), together with other legal instruments that followed, had direct implications on global communications policy regulating technology (number 14b in Figure 3). Understanding communication as terrorist activity consequently had implications for variations of free speech laws internationally as it allowed authorities to collect data, store information, and in other ways monitor communication. In this context, crypto rises again as a site of struggle between competing discourses. This time, the stage is global.

The Role of New Uses of Crypto in Extending the Articulation of Crypto

New uses of encryption such as onion routing and leaking offer competing discourses to the anti-terrorist legal discourse. *Onion Routing* refers to anonymous online communication systems in which the communication goes through layers of encryption (like an onion), bouncing through several relays, also called routers, or nodes (The Electronic Frontier Foundation, n.d.). This process hides the IP address of users, removing the possibility to identify them online. The functions of onion routing are directly inspired by Cryptographer David Chaum’s writings on anonymity systems from the 1980s (Chaum, 1981, 1985; Moore & Rid, 2016). The act of *leaking,* or whistleblowing, refers to the act of disclosing classified documents. Due to layers of encryption, onion routing largely facilitates leaking, as the whistleblower can remain anonymous while disclosing large amounts of data.

The most prominent onion routing system is Tor that emanates from MIT crypto-scientists and the U.S. Navy. Tor is software based on a network of volunteer relays that implements onion routing. The *Tor Browser* is a version of the Firefox browser through which users can browse the Internet anonymously. The *Tor Project* is the organization that maintains Tor software and was founded by Roger Dingledine and Nick Mathewson in 2006 (number 15a in Figure 3), who together with Paul Syverson had developed Tor ("Onion Routing: History," 2005; The Tor Project, Inc, n.d.-a). The name Tor comes from The Onion Router, which refers to the original version of Tor. The original version of Tor was an initiative funded by the U.S. Department of Defense (DARPA) and the U.S. Navy's science and technology programs (ONR) and designed in the late 1990s. In the early 2000s, Tor released its source code as free and open under MIT licence ("Onion Routing: History," 2005) and already had a few nodes in the United States and in Germany. In 2004, the Electronic Frontier Foundation began to fund the network and up until today various organizations, foundations, organizations, and government agencies globally fund the network (The Tor Project, Inc, n.d.-d).

Tor also offers so called hidden services. Hidden services are not accessible through a regular browser. Instead, they are located outside of the regular consumer Internet through services such as "*.onion" sites, available only through the Tor Browser. Although they constitute a very small part of Tor services (Moore & Rid, 2016), hidden services are mostly represented in media as the "Darknet" (Chacos, 2013; Moore & Rid, 2016) due to the mediatized trials such as the ones regarding Silk Road in 2015. Silk Road is a hidden black market similar to the ones May envisioned in the “Crypto Anarchist Manifesto” that uses crypto currencies (electronic currency) for online transactions (Greenberg, 2015a; Knibbs, 2015). Potential and actual activity on hidden services (such as the exchange of child pornographic material, illegal drug and arms trade, and assassination markets) is according to Moore and Rid (2016) what gives encryption a “bad name” (Moore & Rid, 2016, p. 30). Tor spokesperson Jacob Appelbaum has also addressed these issues as representations of Tor, although he deflects these depictions of the system.

Greenpeace activist and hacker Jacob Appelbaum argues that the depictions of illegal practices related to encryption represent the four horsemen of the infocalypse. He contends that this representation is a strategy repeatedly used to discredit the use of privacy-enhancing technologies as criminal. The four horsemen is wordplay on the biblical reference to an apocalyptic vision brought by four horsemen representing Conquest, War, Famine and Death. In the infocalypse, they represent instead “child pornography, terrorism, money laundering, and The War on Some Drugs” (Assange et al., 2012, p. 43). The term was coined by Tim C. May, founding member of the Cypherpunk Mailing List who explains in the “Cyphernomicon” (1994), a Cypherpunk FAQ (number 12a in Figure 3), how privacy and anonymity will be attacked by authorities as a tool for the “Four Horsemen” and a haven for online criminal activity:

> 8.3.4. "How will privacy and anonymity be attacked?"
>
> - the downsides just listed are often cited as a reason we can't have "anonymity"
>
> - like so many other "computer hacker" items, as a tool for the "Four Horsemen": drug-dealers, money-launderers, terrorists, and pedophiles.
>
> - as a haven for illegal practices, e.g., espionage, weapons trading, illegal markets, etc.
>
> (May, 1994)

Appelbaum thus invokes crypto-discourse as articulated by May, in his response to representations of onion routing. In his foreword, May excluded this threat from his crypto-discourse by subordinating the importance of arresting criminals to the right to free speech and privacy:

> + The Basic Issues
>
> + Great Divide: privacy vs. compliance with laws
>
> + free speech and privacy, even if means some criminals cannot be caught (a stand the U.S. Constitution was strongly in favor of, at one time).
>
> (May, 1994)

This is one example of a Tor advocate countering the representational discourse of crypto with articulations that exclude the role of the state. In other examples, tor advocates refer to the system as a tool to bypass censorship in authoritarian regimes, such as Egypt during the Arab Spring in 2012, thus as a liberating technology (Zahorsky, 2011).

The popularity of Tor is crucial for the functionality of its services. With more people using it, it becomes more difficult to identify nodes and consequently users (The Tor Project, Inc, n.d.-c). The Tor Project refers to the software as a: “censorship circumvention tool” (The Tor Project, Inc, n.d.-b), articulating a social antagonism towards corporate and government mass surveillance. Tor explains that this tool can be used by individuals to access blocked sites, by activists, bloggers, and journalists who communicate with whistleblowers and dissidents, and by civil liberty organizations such as the EFF that want to advance civil liberties online. Corporations can also employ Tor to survey their competition anonymously. In addition, the U.S. Navy and law enforcement can turn to Tor in attempts to prevent crime (The Tor Project, Inc, n.d.-b). By listing these types of use and users, Tor establishes a connection between online anonymity and journalistic practices, online free speech, national security, crime prevention, and emphasizes individual control over security and privacy. This chain of equivalence absorbs concepts that previously were part of differentiating chains of equivalence, such as national security and crime prevention. In addition, the chain extends to encompass leaking practices.

Tor cryptographers such as Appelbaum unite with Cypherpunks such as Julian Assange in the articulation between encryption software and the practice of leaking classified information. Jacob Appelbaum is not only a Tor spokesperson, but also a WikiLeaks spokesperson.[16]

[16] Jacob Appelbaum replaced Julian Assange as a representative of WikiLeaks at the Next HOPE (Hackers On Planet Earth) conference in 2010 (number 16 in Figure 3) (Appelbaum, 2010). The First HOPE conference (number 12 in

WikiLeaks is a media organization founded in 2006 by Julian Assange (number 15b in Figure 3), who is perhaps one of the better-known characters of the Cypherpunks. The purpose of WikiLeaks is to publish classified material that addresses “war, spying, and corruption” (“What is WikiLeaks,” n.d.). Examples of such big leaks are the *Collateral Murder Video* (number 16a in Figure 3) in 2010, showing Iraqi civilians being shot by American soldiers and *Cablegate* (number 17 in Figure 3) in 2011, hundreds of diplomatic cables released in cooperation with several European and North American news organizations. These mass leaks were possible because of encryption software.

