UNIVERSITY OF CALIFORNIA

Santa Barbara

A Web of Extended Metaphors in the Guerilla Open Access Manifesto of Aaron Swartz

A dissertation submitted in partial satisfaction of the

requirements for the degree Doctor of Philosophy

in Education

by

Kathleen Anne Swift

Committee in charge:

Professor Richard Duran, Chair

Professor Diana Arya

Professor William Robinson

September 2017

The dissertation of Kathleen Anne Swift is approved.

.....

Diana Arya

.....

William Robinson

.....

Richard Duran, Committee Chair

June 2017

A Web of Extended Metaphors in the Guerilla Open Access Manifesto of Aaron Swartz

ACKNOWLEDGEMENTS

I would like to thank the members of my committee for their advice and patience as I worked on gathering and analyzing the copious amounts of research necessary to write this dissertation. Ongoing conversations about hacktivism, Anonymous, Swartz, Snowden, and the rise of the surveillance state have been interesting to say the least. I appreciate all the counsel and guidance I have received over the years.

In that Empire, the Art of Cartography attained such Perfection that the map of a single Province occupied the entirety of a City, and the map of the Empire, the entirety of a Province. In time, those Unconscionable Maps no longer satisfied, and the Cartographers Guilds struck a Map of the Empire whose size was that of the Empire, and which coincided point for point with it. The following Generations, who were not so fond of the Study of Cartography as their Forebears had been, saw that that vast map was Useless, and not without some Pitilessness was it, that they delivered it up to the Inclemencies of Sun and Winters. In the Deserts of the West, still today, there are Tattered Ruins of that Map, inhabited by Animals and Beggars; in all the Land there is no other Relic of the Disciplines of Geography.

purportedly from Suárez Miranda, Travels of Prudent Men, Book Four, Ch. XLV, Lérida, 1658

VITA OF KATHLEEN ANNE SWIFT

June 2017

EDUCATION

B.A. in English Literature, Michigan State University, June 1989
M.A. in Rhetoric and Writing Studies, San Diego State University, June 2008
Ph.D. in Education, University of California, Santa Barbara, September 2017

PROFESSIONAL EMPLOYMENT

- *Graduate Teaching Assistant* — March 2011 to June 2011
  University of California, Santa Barbara
  Department of Chicana and Chicano Studies
- *Graduate Research Assistant* — January 2013 – March 2013
  University of California, Santa Barbara
  McEnroe Reading Clinic
- *English Instructor* — September 2013 – May 2014
  Brooks Institute
- *Graduate Teaching Assistant* — September 2014 – December 2014
  University of California, Santa Barbara
  Department of Chicana and Chicano Studies
- *Vice President of Graduate Student Affairs* — September 2015 – June 2016
  UCSB Graduate Student Association

PUBLICATIONS

Chapter in an Anthology
Swift, K. (2010). Eugenics, nazism, and the sinister science of the human betterment foundation. In Michelle Smith and Barbara Warnick (Eds.), *The responsibilities of rhetoric* (pgs. 214 - 218). Long Grove, Illinois: Waveland Press.

Editorialist and Blogger at
- Op-Ed News
- Counterpunch
- Radiooccupy.net
- Noozhawk
- The Independent
- The Bottom Line
- Edhat

ABSTRACT

A Web of Extended Metaphors in the Guerilla Open Access Manifesto of Aaron Swartz

by

Kathleen Anne Swift

Hacktivists tend to be an anonymous group of individuals asynchronously distributed across widely different locales around the planet. They frequently use computers and other forms of information and communication technologies (ICT) to advance such digital rights causes as free culture and open access to the Internet, in addition to the open source software movement. Their arguments against the encroachments of intellectual property rights on the digital commons have pitted them against government and corporate institutions with vested security and remunerative interests in the World Wide Web. While a great many studies have been conducted on the sociological and historical implications of the hacktivist phenomenon, few if any have been conducted on the underlying stances and arguments of the hacktivist community and the corporations and governments they frequently oppose.

