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

Paper prepared for the 11th Annual GigaNet Symposium
5 December 2016, Guadalajara, Mexico

Isadora Hellegren, McGill University, Montreal, Canada

Introduction

"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.

Stakeholders attempt to construct meaning through Internet-specific technologies in several ways. Social actors such as computer scientists, software developers, and hackers design the architecture of the Internet by writing protocols and algorithms that structure how information is exchanged over the Internet. Take for example the BitTorrent Protocol that allows for peer-to-peer file sharing, or the RSA algorithm that protects data in transmission. Other actors, such as policy-makers on national and international level, seek to define what constitutes appropriate online practices through policy regulation. Media representations of Internet-specific technologies, practices, and their users shape understandings of the Internet. 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. Efforts to shape the form and function of Internet-specific technologies are hence not separate from attempts to construct meaning through them. 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.

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). Gillespie hence 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). This paper addresses a meaning-making process through crypto. *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. While the design function of this software may have material impacts (Winner, 1986), the design or use of a technology like computer software is never inherently positive or negative (Pinch & Bijker, 1984). Different discourses in various contexts have long competed to establish the meaning of encryption. For example, until the 1990s, the Unites States government classified encryption as war materiel, which made encryption algorithms illegal to export. In a series of legal battles that took place in the early 1990s, namely the Crypto Wars (Barrett, 2016; Froomkin & McLauglin, 2016), online rights advocates and the United States Department of Justice disputed the legal status of encryption software in court (Barrett, 2016; Froomkin & McLauglin, 2016).

More recently, the United Nations also contributed to the debate about the relationship between Internet freedom and encryption software. 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. This report establishes a direct relationship between encryption software and human rights as it states that encryption is essential to safeguard the human right to freedom of opinion and expression (United Nations, 2015). Struggles to define the meaning of encryption software do not, however, only take place in courtrooms and policy-making processes. They also take place in academic journals, conferences, online spaces, and in technology magazines. Cryptographers, hackers, online rights advocates, and journalists alike have long sought to challenge the meaning of encryption as war material by establishing a relationship between the technology and online rights. The representation of encryption software thus serves as a battlefield in a larger discursive struggle to define the meaning of Internet freedom.

This paper explores how specific communities of participants in the Internet governance debate, namely public-key cryptography advocates, have constructed a discourse in which encryption software serves as an enabler of freedom. The study 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. 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. Members of the Cypherpunk community have

actively advanced a negative meaning of crypto and freedom that positions the state as their adversary—an antagonist—in debates about online privacy.[1] 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. 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. Discourse theory provides conceptual tools that help advance this enhanced understanding.

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. 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). 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, and consequently to debates about what signifies Internet freedom. Yet, I argue, 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.

By conceptualizing "crypto-freedom" in discourse-theoretical terms, this paper 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. 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. Such a representation has normative implications for future policy regarding expectations on state authorities to uphold online rights.

---

[1] In this paper, 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 paper.

[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 article, 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). Drawing on Laclau and Mouffe's theory of discourse, I analyze these events in order to explore crypto-advocates' discursive strategies to construct meaning through crypto in relation to the state.

The paper proceeds as follows. I begin by providing an overview of previous research on Cypherpunks and the concept of crypto-freedom underpinning this study. Next, I describe the discourse theoretical framework that guides my research of crypto-discourse. I then present the evolution of crypto-discourse as comprised of three periods representing three pivotal moments in the evolution of the crypto-discourse: *the origins*, *crystallization*, and *revitalization*. I conclude with a summary of my findings and a discussion of their relevance to future policy relating to the use of encryption software.

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 (Coleman & Golub, 2008; Kelty, 2005; McKelvey & Beyer, 2015). 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). Through a topography of hacker moral genres 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).