WikiLeaks employed encryption in ways that threatened the authority of the state while securing the safety of the information that the organization was handling. The organization primarily used Tor and Tor’s hidden services to protect its sources and its own site (Greenberg, 2012). In addition, it distributed encrypted material among its members, ensuring that the material would remain safe in case an adversary would seek to get a hold of it. Similarly, the distribution of the material makes prosecution or other menacing acts towards WikiLeaks members meaningless, as it could not stop the publication of the material. Cindy Cohn, legal director of the Electronic Frontier Foundation has stated that WikiLeaks’ use of encryption to

Figure 3) was organized in New York in 1994 as a celebration of hacker magazine *2600: The Hacker Quarterly*. The conference has since brought together hackers, online rights advocates, researchers, and others to discuss issues related to hacker practice, such as Internet-specific technologies and online rights (“2600 News | 2600,” n.d.).

distribute and safeguard material is not a new tactic (Vallance, 2010). Julian Assange, however, as representative of an organization that leaks top-secret classified documents, gives new meaning to the strategy, as it directly antagonizes law enforcement's ability to stop classified information from gettinJulian Assange, Editor-in-Chief of WikiLeaks, is a self-proclaimed journalist. While some recognize him as a journalist, many oppose him due to conventional understandings of what should or should not constitute journalistic practices. Nevertheless, in claiming to be a journalist, he reconceptualizes his antagonistic position to extend to a role that is compatible with democratic state practices in which a role of journalists is to hold governments accountable. This title, while threatening to state authority, yet calls for public accountability. In addition to WikiLeaks' practices, another event that contributed to the reinvigoration of crypto-discourse during this period include the large leaks of classified information by Edward Snowden.

In 2013, former CIA contractor Edward Snowden disclosed classified documents that revealed secret mass surveillance practices on a global scale (number 19 in Figure 3). The Snowden-leaks, that were first published in news media outlets worldwide such as The Guardian, Der Spiegel, and Le Monde, showed how governments, and in particular the United States government and National Security Agency (NSA), collected online data from millions of people, both within and outside of the country's borders (Eaton, 2016; Greenwald, 2013; Lesnes, 2013).

Snowden articulated a relationship between the political objective of his leaks and the guiding principles of the EFF, Tor, and other leaks.[17] Pictures circulating the Internet and online news sites featuring him holding his laptop, which has two stickers of the two organizations' labels stuck to it, serve as an example of such an articulation (Galveston, 2014). His use of Pretty Good Privacy (PGP) encryption software (Garside, 2015) to communicate his leaks with journalists further prompted debates about the relation between encryption and freedom of expression. Notably, the U.S. Department of Justice has charged Edward Snowden for violating the Espionage act, depicting him as a traitor, while the United Nations launched consultations on the status of encryption and whistleblowing practices. In 2014, the HOPE X conference in New York (number 20b in Figure 3) featured Daniel Ellsberg, who leaked the "Pentagon Papers" in the early 1970s, and Edward Snowden, among other whistleblowers as keynote speakers (Cameron, 2014; Snowden, 2014). This conference established a relationship between hacking and whistleblowing. Furthermore, this digital form of leaking that was made possible through encryption and the practices that it entailed, such as conferences, established a relationship between encryption and the role of journalists to be watchdogs of government wrongdoings.

During its revitalization period, crypto-discourse transformed and extended its articulation of social antagonism to states all over the world, while the logics of difference and equivalence were hard at work to include and exclude new meaning. The discursive practices of Tor,

[17] Snowden did not employ Wikileaks for his disclosures.

WikiLeaks, and the Snowden leaks did not only extend the chains of equivalence to include journalistic practices in a national context, as these events took place and had repercussions on a global scale.

The Role of Journalistic Accounts in Revitalizing Crypto-Discourse

Crypto as an empty signifier and Cypherpunks as a discursive community reinvigorated visibility and popularity through coverage in journalistic accounts by Julian Assange and *Wired* reporters, which are seminal to the revitalization of crypto-discourse. In 2012, Julian Assange published *Cypherpunks: Freedom and The Future of the Internet* (number 18b in Figure 3). This book is a transcribed account of two episodes from his own television series, *The World Tomorrow*, that are dedicated to the Cypherpunks (Assange, 2012c). During these episodes, which are held inside the Ecuadorian embassy where Assange is residing, Assange discusses together with Jérémie Zimmerman, Andy Müller-Maguhn and Jacob Appelbaum, about Internet surveillance, its relationship to control and possibilities to stem mass surveillance. In his book, Assange also publishes an introductory statement that calls to "cryptographic arms" (Assange, 2012b) in the spirit of the Cypherpunks.

The introduction to this book is called "A Cryptographic Call to Arms", and follows the genre of a political manifesto. In this manifesto, which Assange ironically states: "[…] is not a manifesto. There is not time for that" (Assange, 2012a) Assange reinvigorates discursive work from the Cypherpunks during the crystallization period of crypto-discourse. Most notable is his representation of crypto as a force endorsed by the universe itself referring to its mathematical nature: “The universe believes in encryption” (Assange, 2012a, p. 4), “the embodiment of the laws of physics”, “The universe smiles on encryption” (Assange, 2012a, p. 5). Assange also applies the language of war, reappropriating the concept of crypto as a weapon: “call to arms” (1), “It is time to take up the arms of our new world, to fight for ourselves for those we love”. Consequently, he also allows more agency to social actors than May did, as he argues that a surveillance dystopia is on its way, which “we” need to fight with the help of this property of the universe. He clearly delineates through the logics of difference and equivalence the Cypherpunk identity and the meaning of freedom in relation to the state: “[…] regions free from coercive force of the outer state. Free from mass interception. Free from state control” (Assange, 2012a, p. 5), eliciting the discussions of Hakim Bey’s Temporary Autonomous Zone’s in the *Cypherpunk Mailing List* (McKelvey & Beyer, 2015).

The ensemble of this work revived previous articulations of crypto-discourse by reconstructing the Cypherpunk identity. Besides his cryptographic call to arms, Assange provided the reader with a definition of a Cypherpunk: “Cypherpunks advocate for the use of cryptography and similar methods as ways to achieve societal and political change” (Assange, 2012a). He also directly established a relationship to Internet freedom, through the title of his book. What is more, he portrays the Cypherpunks as the original constructors and citizens of the Internet while presumably referring to his own time on the *Cypherpunk mailing List*: “Once upon a time in a place that was neither here nor there, we, the constructors and citizens of the young internet discussed the future of our new world" (Assange, 2012b).[18] The previous articulation of crypto from the crystallizing period make this revitalization possible, as Assange draws on the identity construction of the Cypherpunks and the articulations of the state as the antagonist through the same discursive strategies as the Cypherpunks of the early 1990s. In addition, Assange excludes the possibility of the state as a protector of privacy similar to how Hughes had performed his exclusion in his Cypherpunk manifesto in 1993. Assange states that "strategic interception […] cannot be meaningfully constrained by regulation" (Assange, 2012a, p. 42), in a discussion about whether human made laws can protect privacy rights reminiscent of John Gilmore's speech at the *First Conference on Computers, Freedom, and Privacy* (Gilmore, 1991). Besides Assange's own discursive work, *Wired* journalists participated in revitalizing crypto-discourse.