For my research, I have analyzed linguistic framing and metaphor usage in combination with theories of Critical Discourse Analysis (CDA), Frame Semantics, and Cognitive Linguistics as a means to examine the stances of three principal antagonists in the debate over freedom of information on the Internet: 1) hackers and hacktivists; 2)

civil rights groups; and 3) governments and corporations. I have focused in particular on the hacktivist, Aaron Swartz, whose authorship of *Guerilla Open Access Manifesto* (2015, p. 26) coupled with his act of content liberation when he downloaded millions of academic articles, led to his indictment by the Department of Justice.

My eclectic methodology serves to unpack the construction of meaning arising from texts produced by and about hacktivists with a focus on linguistic framing as a tool for analyzing the metaphors that inform stances. Relevant to my study has been the function of metaphorical concepts as ways to create complex frames that in turn capture the attitudes, values, and beliefs that accompany the stances associated with metanarratives and worldviews. Such a methodology has helped elucidate the conflicting epistemological attitude of hacktivists and authorities toward online freedom of information.

The findings of my study reveal that the metaphors used to talk about the social epistemology of the Internet lie at the heart of the debate. Lakoff and Johnson's expansion on Michael Reddy's conduit metaphor has been meaningfully applied to an interpretation of the Internet itself in order to facilitate an understanding of the significance of the knowledge ecology in the Information Age. My findings show that Reddy's conduit metaphor is directly implicated in the downfall of Aaron Swartz and provides a cautionary tale for those fighting to preserve public access to the electronic knowledge commons.

TABLE OF CONTENTS

I. The Debate Over Freedom of Information on the Net

My dissertation examines online social movements and in particular the hacktivist movement. Orthodox theories and explanations of social movements are not necessarily applicable to hacktivists which makes a simple definition of hacktivism misleading since these groups and individuals often lack the traditional hierarchical structure of spatially domiciled social advocacy organizations. Hackers, hacktivists, and the alternative computing crowd are distributed across the Internet in time and space rendering them non-linear in structure and protean by nature. A cursory examination of 4Chan, progenitor to Anonymous, is evidence enough of this (Stryker, 2011).

Yet hacktivists do constitute themselves as a group with definable plans and objectives and this may be seen in their promotion of hacker ethics as outlined by Gabriella Coleman in *Hacker Politics and Publics* (2011, pp. 511 - 516). Such hacker ethics include: 1) freedom of information 2) prevention of censorship 3) and protection of personal privacy on the World Wide Web. The hacktivist fight for freedom of information in cyberspace is no mere philosophical conundrum. It is a struggle for open access and free culture on the Internet in order to preserve the fair use of copyrighted works in the public domain.

For my research, I explore the role of conceptual metaphor in developing a theory of knowledge as argued by two primary disputants over information policy on the Net: hackers and hacktivists versus governments and corporations. In examining competing metaphors for the Internet, I explore the significance of social epistemology in cyberspace. I have limited the scope of my investigation to the famous hacktivist, Aaron Swartz, and the notorious hacker collective, Anonymous, because I believe that the circumstances surrounding the short life of Swartz and the attempts of Anonymous to defend him from his

detractors encapsulate many of the most controversial features of the hacktivist movement. For purposes of my study, I have examined the role of the authorities who prosecuted Aaron Swartz, and the hacktivists, civil rights advocates, and scholars who fought to maintain the viability of his ideas after his death. Centering on the debate between officialdom and Swartz over freedom of information on the Internet, my investigation looks at how their arguments have drawn in other data activists and civil liberty groups and how they too have been met with hardline opposition from corporate and government institutions. I have examined key texts produced by government and corporate stakeholders seeking to regulate the Internet for purposes of law and commerce, and compared them to the texts produced by Swartz and his allies arguing for open access to the Internet. Using Critical Discourse Analysis, Frame Semantics, Cognitive Linguistics, Linguistic Framing and Metaphor Theory as a multifaceted lens to analyze the disputes between the key players in the debate, I take a closer look at the polemics of each side as they struggle for control of the Internet. By examining the linguistic framing devices and metaphors of the texts produced by the relevant parties, I seek to provide a granular analysis that explicates the political and ideological stances of the antagonists in the debate. Such an analysis also helps uncover the embedded metaphors and hidden premises comprising the linguistic frames that narrate the disputant's version of affairs.