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).[3]

Hackers, geeks, or other communities are united through a shared affinity with Internet specific technologies, as well as a shared social imaginary (Kelty, 2005, 2008). Anthropologist Christopher Kelty's major contribution to cultural studies of hacking is the notion of "recursive publics" to describe how geeks relate to free and open software, and to each other. These publics share a concern for their main mechanism for communication: the Internet and Internet specific technologies (Kelty, 2005). 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). The development of encryption software is thus equally significant to this study of crypto-discourse as is other forms of text or speech. 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, 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). Scholars McKelvey and Beyer, trace artifacts such as *The Cypherpunk Mailing List* that contain articulations of a political philosophy arising prior and parallel to 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 note that while pirate imagery inspired the construction of a social imaginary among 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). Similar to the Cypherpunks, "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 ways that pirates, geeks, and hackers identify as members of communities vary broadly. (Andersson, 2011; Beyer, 2014; Coleman & Golub, 2008; Dahlberg, 2011; McKelvey & Beyer, 2015; Schwarz et al., 2015).[4] Hackers' technology-related practices

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

[4] For sake of consistency and clarity, I will hereafter use the term "hacker" throughout this paper, to refer to members of communities that unite in their practices of developing and modifying internet-specific technologies.

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. 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).

I have consulted this aforementioned research in order to foreground significant discursive practices that unite hackers and related groups as communities. This scholarship provides insight into the historical and cultural conditions pertinent to my analysis of crypto-discourse. In my analysis of crypto-discourse, I build 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.

Research Design

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 order to investigate how crypto-advocates, and in particular members of the Cypherpunk community, have articulated 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 (Jørgensen & Phillips, 2002; Laclau, 1996; Laclau & Mouffe, 1985c).

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 struggles to determine meaning, actors articulate social antagonisms. *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). Articulations of social antagonisms take place in discourses where social actors

experience that their identities cannot be fulfilled due to this "Other". Conceptualizing crypto-advocate practices as articulations of social antagonism helps us understand the functions of crypto-discourse.

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 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). To understand how crypto-advocates have constructed crypto-discourse, I examine how they have emptied the signifier "crypto" of its 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. 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).

The concept of empty signifiers lends itself particularly well to understand Internet-related debates as it serves to illustrate the contingency of meaning-making processes. Lentz states for example that the term "neutral" functions in a similar manner to an empty signifier in the historicity of the net neutrality debate (2013). While advancing intertextuality as a theoretical approach to study policy change, Becky Lentz provides an example of how definitions in policy debates over net neutrality serve as critical nodal points. 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. Situating empty signifiers in their historical context is thus necessary to understand their evolution over time. This approach has informed my research design.

In this paper, I conceptualize "crypto", short for cryptography, as an empty signifier. 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.

Lastly, in order to trace the evolution of crypto and how it operates as an empty signifier, I employ the logics of difference and equivalence. The *logics of difference and equivalence* that are at work in the empty signifier function simultaneously through the passage of antagonism. 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 differential 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 (Norval, 1996; Vezovnik, 2013).

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. *Discourse communities*, like hacker moral genres (Coleman & Golub, 2008) or recursive publics (Kelty, 2005), are bound together through their discursive practices that govern the rules and conditions for meaning-making processes within them (Swales, 1990). Members of a discourse community may engage in different practices at different times. My separation of these communities is 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 paper, I focus particular attention on the discursive work of Cypherpunks as well as technology journalists at *Wired* magazine and how their discursive practices have sought to establish meaning in the empty signifier "crypto". The Cypherpunks only formally formed in 1992, 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, 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 (Coleman & Golub, 2008; McKelvey & Beyer, 2015).

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 (Assange, 2012b; Hughes, 1993a; May, 1992, 1994). 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, especially Steven Levy, and his role in constructing crypto-discourse.

The second category of objects includes covers, articles, and books produced by Steven Levy and other *Wired* reporters that feature prominent crypto-advocates (Bamford, 2014; Gardner, 1977; "Hackers' Conference 1984," 1985; Levy, 1993, 1994b, 2001). 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.

The Crypto-Discourse Timeline

The Origins of Crypto-Discourse (1975 – 1990)

In this section, I establish the historical context in which social antagonism sets the stage for the emergence of crypto as an empty signifier. 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. This was an era characterized by a "closed world discourse" capable of encompassing all political struggles taking place in that context (Edwards, 1997). In this context, the US government developed Arpanet, the predecessor to the Internet, in 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.