Following the rise in mega-leaks by controversial media organization WikiLeaks, a journalist took special interest in the phenomenon and its editor-in-chief Julian Assange. Technology and civil liberties journalist Andy Greenberg, who covers information security, privacy, and freedom issues at both *Wired* magazine and business magazine Forbes, wanted to understand where the ideas behind WikiLeaks came from. As he set out to tell the story of Julian Assange, he concluded that "Wikileaks was basically a Cypherpunk vision" (Greenberg, 2012a). In December 2010, Julian Assange featured the cover of Forbes Magazine and in 2012, he was

[18] Assange joined the *Cypherpunk Mailing List* under the name "Proff", in 1995 (Greenberg, 2012b, p. 143).

one the main character of Greenberg's book *This Machine Kills Secrets: How Wikileakers, Cypherpunks, and Hactivists Aim to Free the World's Information* (number 18c in Figure 3).

Through this book, Greenberg reinvigorated crypto-discourse by once again popularizing Cypherpunks, while also drawing on their articulations. Greenberg united the early cryptographers with this period's crypto-communities, focusing on the relationship between the disclosure of classified documents (leaking) and the development and use of encryption software. In addition, he articulated a global crypto-discourse. Greenberg described the globalized nature of information and leaking practices in the modern world. The book tells about encounters with individuals such as Birgitta Jónsdóttir in Iceland who is attempting to construct the International Modern Media Initiative, as well as of Bulgarian leakers training journalists how to use Tor. The book title also refers to Wikileakers, Cypherpunks, and hacktivisits, as a group that is "freeing" the world's information. The title thus alludes to the statement that "information wants to be free", a statement that continues to reappear throughout crypto-discourse. A year after Greenberg published this book Snowden "freed" an unprecedented amount of information.

In August 2014, a year after whistleblower Edward Snowden made his disclosures *Wired* published an issue featuring Snowden with an article written by James Bamford (number 20c in Figure 3) (Bamford, 2014). Bamford, who has written several journalistic accounts on whistleblowing in the United States, offers in this article in Wired one of the longest in-person interviews with Edward Snowden yet to be published. The cover of this issue features Snowden with a grey background, holding the American flag close to his heart (see Figure 6). The picture was taken by acclaimed photographer Platon, who has also shot magazine covers with world leaders such as United States President Barack Obama and Russian President Vladimir Putin

(Mirkinson, 2014; Platon, 2013). Whether intentional or not, the resemblance between this cover and the 1993 cover featuring the Cypherpunk founders May, Hughes, and Gilmore, is striking.

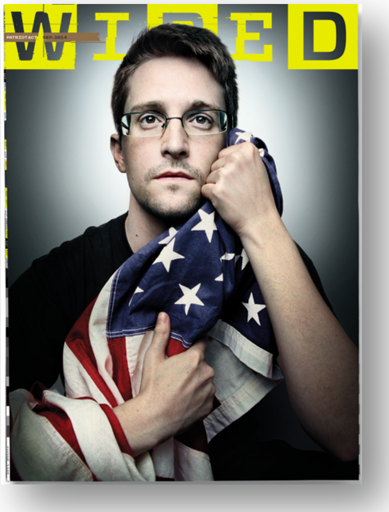

Figure 6 The cover of *Wired* Magazine 22.09 September 2014.

The cover features whistleblower Edward Snowden.

Conclusion

In this chapter, I have presented the role of the U.S. government in forwarding a global counter-terrorist agenda that has implications for global communication policy. By doing so, I have argued that the U.S. state has tried to reconstitute the meaning of crypto as a weapon of war, which provides the backdrop for the resurgence of crypto-discourse. I have also discussed new uses of encryption and their challenge to the state's attempt to define crypto. These include onion routing and leaking. I have outlined the formation of The Onion Router (Tor), WikiLeaks, and the Snowden leaks to illustrate how these events establish a relationship between encryption and journalistic practices. These practices take place in a global context but revitalize crypto-discourse as articulated during the crystallization period.

I have demonstrated how Julian Assange's introduction to *Cypherpunks: Freedom and the Future of the Internet*, calls for political action using similar strategies to those present in previous Cypherpunk political manifestos. These strategies seek to construct a meaning of crypto that appears inherent and universal, thus naturalizing a specific understanding of crypto that is simultaneously capable of encompassing multiple other possible meanings of Internet freedom. Additionally, I have shown how technology journalism has played a significant role in revitalizing Levy's and *Wired's* popular crypto-discourse from the 1990s. *Wired* reporter Andy Greenberg's representation of Cypherpunks, WikiLeaks, and Hacktivists who seek to "free" the world's information is part of this work is. Not to mention the *Wired* cover featuring Edward Snowden in 2014 that reinvigorates memories of the legendary cover from 1993 featuring the three founding members of the Cypherpunk movement. These articles and books constitute important moments of popularization of the Cypherpunks twenty years after the first publications that popularized crypto-discourse in 1993. This is in part due to the continued popularity of WikiLeaks and *Wired* magazine. In these works, the authors rearticulated crypto to establish new chains of equivalence, while drawing on articulations from the crystallization of crypto-discourse in the 1990s. The discursive work of the Cypherpunks and technology reporters during this period thus revitalizes crypto-discourse through Laclau and Mouffe's concepts of social antagonism, empty signifier, and logics of difference and equivalence.

In the next chapter, which is the closing chapter of this thesis, I briefly summarize the findings from all three periods of the crypto-saga and discuss their relevance to future policy about encryption software and its relationship to Internet freedom.

Chapter 6: Conclusion

"*A conjuring trick has taken place; it has turned reality inside out, it has emptied it of history and has filled it with nature, it has removed from things their human meaning so as to make them signify a human insignificance*"

(Barthes, 1972, p. 142).

In this thesis, I have shown how crypto-advocates, and in particular Cypherpunks, have articulated crypto-discourse: a partially fixed construction of meaning that establishes a relationship between crypto (encryption software) and a negative conception of freedom in relation to the state. By negative, I refer to how crypto-discourse advocates an understanding of freedom in which individuals are free *from* state interference. In addition, I have illustrated the significance of technology journalism in popularizing this discourse.

This thesis has outlined discursive events and practices that constitute the evolution of crypto-discourse over a period of forty years (1975 – 2015). I have divided this timeline into three periods: the origins, crystallization, and revitalization of crypto-discourse. Over this time, the empty signifier crypto emerged, crystallized, and re-emerged. From the early cryptographers and Whole Earth network in the 1970s, to onion routing and leaking of classified information in the 2000s, I have described how interrelated discourse communities of cryptographers, hackers, online rights activists, and technology journalists have articulated crypto in relation to freedom. By mapping and analyzing key discursive events in each of the three periods (Figure 3), I have identified instances where the logics of difference and equivalence are at play in the articulation of crypto as an empty signifier (Figure 4). Consequently, I have shown how the Cypherpunks and technology journalists specifically have constructed chains of equivalence through the empty signifier crypto. Cypherpunks and technology journalists universalized a particular understanding of Internet freedom in which only encryption software can protect online rights. This understanding excludes a positive role for the state by removing its responsibility to ensure the protection of online rights.