According to Philip Eubanks in "Poetics and Narrativity" (2004), "Along with metaphor, narrative is one of the most observable ways we conceptualize experience and organize memory" (p. 36). More broadly speaking, my dissertation examines the digital rights movements of hackers and hacktivists in order to provide a grand narrative of the significance of a hacker ethic of cyberspace. Pivotal to my study is the work of Manuel

Castells and his theory of communication and socio-political power. His ideas on "the space of flows" and the network society provide a birds-eye view of the topography of the debate over the right to connect to the Internet.

As a young hacktivist and Internet prodigy advocating for digital rights on the World Wide Web, Aaron Swartz was a passionate proponent of the open access and free culture movement. He called for the reform of restrictive intellectual property rights and championed for the protection of the public domain and fair use of copyrighted materials on the digital commons, a subject of growing legal contention in the Information Age. His commitment to freedom of information and civil liberties on the Web saw his startup of several open access Internet projects including the Creative Commons (offering an alternative form of copyright for Netizens), the Open Library (a free digital data-base of public domain books under the aegis of the Internet Archive), and the Semantic Web project (a project to allow users to create their own online databases).

From an early age, Swartz could claim peers among the Internet's digerati. He founded tech companies like Infogami, Reddit, and Jottit, and gained wide renown as one of the principle creators of the Rich Site Summary (RSS) web feed format. His many other technical accomplishments included such ventures as his collaboration with John Gruber to create Markdown language (a plain text writing system easily convertible to other forms of writing systems such as HTML), his collaboration with Virgil Griffith to create tor2web (a way to access Tor from a regular browser in order to anonymously publish articles on the Net), and his collaboration with Kevin Poulsen to create SecureDrop (a.k.a. DeadDrop, a site to allow whistleblowers to send electronic documents to relevant authorities anonymously).

A tireless activist, Swartz founded Watchdog.net in 2008 to allow visitors to compile graphic analytical data on politicians. He founded Demand Progress in 2010, a non-profit organization advocating for freedom of information and digital rights on the Internet. Perhaps most significantly of all, his successful campaign against the Protect IP Act (PIPA) and Stop Online Piracy Act (SOPA) in 2012 curtailed the power of the government to shut down websites accused of intermediary copyright violations.

Ironically, the issue of copyright violation would bring about his eventual downfall when his hacktivism led to his arrest by MIT police and the U.S. Secret Service on January 6, 2011 for downloading close to five million academic articles from JSTOR while on a fellowship to Harvard University. JSTOR is an online database of scholarly journals, books, and articles used by college and university libraries across the United States. According to Parker Higgins at Electronic Frontier Foundation (EFF), federal prosecutors had been overseeing Swartz's case from the moment of his arrest by MIT police and later admitted that they targeted Swartz in part because of his hacktivist views (2013, March 7).

When state charges were dropped against Swartz in 2012 in order to allow Federal authorities to proceed with his case, Secret Service Agent Michael Pickett would team up with assistant U.S. attorney Stephen Heymann to lead the prosecution of the young Harvard research fellow. Swartz was eventually charged with thirteen violations of the Computer Fraud and Abuse Act (CFAA) by the Department of Justice (DOJ). Facing felony theft charges that included up to ninety-five years in prison and over a million dollars in fines and civil asset forfeitures, Swartz committed suicide on January 11, 2013. In response, the hacktivist collective called Anonymous shut down both the Massachusetts Institute of Technology (MIT) and United States Sentencing Commission (USSC) websites and

installed memorials to Swartz in their place. Entitling their tribute, "In Memoriam, Aaron Swartz, November 8, 1986 – January 11, 2013, Requiescat in pace," Anonymous roundly condemned the role of officials in his death and called for sweeping reforms of not only the computer laws used to prosecute him, but the overall judicial system. Significantly, Anonymous also demanded the implementation of Swartz's *Guerilla Open Access Manifesto*.