Through conference and journal publications, cryptographers at MIT and Stanford University challenged the state's dominant position in defining encryption. 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. As Diffie and Hellman presented their proposed solution to the scientific community in 1976 (Diffie & Hellman, 1976a, 1976b; Schneier, 1996), they defined the problem 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 an article that described the RSA algorithm, making the concept of public-key encryption possible to implement (Rivest, Shamir, & Adleman, 1978). In this publication, 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. A description of RSA also reached a broader audience, through Martin Gardner's column "Mathematical

Games", in the popular technology magazine *Scientific American*, in 1977. Gardner described the algorithm as: "A new kind of cipher that would take millions of years to break" (Gardner, 1977), making it appear indestructible. 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. In what would become widely influential writings among hackers and cryptographers, David Chaum established a relationship between anonymity, privacy, and security. Chaum offered a way to "make big brother obsolete", as he introduced anonymous transaction systems that would lay the conceptual foundations of decentralized digital payment systems such as crypto-currencies. These anonymous transaction systems, he argued, would prevent corporations and the government from collecting and misusing information about individual behaviour. 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.

During the origins of crypto-discourse, many American citizens also began to express mistrust of their government, as they learned about so-called state secrets. A few years earlier, military analyst Daniel Ellsberg had leaked the "Pentagon Papers": top-secret documents that revealed government wrongdoings in relation to the Vietnam War (National Archives, n.d.). 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. The Whole Earth network, a countercultural discourse community of journalists, communalists, and entrepreneurs in San Francisco, turned to technology as a means to achieve societal change. Stewart Brand founded the *Whole Earth Catalog* in the 1960s in San Francisco that 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 portrayed technology as a countercultural force in and of itself (Turner, 2006). The Whole Earth network united in their celebration of high technology and a decentralized system of collaboration (Turner, 2005). According to technology journalist Steven Levy, hackers also united through these shared values.

Technology journalist Steven Levy significantly added to this articulated relationship between technology and freedom through his writing on hackers. In 1984, Levy published *Hackers: Heroes of the Computer Revolution* 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". The Hacker Ethic constituted a set of "concepts, beliefs, and mores" that Levy considered shared among hackers (Levy, 1984, p. 27), such as a belief that access to both computers and information should be unlimited: "all information should be free" (Levy, 1984, p. 28). Through his book, Levy accomplishes several things. First, he articulates a representation of 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 ("Hackers' Conference 1984" 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 ("Hackers' Conference 1984," 1985; Malcolmson, 2016). The Hackers' Conference 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" ("Hackers' Conference 1984," 1985), attributing to information a will of its own, a form of necessity. 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. 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 WELL, as a computer conferencing system, followed "a countercultural conception of community and a cybernetic vision of control" (Turner, 2006, p. 143).[5] 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 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 (Malcolmson, 2016; National Science Foundation, n.d.). The U.S. government extended the definitions of what constituted illegal online activity in the Computer Fraud and Abuse Act (CFAA). This act criminalized much hacker activity, including accessing computers and networks without authorization (Wong, Silvers, & Opsahl, 2003). The WELL paid close attention to these restrictions as a tension arose 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 (Sterling, 1992). In the 1990s, this battle would transform into a series of legal battles using crypto as their battlefield.

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

The aforementioned events and practices would become crucial to the production of crypto-discourse as members of the hacker community (including cryptographers) and the Whole Earth network met and merged. These articulations of social antagonism towards the state led to the genesis of crypto as an empty signifier.

The Crystallization of Crypto-Discourse (1990 – 2000)

In this section, I present the period of crystallization of crypto-discourse by reviewing the events and discursive work that solidifies crypto-discourse during the early 1990s. The U.S. government played an essential role 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. The 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. In 1991, as a direct response to a proposed amendment to counter-terrorist Senate Bill 266, Zimmermann developed public-key encryption software entitled Pretty Good Privacy (PGP). Zimmermann and other cryptographers circulated PGP widely through bulletin board systems and other forums, as well as through journalists. 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 over the Internet. 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) felt targeted by the government's actions. In 1990, Mitchell Kapor from the Lotus Development Corporation, together with John Perry Barlow, lyricist for the Grateful Dead, and John Gilmore, software developer from Sun Microsystems, founded the civil liberties organization the Electronic Frontier Foundation (EFF). EFF fought for civil liberties online in the 1990s' Crypto Wars, 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. During these battles, encryption source code went from being classified as munitions, to speech protected by the First Amendment (Bennett, 2008). Besides legal disputes, online rights advocates also advanced their articulations of crypto through other practices, such as conference presentations.