During the origins of crypto-discourse (1975–1990), articulations of social antagonisms, empty signifiers, and logics of differences and equivalences set the stage for the crystallization of crypto-discourse between 1990 and 2000 where the empty signifier crypto emerged as a site of struggle between competing discourses. It is during the crystallization period that crypto-advocates, and in particular Cypherpunks, employed the logics of difference and equivalence to exclude the possibility of a positive meaning of freedom in their articulation of crypto. This exclusion of meaning took place through the passage of social antagonism articulated by cryptographers and countercultural movements during the previous period. This articulation crystallized as technology journalists popularized crypto-discourse and established chains of equivalence between varying political objectives (such as privacy, anonymity, anarchy, free trade, and decentralization) among crypto-advocates.

Lastly, during the revitalization of crypto-discourse between 2000 and 2015 the discursive struggle over the meaning of encryption software went global. New articulations of encryption extended the existing chains of equivalence to include journalistic practices all over the world, while simultaneously extending the social antagonism to include governments generally.

Selected members of the Cypherpunks have attempted to construct the social by making crypto-discourse appear natural, as something that is inherent to the natural world and independent of the social. By employing the logics of difference and equivalence, they have presented crypto as a property of the universe that holds meaning in and of itself. They have for example excluded the state from their representation of freedom by presenting the evolution of crypto as inevitable, as a productive force of its own. For example, in Chapter 4 and 5, I described crypto-advocates' discursive strategies in selected artefacts that removed any significance that the state could have in directing future development or regulation of crypto. Consequently, they also removed responsibility from the state to ensure the protection of rights such as privacy or freedom of speech, as they argue that only the laws of physics (encryption) can truly protect such rights. This strategy is present already in the origins of crypto-discourse, where members of the cryptographic community and the Whole Earth network articulate a relationship between technology and freedom that excludes the state.

Technology journalists, in particular Steven Levy and other reporters at *Wired* magazine, have perpetuated crypto-discourse through their heroic representations of hackers, crypto-advocates, and Cypherpunks. Basing these representations on statements such as "information should be free" (Levy, 1984) that later evolved into "information wants to be free" (Barlow, 2001; Brand, 1985), technology journalists have depicted hackers and Cypherpunks as liberators of the world's information (Greenberg, 2012). Using a language of war, similar to Julian Assange's repertoire (Assange, 2012a), Levy and Greenberg have represented Cypherpunks as heroes, rebels, and saviours that are here to liberate information held hostage (Gilmore, 1991) by governments worldwide (Greenberg, 2012; Levy, 1993, 2001).

These strategies suggest a process of myth-making as crypto-advocates seek to establish crypto-discourse as a reality that exists independently of the meaning that anyone seeks to attribute to it: "the very principle of myth [is to transform] history into nature" (Barthes, 1972, p. 129). Myth is "metalanguage", or "a second language, in which one speaks of the first" (Barthes, 1972, p. 115). We can consider this in terms of what Cypherpunks did during the crystallization of crypto-discourse. As a primary language, Cypherpunks wrote encryption code and engaged directly with the object of crypto-discourse. This engagement creates a direct relationship between the hacker and the software which he, or she (although no "shes" are present among the prominent constructors of crypto discourse, with the exception of Jude Milhon) builds or modifies. We can consider political statements and journalistic accounts as artifacts through which Cypherpunks speak *of* crypto. Having established in the previous chapters that there is no intrinsic meaning in encryption software, nor in the term "crypto" used to signify encryption software, we see that the articulation of crypto in relation to freedom is a construction suggestive of myth-making which deserves further examination.

A myth is a social phenomenon that takes shape when dominant understandings of reality are shaken, or 'dislocated', which allows for "'new' spaces of representation" to emerge (Howarth, 2000, p. 111). The process of myth making partially fixes meaning in an instance of dislocation, much like the dislocation described in Chapter 3 during the origins of crypto-discourse, in which discontent grew towards United States government. Myth-making consolidates various objectives and ideals, similar to how crypto-discourse unites various political viewpoints. Importantly, myth-making causes certain meanings that correspond to the interest of myth-makers, to be understood as fact, and those facts then become a collective social imaginary (Barthes, 1972; Howarth, 2000). In so doing, myth removes the human from the process of meaning-making “to make [things] signify a human insignificance” (Barthes, 1972, p. 142). Myth consequently renders responsibility meaningless, much like Cypherpunks portrayed any attempt to stop the spread of encryption, meaningless.

Such a naturalized understanding of crypto as a natural force has normative implications for larger debates about Internet freedom. Importantly, by attributing agency to crypto as a natural force, crypto-discourse removes accountability from a government representing a democratic state as an actor. In turn, this removal of accountability may justify further state transgression. In addition, crypto-discourse emphasizes a negative individual freedom free from state coercion, at the expense of alternative understandings of freedom, such as a positive freedom where the state would be responsible of enabling individual freedom equally. These discursive strategies are not unique to crypto-discourse. They are, however, contextually specific.[19] By globalizing crypto-discourse, crypto-advocates may overrun culturally or contextually specific understandings of freedom.

That said, the purpose of this study is not to label all Cypherpunks and hackers as crypto-advocates, anarchists, or libertarians. Nor is it to present encryption as an inherently good or bad technology. Rather, the purpose is to demonstrate how the discursive work of prominent

[19] The discursive strategies present in the gun lobbying discourse of the National Rifle Association (NRA) that advocates for the constitutional right to bear arms would serve as an intriguing comparison in future research.

members of these discourse communities has produced a notion of freedom through the empty signifier "crypto" such that it is able to lend itself to a variety of differentiating political objectives. This process has not only taken place over time, but also over space as it has travelled from a specific Anglo-American context to now encompass many of the world's governments through both leaking practices and the harmonization of communication policy.

Throughout the trajectory mapped in Chapters 3, 4, and 5, I have shown how crypto-discourse derives from communities who articulated a social antagonism towards their nation-state and government in particular (the United States). I have also shown how crypto-advocates have revitalized this discourse in relation to mass leaks of secret documents in a manner that rearticulates this social antagonism towards governments in general. This is a strategic articulation in part possible due to an increasingly globalized communication technology and policy environment. For example, the empty signifier crypto lends itself well to the United Nations' representation of encryption as an essential tool for the protection of human rights (United Nations, 2015).[20] This articulation of crypto has hence universalized a particular political objective that now appears equal to other differential objectives. Consequently, this construction

[20] The Electronic Frontier Foundation among many other civil liberty and human rights organizations, participated in the multi-stakeholder consultation for the *Report of The Special Rapporteur on The Promotion and Protection of The Right to Freedom of Opinion and Expression, David Kaye* (2015).

of meaning excludes the possibility of a meaning of Internet freedom in which a state is actually responsible for ensuring the protection of individual freedoms and rights online.

The implications of this research calls for a more nuanced and contextualized debate about the role of democratic governments in upholding privacy rights and freedom of speech. Such a debate is especially pertinent in holding governments accountable for surveillance practices that infringe on personal privacy or hinder free speech in the context of legal anti-terrorism discourses. If the discursive struggle taking place in crypto is indeed overshadowing a governmental legitimacy crisis in the United States (Benkler, 2016), then crypto-discourse as currently articulated by crypto-advocates could deepen such democratic deficit by further removing responsibility from government. Furthermore, by making individual privacy an *individual* rather than state responsibility, crypto-discourse forwards a negative conception of freedom internationally. Future encryption policy should therefore seek to take into account national variations in perceptions of freedom and consider what should constitute desirable governmental responsibilities in a democracy.