In the ensuing months, investigations were conducted into MIT's role in the affair, online petitions were launched to demand the dismissal of lead prosecutors in the case, calls were made to reform the CFAA, Congressional inquiries into the DOJ were initiated, and Swartz's family and friends engaged in a bitter dispute with government and university officials over their role in his suicide. Swartz was posthumously admitted into the Internet Hall of Fame in June of 2013 and awarded the American Library Association's James Madison Award for his hacktivism. He also posthumously received the Electronic Frontier Foundation (EFF) Pioneer Award in 2013.

A. Synopsis of Previous Research

No academic publications about Aaron Swartz and his connection to Anonymous and the larger hacktivist community have yet been produced that I am aware of. However, a publication of Aaron Swartz's writings is available from The New Press entitled *The Boy Who Could Change the World* (2015). It has compiled some of his many essays, blogs, and musings into a highly readable account of his views on civil liberties, digital rights, and technological trends on the Internet. A semi-biographical book written by journalist Justin Peters called *The Idealist* (2016) gives a summary account of the life and times of Aaron

Swartz in conjunction with an historical overview of the evolution of data activism. Peters investigates the context for "data moralists" like Swartz against the historical backdrop of the struggle to maintain the fair use of copyrighted materials in the public domain. Additionally, there are many non-academic articles about Swartz from news sources and tech websites. There have also been a scattering of academic books about 4chan and Anonymous – most notably by Gabriella Coleman (2011, 2013, 2014) and Cole Stryker (2011) – but these have typically taken a historical or sociological perspective on hackers in general.

Most academic publications in this area of research appear to be concerned with describing the new organizing structures of the Internet rather than in providing an in-depth analysis of the question of civil liberties and digital rights in the Information Age. Common areas of inquiry include studying the Internet's enabling of crowd sourcing, the development of online social movements through social media, the phenomena of Big Data and Geographical Information Systems (GIS) (or human information/social mapping), and the Internet-facilitated Indymedia movement.

B. Methods of Data Collection and Analysis

In the case of Swartz, a thoughtful linguistic analysis of the key players in the struggle for control of the Internet has greatly contributed to our understanding of the ongoing debate over the freedom of information on the Net. The arguments of hackers and hacktivists championing for privacy and freedom in cyberspace has provoked an understandably antagonistic reaction from the government agencies and corporate institutions bent on monetizing, systematizing, and securing the information freeway. This in turn has

galvanized the defenders of civil rights who support hacktivists and their populist ethics of free speech and digital rights on the World Wide Web. In my work on the hacktivist community, the rhetorical and linguistic features of texts used by all three protagonists are essential for an understanding of the wider social implications of the hacktivist movement. By employing a blended methodology of Cognitive Linguistics, Linguistic Framing, and Metaphor Theory I have created an eclectic orientation to my research that is uniquely my own. A contrastive analysis of the relevant texts produced by the three involved principals has helped to further deconstruct their arguments in order to examine their embedded metaphors and ideological premises.

C. Specific Research Questions

In order to study Swartz and the social phenomenon of the hacktivist movement I have posed a series of questions to address in my analysis. How do Internet communications among hacktivists, government/corporations, and social justice advocates reflect their conceptual and ideological framing of perspectives and stances in public communications concerning key issues underlying the hacktivist movement? More specifically, how do the linguistic framing practices of all parties reflect their stances about the protection of civil liberties on the Net? In particular, how does the use of terminology and metaphor, as well as the rhetorical discourse posturing of stance, reveal assumptions and claims about the nature of the issues? The heart of my text analysis has examined the key discussion points raised in each text for their use of metaphor and linguistic framing to illustrate the ideological stances of the people and institutions involved. One feature of this analysis includes the examination of embedded metaphors. Embedded metaphors (or what Michael Reddy calls

"dead metaphors") are hidden or implied metaphors underlying the ideological arguments of the disputants. An analysis of hacktivism as a social movement can reveal how forces of symbolic capitalism – what counts as value in the information age – function to control information on the Internet and how these forces are countered by hackers and hacktivists acting as populist guardians of the World Wide Web.