At the First Conference of Computers, Freedom, and Privacy (1991), 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. Gilmore

used a number of strategies in his articulation of what constitutes a desirable society with such a freedom. Gilmore excludes for example the possibility of trust in government by juxtaposing trust in government 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). He yet refers to aspects such as privacy, financial privacy, and anonymity as individual "rights" that everyone should be entitled to by law, whether manmade or physical, although such rights are defined by the former. While these are examples articulating a relationship between encryption and online rights, a group of individuals including Gilmore, took it upon themselves to establish the meaning of the term "crypto", namely the Cypherpunks.

The discursive work of the Cypherpunk community constitutes a crystallizing moment in crypto-discourse. 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). The name "Cypherpunk", is a direct spin-off of "cyberpunk" (Boulware, 1995). 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.

The Cypherpunk Mailing List served several functions. Originally comprising a handful of members, the list eventually grew to accommodate thousands of members that would continue to contribute to the list until the early 2000s (Greenberg, 2012). 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" posted to the list, that "Cypherpunks write code" (Hughes, 1993b), 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.[6] 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.[7]

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

[7] 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 manifestos have circulated the Internet and come to signify the practices of the entire movement. They utilize discursive strategies that construct an understanding that crypto anarchy is inevitable while simultaneously depicting Cypherpunks as its liberators. The "Crypto Anarchist Manifesto", for example advances the understanding of crypto as a productive force of its own. May describes an anticipated "social and economic revolution" brought about by encryption (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. 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.

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. A key discursive artifact in the crystallization of crypto-discourse is the second issue of Wired magazine 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 portrays the Cypherpunks as rebels and 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. In Crypto: How the Code Rebels Beat the Government, Saving Privacy in the Digital Age (Levy, 2001), Levy assembles the story of the cryptographers, the civil libertarians, and Cypherpunks behind the empty signifier crypto in one popular journalistic account. Through the works of Levy (Levy, 1994a, 1994b, 2001), the Cypherpunks became synonymous with crypto, privacy, anonymity, free speech, American, and Internet freedom. Levy spread awareness of the Cypherpunks to a broader public, in a manner that popularized the movement, and sedimented the chains of equivalence that had been articulated by the Cypherpunks.

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.

The Revitalization of Crypto-Discourse (2000 – 2015)

In this final section of the crypto-discourse timeline, 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 U.S. government plays a significant role 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, the Bush administration, together with the United Nations, constructed an anti-terrorist legal discourse – The War on Terror - that affected global communication policy. This discourse had direct implications on global communications policy regulating technology and 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.

New uses of encryption such as onion routing and leaking offer a competing discourse to the anti-terrorist legal discourse and extend the articulation of crypto. *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. 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.). 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; Greenberg, 2013; Knibbs, 2015; Moore & Rid, 2016). 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 addressed these issues, contending that this representation is a strategy repeatedly used to discredit the use of privacy-enhancing technologies as criminal. Appelbaum invokes crypto-discourse as articulated by May, in his response to representations of onion routing, by subordinating the importance of arresting criminals to the right to free speech and privacy. 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 chain of equivalence articulated by Tor 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.[8] WikiLeaks is a media organization founded in 2006 by Julian Assange, 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* in 2010, showing Iraqi civilians being shot by American soldiers and *Cablegate* in 2011, hundreds of diplomatic cables released in cooperation with several European and North American news organizations. These mass leaks, as well as those of former CIA contractor Edward Snowden in 2013 that showed how governments world-wide, 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), were possible because of encryption software.

This encryption enabled form of mega-leaks re-invigorated crypto-discourse while simultaneously extending it by establishing a relationship between encryption and journalistic practices. Julian 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. Similarly, Snowden's 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 relation to these leaks, Wikileaks and Snowden extend the meaning of encryption to include the role of journalists as watchdogs of government wrongdoings.