Bibliography

2600 News | 2600. (n.d.). Retrieved May 5, 2016, from http://www.2600.com/

About IMMI. (n.d.). Retrieved from https://en.immi.is/about-immi/

Andersson, J. (2011, February). It takes (at least) two to tango. *Re-Public. Re-Imagining Democracy*, (6). Retrieved from https://web.archive.org/web/20130824095524/http://www.re-public.gr/en/?p=3878

Appelbaum, J. (2010). The Next HOPE Conference keynote presentation. New York. Retrieved from https://www.youtube.com/watch?v=aRVDIohWPVM

Assange, J. (2012a). *Cypherpunks: Freedom and the Future of the Internet*. New York ; London: OR Books.

Assange, J. (2012b). Introduction: A Call to Cryptographic Arms. In J. Assange, *Cypherpunks: Freedom and the Future of the Internet*. New York ; London: OR Books.

Assange, J. (Director). (2012c, July 29). The Julian Assange Show: Cypherpunks Uncut (p.1) [Television series episode]. In J. Assange (Producer), *The World Tomorrow*. London, UK: RT. Retrieved from http://assange.rt.com/cypherpunks-episode-eight-full-version-pt1/

Bakhtin, M. M. (1981). *The Dialogic Imagination: Four Essays*. (M. Holquist, Ed., C. Emerson & M. Holquist, Trans.). Austin: University of Texas Press.

Bakhtin, M. M. (1986). *Speech Genres and Other Late Essays*. (M. Holquist & C. Emerson, Eds., V. McGee, Trans.). Austin: University of Texas Press.

Bamford, J. (2014, September). Edward Snowden: The Untold Story. *Wired*, *22*(09). Retrieved from http://www.wired.com/2014/08/edward-snowden/

Barbrook, R. (2007). *Imaginary Futures: From Thinking Machines To The Global Village*. London: Pluto.

Barlow, J. P. (2001). A Declaration of The Independence of Cyberspace. In P. Ludlow (Ed.), *Crypto Anarchy, Cyberstates, and Pirate Utopias*. Cambridge, MA: MIT Press.

Barrett, B. (2016, March 30). The Apple-FBI Battle Is Over, But the New Crypto Wars Have Just Begun. Retrieved from http://www.wired.com/2016/03/apple-fbi-battle-crypto-wars-just-begun/

Barthes, R. (1972). Myth Today. In R. Barthes, A. Lavers (Trans.), *Mythologies* (pp. 109 – 161). New York: Hill and Wang.

Benkler, Y. (2016, February 22). We Cannot Trust Our Government, So We Must Trust the Technology. *The Guardian*. Retrieved from http://www.theguardian.com/us-news/2016/feb/22/snowden-government-trust-encryption-apple-fbi

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

Berlin, I. (1969). *Four Essays on Liberty*. London; New York: Oxford University Press.

Beyer, J. L. (2014). *Expect Us: Online Communities and Political Mobilization*. Oxford University Press.

Bey, H. (2001). The Temporary Autonomous Zone, Ontological Anarchy, Poetic Terrorism. In P. Ludlow (Ed.), *Crypto Anarchy, Cyberstates, and Pirate Utopias*. Cambridge, MA: A Bradford Book.

Boulware, J. (1995, October 11). Mondo 1995: Up and Down With the Next Millennium's First Magazine. *SF Weekly*. San Francisco, CA. Retrieved from http://www.sfweekly.com/sanfrancisco/mondo-1995/Content?oid=2132494

Braman, S. (2011). Anti-Terrorism and the Harmonization of Media and Communication Policy. In M. Raboy & R. Mansell (Eds.), *The Handbook of Global Media and Communication Policy* (pp. 486–504). Wiley-Blackwell.

Brand, S. (Ed.). (1985, May). Hackers' Conference 1984 - "Keep Designing": How the Information Economy is Being Created and Shaped by the Hacker Ethic. *The Whole Earth Review, 46,* 44-55. Retrieved from http://tech-insider.org/personal-computers/research/acrobat/8505-a.pdf

Brand, S. (1993, January 1). Scream of Consciousness. *Wired*, *1*(1). Retrieved from http://www.wired.com/1993/01/paglia/

Burkart, P. (2014). *Pirate Politics the New Information Policy Contests*. Cambridge, MA: The MIT Press.

Cameron, D. (2014, July 17). Everything You Need to Check Out at NYC's HOPE X Hacker Conference. Retrieved May 5, 2016, from http://www.dailydot.com/politics/best-speakers-events-hope-x-2014/

Carlbom, A. (2006). An Empty Signifier: The Blue-and-Yellow Islam of Sweden. *Journal of Muslim Minority Affairs*, *26*(2), 245–261.

Chacos, B. (2013, August 12). Meet Darknet, The Hidden, Anonymous Underbelly of The Searchable Web. *PCWorld*. Retrieved from http://www.pcworld.com/article/2046227/meet-darknet-the-hidden-anonymous-underbelly-of-the-searchable-web.html

Chaum, D. (1981). Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communications of the ACM*, *24*(2), 84–90.

Chaum, D. (1985). Security Without Identification: Transaction Systems to Make Big Brother Obsolete. *Communications of the ACM*, *28*(10), 1030–1044.

Clute, J., Langford, D., Nicholls, P., & Sleight, G. (Eds.). (2012). Cyberpunk. In *The Encyclopedia of Science Fiction* (3rd ed.). Retrieved from http://www.sf-encyclopedia.com/entry/cyberpunk

Coleman, E. G., & Golub, A. (2008). Hacker Practice: Moral Genres and the Cultural Articulation of Liberalism. *Anthropological Theory*, *8*(3), 255–277.

Dahlberg, L. (2011). Pirates, Partisans, and Politico-Juridical Space. *Law and Literature*, *23*(2), 262–281.

Dame-Boyle, A. (2015, April 16). EFF at 25: Remembering the Case that Established Code as Speech. Retrieved from https://www.eff.org/deeplinks/2015/04/remembering-case-established-code-speech

DeNardis, L. (2013). *The Global War for Internet Governance*. New Haven: Yale University Press.

Diffie, W., & Hellman, M. (1976a). New Directions in Cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644–654.

Diffie, W., & Hellman, M. E. (1976b). Multiuser Cryptographic Techniques. In *Proceedings of AFIPS* (pp. 109–112).

Dinev, T., Bellotto, M., Hart, P., Russo, V., & Serra, I. (2006). Internet Users' Privacy Concerns and Beliefs About Government Surveillance: An Exploratory Study of Differences Between Italy and the United States. *Journal of Global Information Management*, *14*(4), 57–93.

Eaton, J. (2016). Timeline of Edward Snowden's Revelations. *Al Jazeera America*. Retrieved from http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html

Edwards, P. N. (1997). *The Closed World Computers And The Politics of Discourse in Cold War America*. Cambridge, MA: MIT Press.

Feenberg, A. (1999). *Questioning technology*. London; New York: Taylor & Francis.