I further wish to address how the Internet as a medium of publication and communication has changed the notion of intellectual property rights in the digital age. Legal scholars such as Lawrence Lessig have already covered this ground quite thoroughly in *Free Culture* (2004) and other such works. He has addressed the advent of the Internet and how it has modified our notions of the fair use of copyrighted materials available to the public on the digital commons. For this reason, we might ask ourselves: Why is the hacktivist insistence that "information wants to be free" so important to the progressive causes they advocate? How does the free exchange of ideas over the Internet shape the epistemological attitudes of hackers and hacktivists toward information and facilitate the meeting of the minds in cyberspace?

D. A Close Examination of Six Texts

The six primary sources I have used for my analysis provide a narrative account of the life and times of Aaron Swartz. This narrative follows a roughly chronological order that culminates with his death as a result of his prosecution by the U.S Department of Justice (DOJ) and the Massachusetts Institute of Technology (MIT) for the alleged theft of JSTOR articles. The texts are linked by time and incident to form a tight narrative of Swartz's

arguments with authorities over the right to freedom of information on the Internet. Taken all together, these six texts provide a casebook analysis of the hacktivist movement.

I have examined each text for its stance on the commodification of information on the World Wide Web and the consequences for scofflaws of intellectual property rights. Swartz's fundamental role in creating the architecture of the Internet through the development of the RSS feed, along with his dedication to hacktivism and his ongoing political reform efforts, are examined in terms of the government's decision to prosecute him. The selected texts create a grand narrative delineating the respective values and ideological stances of the aforementioned principals in their arguments over intellectual freedom. Once again, these are Internet hacktivists representing research-oriented, anti-authoritarian, and even anarchist values; governments and corporations representing profit and security driven values; and civil rights activists representing humanitarian and egalitarian social values. Taken altogether, these texts embed conceptual metaphors to tell the story of an evolving social epistemology in the struggle for information on the Net.

The first text I have looked at is Swartz's *Guerilla Open Access Manifesto.* This short text written by Aaron and four others while at a conference of librarians in 2008 Eremo, Italy, was given to prosecutors by his former girlfriend, Quinn Norton, after they pressured her to provide them with something they could use in their case against Swartz. A writer for *Wired,* Norton would go on to describe her ordeal with Swartz's prosecutors in an article she wrote for *The Atlantic* (Mar. 3, 2013). As a testament to his dedication to the hacker ethic for the free and open exchange of knowledge on the Internet, Swartz's *Guerilla Open Access Manifesto* (2015) serves to bookend a brief period of his meteoric life that started in approximately 2008 and ended in 2013. It is significant that he wrote the *Manifesto* in 2008,

the same year he committed his first widely publicized act of content liberation with PACER (Public Access to Court Electronic Records). Swartz committed suicide in 2013 when the DOJ rejected his plea of not guilty because it claimed his authorship of the manifesto demonstrated his intention to breach copyright law.

The second text I have looked at is the FBI and Secret Service files on Swartz. Swartz found out about the FBI's covert surveilling of his activities when agents visited his house shortly after he was cleared of any wrongdoing in the PACER case. He subsequently filed a Freedom of Information Act (FOIA) for his FBI file. According to FBI documents, he first came up on the FBI's radar screen in 2008 when he downloaded over two million federal court documents from a government website for archiving public court records. Known as Public Access to Court Electronic Records (PACER), the website maintains paywalled public records archived by the federal judiciary. PACER charges up to eight cents a page for copies of their electronic documents even though federal documents are not covered under copyright laws and so – at least in theory – freely available to everyone. Using a free trial account at the Sacramento Public Library, Swartz downloaded more than two million PACER documents and turned them over to Public.Resource.org., a website to return public documents to the public domain. Carl Malamud, the owner of the website, and Aaron Swartz promptly came under secret investigation by the FBI. Though it was later determined that neither Swartz or Malamud had committed data theft, the FBI began closely monitoring Swartz's activities from that point onward. An article by Will Wrigley appearing in the Huffington Post on February 7, 2013, has provided an account of the investigation that sums it up thusly: "Swartz downloaded public court documents from the PACER system in an effort to make them available outside of the expensive service. The move drew the attention