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*. 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

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

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 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. Besides Assange's own discursive work, *Wired* journalists participated in revitalizing crypto-discourse.

Following the mass disclosures, technology journalists took special interest in the leaking phenomenon. 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 one the main character of Greenberg's book *This Machine Kills Secrets: How Wikileakers, Cypherpunks, and Hactivists Aim to Free the World's Information*. 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 (Bamford, 2014). The cover of this issue features Snowden with a grey background, holding the American flag close to his heart. Whether intentional or not, the resemblance between this cover and the 1993 cover featuring the Cypherpunk founders May, Hughes, and Gilmore, is striking.

The discursive work of the Cypherpunks and technology reporters during this period thus revitalizes crypto-discourse by drawing on the discursive work that allowed for its crystallization. I my conclusion, I discuss the relevance of these findings and their pertinence to future policy about encryption software and its relationship to Internet freedom.

Conclusion

In this paper, 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. In addition, I have illustrated the significance of technology journalism in popularizing this discourse.

This research outlines discursive events and practices that constitute the evolution of crypto-discourse over a period of forty years (1975 – 2015). 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 and freedom in relation to the state. This crypto-discourse timeline thus describes how crypto, as an empty signifier, serves as a battlefield in a larger discursive struggle over the meaning of Internet freedom.

Cypherpunks and technology journalists crystallized a particular understanding of Internet freedom in which only encryption software can protect online rights. This understanding removes any responsibility from the state to ensure the protection of online rights. 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. I described for example 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. Similarly, 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. In addition to depicting hackers and Cypherpunks as liberators of the world's information that is held hostage by governments world wide (Gilmore, 1991; Greenberg, 2012; Levy, 1993, 2001), they have described information as an agent with a determined will of its own.

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. 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). By globalizing crypto-discourse, crypto-advocates may, however, overrun culturally or contextually specific understandings of freedom.

That said, the purpose of this study is not to label all hackers as crypto-advocates, or all Cypherpunks as 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 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. This harmonization does not take into account 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 paper argues 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 residents. 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 by ensuring that mechanisms of power and control are in place to *uphold* democratic principles of transparency, accountability, and public participation, while also safeguarding personal data.

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, crypto-discourse forwards a negative conception of freedom internationally, by making individual privacy an *individual* rather than *state* responsibility. 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.

References

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

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

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.

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

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/

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.

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

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.

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.

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/

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

Greenberg, A. (2013, November 6). “Silk Road 2.0” Launches, Promising A Resurrected Black Market For The Dark Web. *Forbes*. Retrieved from http://www.forbes.com/sites/andygreenberg/2013/11/06/silk-road-2-0-launches-promising-a-resurrected-black-market-for-the-dark-web/

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

Hackers’ Conference 1984 - “Keep Designing”: How the Information Economy is Being Created and Shaped by the Hacker Ethic. (1985, May). *Whole Earth Review*, (46), 44–55.

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

Hughes, E. (1993a). A Cypherpunk’s Manifesto. In P. Ludlow (Ed.), *Crypto Anarchy, Cyberstates, and Pirate Utopias* (This chapter has been widely distributed on the Internet. Reprinted by permission of the author., pp. 81–84). Cambridge, Mass.: MIT Press.

Hughes, E. (1993b, March 9). RANTS: A Cypherpunk’s Manifesto.

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

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.

killab66661. (2010). *The Next HOPE (2010) - Keynote Address - Wikileaks.m4v*. New York. Retrieved from https://www.youtube.com/watch?v=aRVDIohWPVM

Knibbs, K. (2015, February 6). How the Silk Road Trial Could Lead to a Dangerous Legal Precedent. Retrieved April 18, 2015, 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.

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 Archive*, *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

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.

May, T. C. (1992). The Crypto Anarchist Manifesto. In P. Ludlow (Ed.), *Crypto Anarchy, Cyberstates, and Pirate Utopias* (This chapter has been widely distributed on the

Internet. Reprinted by permission of the author., pp. 61–64). Cambridge, Mass.: MIT Press.

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.

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.

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.

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.

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.

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.). Tor: Sponsors. Retrieved April 15, 2016, from https://www.torproject.org/about/sponsors.html.en

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

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. 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).

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.

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.

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