Free Software Foundation. (2007). The GNU General Public License v3.0. Free Software Foundation. Retrieved from http://www.gnu.org/copyleft/gpl.html

Froomkin, D., & McLauglin, J. (2016, February 26). FBI vs. Apple Establishes a New Phase of the Crypto Wars. *The Intercept*. Retrieved from https://theintercept.com/2016/02/26/fbi-vs-apple-post-crypto-wars/

Galveston, W. W. (2014, January 10). A Case for Clemency for Snowden. *The Economist*. Retrieved from http://www.economist.com/blogs/democracyinamerica/2014/01/whistleblowers-and-national-security

Gardner, M. (1977, August). A New Kind of Cypher That Would Take Millions of Years to Break. *Scientific American*, (8), 120–124.

Garside, J. (2015, May 25). Philip Zimmermann: King of Encryption Reveals His Fears for Privacy. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2015/may/25/philip-zimmermann-king-encryption-reveals-fears-privacy

Gillespie, T. (2006). Engineering a Principle "End-to-End" in the Design of the Internet. *Social Studies of Science*, *36*(3), 427–457.

Gilmore, J. (1991, March). Privacy, Technology, and the Open Society. Speech presented at the First Conference on Computers, Freedom, and Privacy, Burlinggame, California. Retrieved from http://www.toad.com/gnu/cfp.talk.txt

Gilmore, J. (n.d.). John Gilmore's home page. Retrieved February 26, 2016, from http://www.toad.com/gnu/

Greenberg, A. (2012a). *This Machine Kills Secrets* [Video trailer]. Pilcrow Studio. Retrieved from http://www.thismachinekillssecrets.com/video-trailer/

Greenberg, A. (2012b). *This Machine Kills Secrets: How WikiLeakers, Cypherpunks And Hacktivists Aim to Free The World's Information*. New York: Dutton.

Greenberg, A. (2015a, January 9). Why the Silk Road Trial Matters. *Wired*. Retrieved from http://www.wired.com/2015/01/why-silk-road-trial-matters/

Greenberg, A. (2015b, January 28). No, Department of Justice, 80 Percent of Tor Traffic Is Not Child Porn. *Wired*. Retrieved from http://www.wired.com/2015/01/department-justice-80-percent-tor-traffic-child-porn/

Greenwald, G. (2013, June 6). NSA Collecting Phone Records of Millions of Verizon Customers Daily. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Hall, S. (1996). *Race, the Floating Signifier* [VHS]. Goldsmith's College, New Cross, London.

Hirsch, A. (2010, July 12). Iceland Aims to Become a Legal Safe Haven for Journalists. *The Guardian*. Retrieved from http://www.theguardian.com/media/2010/jul/12/iceland-legal-haven-journalists-immi

Howarth, D. R. (2000). *Discourse*. Buckingham [England]; Philadelphia, PA: Open University Press.

Hughes, E. (1993, March 9). RANTS: A Cypherpunk's Manifesto. Posted to the Cypherpunk Mailing List.

Human Rights Foundation. (2013, September 10). Encrypted Communications Gives Voice to Dissidents. Retrieved May 5, 2016, from https://humanrightsfoundation.org/news/encrypted-communications-gives-voice-to-dissidents-00317

IACR. (n.d.). History of IACR Conferences and Workshops. Retrieved April 11, 2016, from https://www.iacr.org/conferences/history.html

Jørgensen, M., & Phillips, L. (2002). Laclau and Mouffe's Discourse Theory. In *Discourse Analysis as Theory And Method*. London; Thousand Oaks, CA: Sage Publications.

Kapor, M. (1991). Civil Liberties in Cyberspace: When Does Hacking Turn From an Exercise of Civil Liberties Into Crime? *Scientific American*, *265*(3), 158–164.

Kelty, C. M. (2005). Geeks, Social Imaginaries, and Recursive Publics. *CUAN Cultural Anthropology*, *20*(2), 185–214.

Kelty, C. M. (2008). *Two Bits: The Cultural Significance of Free Software*. Durham: Duke University Press Books.

Knibbs, K. (2015, February 6). How the Silk Road Trial Could Lead to a Dangerous Legal Precedent. *Gizmodo.* Retrieved from http://gizmodo.com/how-the-silk-road-trial-set-a-dangerous-legal-precedent-1684208875

Laclau, E. (1996). Why Do Empty Signifiers Matter to Politics? In *Emancipation(s)* (pp. 36 – 46). New York: Verso.

Laclau, E., & Mouffe, C. (1985a). Beyond The Positivity of The Social: Antagonisms and Hegemony. In *Hegemony and Socialist Strategy: Towards a Radical Democratic Politics* (pp. 93 – 148). London: Verso.

Laclau, E., & Mouffe, C. (1985b). Hegemony and Radical Democracy. In *Hegemony and Socialist Strategy: Towards a Radical Democratic Politics* (pp. 149 – 194). London: Verso.

Laclau, E., & Mouffe, C. (1985c). *Hegemony and Socialist Strategy: Towards a Radical Democratic Politics*. London: Verso.

Lee, D. (2016, February 17). Apple Ordered to Unlock San Bernardino Gunman’s Phone. *BBC News*. Retrieved from http://www.bbc.com/news/technology-35593048

Lentz, B. (2013). Excavating Historicity in the U.S. Network Neutrality Debate: An Interpretive Perspective on Policy Change. *Communication, Culture & Critique*, *6*(4), 568–597.

Lesnes, C. (2013, June 6). L’opérateur téléphonique Verizon fournit à la NSA des informations sur des millions d’abonnés. *Le Monde.fr*. Retrieved from http://www.lemonde.fr/international/article/2013/06/06/l-operateur-telephonique-verizon-fournit-a-la-nsa-des-informations-sur-des-millions-d-abonnes_3425394_3210.html

Levy, S. (1984). *Hackers: Heroes of the Computer Revolution*. Garden City, NY: Anchor Press/Doubleday.

Levy, S. (1993). Crypto Rebels. *Wired*, *1*(2), 54–61.

Levy, S. (1994a). E-Money (That’s What I Want). *Wired*, *2*(12). Retrieved from http://archive.wired.com/wired/archive//2.12/emoney_pr.html

Levy, S. (1994b, November). Cypher Wars. *Wired*, *2*(11). Retrieved from http://archive.wired.com/wired/archive//2.11/cypher.wars.html?person=phil_zimmermann&topic_set=wiredpeople

Levy, S. (2001). *Crypto: How the Code Rebels Beat the Government - Saving Privacy in the Digital Age*. New York: Viking Penguin. Retrieved from http://www.penguin.com/book/crypto-by-steven-levy/9780140244328

Lichtblau, E., & Benner, K. (2016, February 17). Apple Fights Order to Unlock San Bernardino Gunman’s iPhone. *The New York Times*. Retrieved from http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html

Ludlow, P. (Ed.). (1996). *High Noon on The Electronic Frontier : Conceptual Issues in Cyberspace*. Cambridge, MA: MIT Press.

Ludlow, P. (2001). *Crypto Anarchy, Cyberstates, and Pirate Utopias*. Cambridge, MA: MIT Press.

Malcolmson, S. (2016). *Splinternet: How Geopolitics And Commerce Are Fragmenting The World Wide Web*. New York: OR Books.

Marchart, O. (2012). Elements of Protest: Politics and Culture in Laclau's Theory of Populist Reason. *Cultural Studies*, *26*(2-3), 223–241.

Marx, K., & Engels, F. (2008). *The Communist Manifesto*. London: Pluto Press.