of the FBI, which ultimately decided not to press charges as the documents, were, in fact, public."

The third text I have examined is a report issued by the Massachusetts Institute of Technology (MIT) following an internal investigation of its involvement in the suicide of Aaron Swartz after he was prosecuted for downloading JSTOR articles. MIT conducted the self-review with the intent to evaluate its role in Swartz's death and to justify its actions to the public. With that goal in mind, it issued a 162-page report to MIT President L. Rafael Reif and the campus community at large. From this report, I have chosen select pages which shed light on MIT's stance on Aaron's case and subsequent discussions about it with his father, Robert Swartz. MIT's role in the affair began when Swartz was on research fellowship at the Edmond J. Safra Research Lab on Institutional Corruption headed up by Lawrence Lessig at Harvard University. Swartz had a guest user account through MIT, that allowed him to access JSTOR'S database of online academic articles. Using a utility closet to plug in to MIT's computer networks, Swartz hooked up a laptop and began downloading millions of JSTOR articles. Unfortunately, this caused JSTOR's server to crash. His computer was subsequently discovered, and two MIT police officers and a U.S. Secret Service Agent at nearby Harvard University arrested him. Over the next year, Swartz was indicted on felony charges of grand larceny, wire and computer fraud, unauthorized access to a computer network, and reckless endangerment of a protected computer. When federal prosecutors took over the case, the charges were increased to thirteen felonies. JSTOR refused to participate in litigations against Swartz, but MIT chose to maintain a position of "neutrality" which meant that it actively assisted prosecutors.

The fourth text I have examined is the press release from the Office of the U.S. Attorney

of the District of Massachusetts concerning Swartz's suicide. After his death, the government dropped all charges against Swartz and, under a barrage of criticisms, Department of Justice (DOJ) prosecutors sought to deny any culpability for their role in his suicide. U.S. Attorney for Massachusetts, Carmen Ortiz (2013), who was in charge of the case, released a press statement that maintained, "This office's conduct was appropriate in bringing and handling this case.... This office sought an appropriate sentence that matched the alleged conduct—a sentence that we would recommend to the judge of six months in a low security setting" (2013, Jan. 6). She denied the fact that the lead prosecutor on the case, Assistant U.S. Attorney Stephen Heymann, had ever threatened Swartz with the maximum penalties in order to force him to accept a plea bargain. Nevertheless, in an article written by Sandra Guy in the Chicago Sun-Times, Swartz's father roundly condemned government and university officials at his son's funeral declaring, "Aaron was killed by the government, and MIT betrayed all of its basic principles" (January 15, 2013).

The fifth text I have looked at is the memorial site installed by the hacktivist group known as Anonymous on MIT's website and the United States Sentencing Commission's (USSC) website. In protest of Swartz's suicide, Anonymous made two hacks into MIT's website and two more into the USSC's website. In both instances, Anonymous demanded the reform of existing copyright laws in addition to the judiciary system itself. Significantly, they also called for the immediate implementation of Swartz's *Guerilla Open Access Manifesto.* Anonymous followed up its initial MIT hack with one on the USSC's website replacing its homepage with a YouTube video titled *Anonymous Operation Last Resort*. Operation Last Resort (@OpLastResort) tweeted links to various YouTube videos criticizing the Department of Justice (DOJ) and its prosecutors. A follow-up attack on the USSC site

gave online protesters the ability to hack the website by using Konami code to blast cartoon missiles at its online text.