May, T. C. (1992, November 22). The Crypto Anarchist Manifesto. Retrieved from http://www.activism.net/cypherpunk/crypto-anarchy.html

May, T. C. (1994, September 10). The Cyphernomicon: Cypherpunks FAQ and More. Retrieved from http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/cyphernomicon/CP-FAQ

McKelvey, F., & Beyer, J. L. (2015). You Are Not Welcome Among Us: Pirates and the State. *International Journal of Communication*, *9*, 890–908.

Methmann, C. P. (2010). "Climate Protection" as Empty Signifier: A Discourse Theoretical Perspective on Climate Mainstreaming in World Politics. *Millennium: Journal of International Studies*, *39*(2), 345–372.

Mirkinson, J. (2014, August 13). Wired's Edward Snowden Cover Shows Him Holding The American Flag. *The Huffington Post*. Retrieved from http://www.huffingtonpost.com/2014/08/13/wired-edward-snowden-cover-american-flag_n_5674454.html

Moore, D., & Rid, T. (2016). Cryptopolitik and the Darknet. *Survival: Global Politics and Strategy*, *58*(1).

National Archives. (n.d.). Pentagon Papers. Retrieved May 5, 2016, from https://www.archives.gov/research/pentagon-papers/

National Science Foundation. (n.d.). The Launch of NSFNET. Retrieved April 30, 2016, from http://www.nsf.gov/about/history/nsf0050/internet/launch.htm

Norval, A. J. (1996). *Deconstructing Apartheid Discourse*. London: Verso.

Offe, C. (2009). Governance: An "Empty Signifier"? *Constellations*, *16*(4), 550–562.

OHCHR. The Right to Privacy in the Digital Age, A/HRC/27/37 § Human Rights Council 16 (2014).

Onion Routing: History. (2005). Retrieved April 15, 2016, from http://www.onion-router.net/History.html

The Economist. (2016, February 27). On The Stump. Why Tech Bosses Are Playing at Being Statesmen. *The Economist.*

Pagliery, J. (2016, February 17). Edward Snowden Defends Apple in Fight Against FBI. *CNNMoney*. Retrieved from http://money.cnn.com/2016/02/17/technology/apple-fbi-phone-unlock-edward-snowden/index.html

Pinch, T. J., & Bijker, W. E. (1984). The Social Construction of Facts and Artefacts: or How the Sociology of Science and the Sociology of Technology might Benefit Each Other. *Social Studies of Science*, *14*(3), 399–441.

Platon. (2013). *Photographer Platon Reveals Power Through Portrait*. Wired Business Conference 2013 presentation. New York. Retrieved from http://library.fora.tv/2013/05/07/Photographer_Platon_Reveals_Power_Through_Portrait

Rivest, R., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, *21*(2), 120–126.

Schneier, B. (1996). Cryptographic Protocols. In *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (2nd ed., p. 758). John Wiley & Sons.

Schwarz, J. A., Burkart, P., Aufderheide, P., Jaszi, P., Kelty, C., & Coleman, G. (2015). Piracy and Social Change. *Popular Communication: The International Journal of Media and Culture*, *13*(1), 1–5.

Slack, J. D. (1989). Contextualizing Technology. In B. Dervin, *Rethinking communication* (Vol. 2, pp. 329–45). Newbury Park, CA; [New Brunswick, NJ]: SAGE publications ; Published in cooperation with the International Communication Association.

Snowden, E. (2014). HOPE X Conference keynote presentation. Retrieved from https://www.youtube.com/watch?v=6PHFjLkwOZE

Snowden, E. (2016, February 16). The @FBI is creating a world where citizens rely on #Apple to defend their rights, rather than the other way around. https://t.co/vdjB6CuB7k [Microblog]. Retrieved from https://twitter.com/Snowden/status/699984388067557376

Söderberg, J. (2013). Determining Social Change: The role of Technological Determinism in The Collective Action Framing of Hackers. *New Media & Society*, *15*(8), 1277–1293.

Sterling, B. (1992). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier* (1st ed.). New York, NY: Bantam.

Swales, J. M. (1990). *Genre Analysis: English in Academic And Research Settings*. Cambridge [England]; New York: Cambridge University Press.

Taylor, C. (1989). *Sources of The Self: The Making of The Modern Identity*. Cambridge, MA: Harvard University Press.

Taylor, C. (2004). *Modern Social Imaginaries*. Durham: Duke University Press.

The Electronic Frontier Foundation. (n.d.). What is a Tor Relay? Retrieved April 15, 2016, from https://www.eff.org/torchallenge/what-is-tor.html

The Tor Project, Inc. (n.d.-a). Tor Project: Core People. Retrieved April 15, 2016, from https://www.torproject.org/about/corepeople

The Tor Project, Inc. (n.d.-b). Tor Project: Overview [The Tor Project]. Retrieved April 15, 2016, from https://www.torproject.org/about/overview.html.en

The Tor Project, Inc. (n.d.-c). Tor Project: Tor Animation. Retrieved April 15, 2016, from https://www.torproject.org/press/video.html.en

The Tor Project, Inc. (n.d.-d). Tor: Sponsors. Retrieved April 15, 2016, from https://www.torproject.org/about/sponsors.html.en

Tully, J. (2013). Two Concepts of Liberty" in Context. In B. D. Baum & R. Nichols (Eds.), *Isaiah Berlin and The Politics of Freedom: "Two Concepts of Liberty" 50 Years Later*. New York, NY: Routledge.

Turner, F. (2006). *From Counterculture to Cyberculture: Stewart Brand, The Whole Earth Network, And The rise of Digital Utopianism*. Chicago: University of Chicago Press.

United Nations. Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including The Right to Development, Agenda item 3 A/HRC/20/L.13 § Human Rights Council 3 (2012).

United Nations. Resolution Adopted by the General Assembly on 18 December 2013 [on the report of the Third Committee (A/68/456/Add.2)], Agenda item 69 A/RES/68/167 3 (2014).

United Nations. Report of The Special Rapporteur on The Promotion and Protection of The Right to Freedom of Opinion and Expression, David Kaye*, Agenda item 3 A/HRC/29/32 § Human Rights Council 21 (2015).

Vallance, C. (2010, August 19). Wikileaks Encryption Use Offers "Legal Challenge." *BBC News*. Retrieved from http://www.bbc.com/news/technology-11026659

Van der Sar, E. (2014, January 4). Top 10 Most Popular Torrent Sites of 2014. *TorrentFreak*. Retrieved from https://torrentfreak.com/top-10-popular-torrent-sites-2014-140104/

Vezovnik, A. (2013). Representational Discourses on the Erased of Slovenia: From Human Rights to Humanitarian Victimization. *Journal of Language and Politics*, *12*(4), 606–625.

Warren, J., Thorwaldson, J., & Koball, B. (Eds.). (1991). The First Conference on Computers Freedom and Privacy. In *The First Conference on Computers, Freedom Privacy, 1991. Proceedings* (pp. i–iii). IEEE Computer Society Press.

What is WikiLeaks. (n.d.). Retrieved February 18, 2016, from https://wikileaks.org/What-is-Wikileaks.html

Winner, L. (1986). Do Artifacts Have Politics? In *Whale and the Reactor : A Search for Limits in an Age of High Technology*. Chicago: University of Chicago Press.

Wong, N., Silvers, R., & Opsahl, K. (Eds.). (2003). *Electronic Media and Privacy Law Handbook*. San Francisco, CA: Perkins Coie LLP.

Wullweber, J. (2015). Global Politics and Empty Signifiers: The Political Construction of High Technology. *Critical Policy Studies*, *9*(1), 78–96.

Zahorsky, I. (2011, August 1). Peace and Conflict Monitor, Tor, Anonymity, and the Arab Spring: An Interview with Jacob Appelbaum [University for Peace]. Retrieved from http://www.monitor.upeace.org/innerpg.cfm?id_article=816

Zimmermann, P. (1995). Author's preface to the book: "PGP Source Code and Internals." Retrieved April 8, 2016, from https://www.philzimmermann.com/EN/essays/BookPreface.html

Zylberberg, H. (2016, March 3). Techno-Populism Won't Help in the Apple vs FBI Debate. *Harvard Kennedy School Review*. Retrieved from http://harvardkennedyschoolreview.com/techno-populism-wont-help-in-the-apple-vs-fbi-debate/

Appendix

Table 1 Crypto-discourse timeline: Key discursive events per discourse community as illustrated in Figure (1975 – 2015)

TIMELINE			DISCOURSE COMMUNITY			
Number	Year	Letter	The State	Civil Rights Advocates	Cryptographers and Hackers	Technology Journalists
1	1976				**New Directions in Cryptography** Whitfield Diffie and Martin Hellman introduce public-key cryptography to the academic community in a journal article entitled *New Directions in Cryptography.*	
2	1977				**Mathematical Games** Martin Gardner describes the RSA algorithm in popular science magazine *Scientific American.*	
3	1978				**A Method for Obtaining Digital Signatures and Public-Key Cryptosystems** Ron Rivest, Adi Shamir, and Leonard Adleman introduce the RSA algorithm in a journal article entitled *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.*	
4	1981				**Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms** Berkley cryptographer David Chaum introduces anonymous communication based on public-key cryptography in a journal article.	
5	1984	a.			**The Hackers' Conference** Members of the Whole Earth network, hacker groups, and cryptographers organize the Hackers' Conference.	
		b.			**Hackers: Heroes of the Computer Revolution** Technology reporter Steven Levy publishes *Hackers: Heroes of the Computer Revolution.*	
6	1985	a.			**The Whole Earth 'Lectronic Link (WELL)** Stewart Brand and the Whole Earth network start using a Bulletin Board System (BBS) entitled the Whole Earth 'Lectronic Link (WELL).	
		b.			**Security Without Identification: Transaction Systems to Make Big Brother Obsolete** Berkley cryptographer David Chaum publishes academic article introducing digital pseudonyms and anonymous transactions.	
7	1986	a.	**Internet** NSFnet connects with ARPANET, creates Internet.			

		b.	**Computer Fraud and Abuse Act (CFAA)** The U.S. government passes the Computer Fraud and Abuse Act (CFAA).			
8	1990			**Electronic Frontier Foundation (EFF)** Mitchell Kapor, John Perry Barlow and John Gilmore found the Electronic Frontier Foundation (EFF) that will engage in legal battles with the U.S. Department of Justice called the "Crypto Wars".		
9	1991	a.	**Senate Bill 266** The U.S. government proposes amendments to counter-terrorist Senate Bill 266.			
		b.			**Pretty Good Privacy (PGP)** Phil Zimmermann develops and spreads Pretty Good Privacy (PGP) encryption software.	
		c.		**The First Conference of Computers, Freedom, and Privacy** Technology reporter Jim Warren initiates the First Conference of Computers, Freedom, and Privacy. Cryptographers, hackers, and members of the EFF attend and present at the conference.		
10	1992	a.		**The Cypherpunk Mailing List** Tim C. May, Eric Hughes, and EFF founder and WELL member John Gilmore found the Cypherpunk Mailing List.		
		b.			**The Crypto-Anarchist Manifesto** Tim C. May publishes "The Crypto-Anarchist Manifesto" on the Cypherpunk Mailing List.	
11	1993	a.			**A Cypherpunk's Manifesto** Eric Hughes publishes "A Cypherpunk's Manifesto" on the Cypherpunk Mailing List.	
		b.				**Wired magazine** Steven Kelly and other members of WELL found *Wired* magazine.
		c.		**Crypto Rebels** *Wired* reporter Steven Levy publishes "Crypto Rebels" in the second issue of *Wired* magazine.		
		d.		**Wired magazine cover issue 1.02** The founders of the Cypherpunks (Tim C. May, Eric Hughes, and John Gilmore) feature the cover of *Wired* magazine.		
12	1994	a.			**Cyphernomicon** Tim C. May publishes the "Cyphernomicon", a Cypherpunk FAQ, on The Cypherpunk Mailing List.	
		b.			**HOPE Conference** The first HOPE (Hackers on Planet Earth) Conference in celebration of hacker magazine *2600: The Hacker Quarterly.*	
13	1996			**A Declaration of the Independence of**		

				Cyberspace John Perry Barlow publishes "A Declaration of the Independence of Cyberspace" online.		
14	2001	a.	**The U.S. Patriot Act** The U.S. government passes the U.S. Patriot Act following the 9/11 terrorist attacks in the United States.			
		b.	**UN Resolution (1373)** The United Nations passes an anti-terrorist resolution drafted by U.S. and U.K. governments.			
		c.		**Crypto: How the Code Rebels Beat the Government, Saving Privacy in the Digital Age** *Wired* reporter Steven Levy publishes *Crypto: How the Code Rebels Beat the Government, Saving Privacy in the Digital Age* as a book.		
15	2006	a.	**The Tor Project** The U.S. government funded The Onion Router develops into the Tor Project. MIT crypto-scientists Roger Dingledine, Nick Mathewson, and Paul Syverson develop the Tor Project. The EFF funds the Tor Project.			
		b.		**Wikileaks** Cypherpunk Julian Assange founds Wikileaks		
16	2010	a.		**The Collateral Murder Video** Wikileaks publishes the *Collateral Murder Video.*		
		b.		**HOPE Conference** Tor spokesperson Jake Appelbaum represents WikiLeaks at HOPE conference.		
17	2011			**Cablegate** Wikileaks publishes *Cablegate.*		
18	2012	a.		**The World Tomorrow** Julian Assange broadcasts his own news show entitled *The World Tomorrow*, or *The Julian Assange Show*, on Russia Today (RT) news network.		
		b.		**Cypherpunks: Freedom and the Future of the Internet** Cypherpunk Julian Assange publishes *Cypherpunks: Freedom and the Future of the Internet.*		
		c.		**This Machine Kills Secrets: How Wikileakers, Cypherpunks, and Hactivists Aim to Free the World's Information** *Wired* reporter Andy Greenberg publishes *This Machine Kills Secrets: How Wikileakers, Cypherpunks, and Hactivists Aim to Free the World's Information.*		
19	2013			**The Snowden Leaks** CIA contractor Edward Snowden leaks confidential documents.		
20	2014	a.		**Edward Snowden: The Untold Story** James Bamford publishes a full-length interview with Edward Snowden in *Wired* magazine issue 22.09.		
		b.		**Wired magazine cover issue 22.09** Edward Snowden features the cover of *Wired* magazine.		
		C.		**HOPE X Conference** The Hope X conference features whistleblowers Edward Snowden, Daniel Ellsberg, and Thomas Drake.		