When Swartz died, there was an immediate outpouring of sympathy for him. Scholars launched #PDFTribute to promote open access to digital information by making their works freely available online. A people's petition was initiated at the White House's online petition site to demand U.S. Attorney Carmen Ortiz be removed from office for prosecutorial overreach. When the petition garnered more than the required 25,000 signatures, the Obama administration not only denied it, but also raised the minimum requirements for future White House petitions to 100,000 (*RT*, 2013, Feb. 13, "Petition to remove prosecutor"). Congressional investigations were launched into the DOJ's handling of the case and people everywhere called for the reform of the Computer Fraud and Abuse Act (CFAA) used to prosecute Swartz.

For this reason, the sixth and final text I have looked at is a bill introduced in 2013 to reform the CFAA. The measure to amend the Computer Fraud and Abuse Act (CFAA) became known as Aaron's Law. It sought to amend Title 18 U.S. Code, section 1030, in order to clarify the meaning of "access without authorization" to computers connected to the Internet and to mitigate the severity of punishments for copyright violations in cases where there is no discernable profit motive. Introduced by a bipartisan group of representatives, Aaron's Law Act was introduced in 2013 and subsequently defeated in 2014. It was re-introduced in 2015 but remains stalled in committee.

The chapter outline for my dissertation includes the following information:

- Chapter 1 – Introduction and statement of the problem (Title: *The Debate Over Freedom of Information on the Net)*

- Chapter 2 – Background and history on hacktivism (Title: *Hacktivists and Hacker Ethics)*
- Chapter 3 – Organizational political theory (Title: *Government and Corporate Responses to Hacktivists)*
- Chapter 4 – Methods of Analysis (Title: *A Framework for Analysis*)
- Chapter 5 – Analysis and Results (Title: *Social Epistemology in Cyberspace)*
- Chapter 6 – Conclusion and implications (Title: *The Conduit Metaphor Writ Large)*

In summary, contemporary perspectives on the nature of literacy call attention to the centrality of communicative functions fulfilled by texts and their linguistic components. More deeply, every term and linguistic relationship among text components points to concepts and beliefs that compose the ideological stances expressed by the disputants. The linguistic frames and conceptual metaphors advanced in their arguments support the respective stances of hacktivists and their adversaries. Cognitive Linguistics, Frame Semantics, and Critical Discourse Analysis reinforce each other in their mutual recognition of the fundamental role of language in the discursive production of a socio-epistemic narrative in the Digital Millennium.

II. Hacktivists and Hacker Ethics

For this section of my dissertation, I provide an overview of select hacker and hacktivist groups with an eye to looking at the evolution of hacktivists as they work to advance freedom of speech and the right to information on the Internet. In this manner, I seek to provide context for my later focus on Aaron Swartz and Anonymous by first offering a historical perspective on hackers and the rise of the hacktivist movement. I examine the hacker ethics underlying their political dissent particularly as expressed through the techniques of culture jamming and reality hacking (a.k.a. guerilla semiotics). Culture jamming and reality hacking are ways to subvert standard social messages using irony and humor in order to present alternative perspectives. The early pranks of student engineers at MIT as well as the social reform campaigns of Adbusters are only a few examples of the reality hacking and cultural jamming tactics of the DIY, anti-consumeristic, and anti-authoritarian propensities of hackers and hacktivists.

As already noted, a simple definition of hacktivists is illusory due to the breadth of activities that have been attributed to such persons and affiliated groups. Nonetheless, it is useful to keep in mind Gabriella Coleman's (2013) definition of individual hackers and hacktivists as "computer aficionados driven by an inquisitive passion for tinkering and learning technical systems and frequently committed to an ethical version of information freedom" (*Coding Freedom*, p. 3). While hacktivist groups, communities, networks, and forums can give the *appearance* of structured organizations, it is important to remember that they are, in fact, amorphous sociopolitical movements lacking structural coherence as traditionally understood. This issue will be addressed in greater detail in the next chapter which shows that their very formlessness derives in some measure from the non-linear

dynamic of the emergent Information Age and the rise of what Castells (2010) calls the network society. I have limited the scope of my investigation to communities and collectives that use computer networks and other forms of advanced information and communication technologies (ICT) to promote progressive causes and who typically self-define as hackers and hacktivists.

In his seminal work *The Rise of the Network Society,* Manual Castells (2010) notes that the advent of advanced communication technologies has "transformed the spatiality of social interaction by introducing simultaneity, or any chosen time frame, in social practices, regardless of the location of the actors." From this he hypothesizes the idea of the space of flows or "the production, transmission and processing of flows of information" (p. xxxii). The fact that hacktivists inhabit the virtual reality created by the space of flows on the Net means they are not constrained by space and time in the way that past social actors have been and are therefore able to reconfigure cybernetic power in new and exciting ways that traditional governing bodies and institutions find problematic.

In this chapter, I examine key examples of hacktivist groups – who they are and what they do – and the frequently adversarial stance they take toward government and corporate authorities. Questions to bear in mind include: What is the role of hacker ethics in the development of an ideology of freedom of information and open access to the Internet? How does the free exchange of ideas and information over the Internet affect the development of hacktivist collectives like Anonymous and facilitate the meeting of the minds in the public discourse arena? What forms of hacktivism trigger a response from government and corporate institutions?

I look at the form, function, significance, and inter-connectedness of hacktivist collectives as they struggle to promote the aforementioned hacker precepts: 1) freedom of information 2) prevention of censorship 3) and protection of personal privacy on the World Wide Web. Toward that end, I examine the following hacktivist collectives and networks: 4chan, Anonymous, WikiLeaks, Hackers on Planet Earth (HOPE), and LuzSec. These groups have been chosen for their relevance to the hacktivist community, their diversity of forms as collectives, forums, databases, and communities, and their respective functions as evinced by their stated purposes, goals, and missions. They have also been selected because of their inter-connectedness as demonstrated by their cross-pollination of ideas and initiatives together. For example, 4chan is an image board catering to American fans of Japanese anime which eventually gave rise to the hacktivist collective Anonymous, while HOPE is a hacker's conference held biennially in the United States which is attended by many in the hacktivist community. (Interestingly, 4chan founder Chris Poole was hired by Google in 2016). I describe key characteristics and accomplishments of each group and their contributions to the evolution of the hacktivist movement.

A. Hacktivist Tools and Practices

Though we frequently take it for granted, it is perhaps worthwhile to look at the history of the Internet for its relevance to the development of the hacker community. *Man-Computer Symbiosis* by J.C.R. Licklider (1960) is an early article about the Internet that speculated, "A network of such [computers], connected to one another by wide-band communication lines [could provide] the functions of present-day libraries together with anticipated advances in information storage and retrieval and [other] symbiotic functions".

Licklider also predicted that, "In a few years, men will be able to communicate more effectively through a machine than face to face" (Licklider, 2003, p. 75).

The Internet is a relatively recent phenomenon and its origins – like so many others in Western technology – lay in the military. An early prototype of the Internet was created in 1969 to facilitate computer communication between U.S. military scientists and public university researchers. It was known as the ARPANET (Advanced Research Projects Agency Network). When it was first initiated, ARPANET connected computers at the Department of Defense to computers at the Computer Science Department of the University of Utah, the Network Measurement Center at the University of California, Los Angeles, the Augmentation Research Center at Stanford Research Institute, and the Culler-Fried Interactive Mathematics Center at the University of California, Santa Barbara. Through their research efforts with ARPANET, early computer scientists such as Licklider "helped to make the iron triangle of industry, the military, and academia as equilaterally triangular as it is today" (Montfort, 2003, p. 73).

Also of importance to the initial development of the Internet were the many computer programmers and hackers who wrote the programming language for open source software like GNU. GNU is an acronym meaning "GNU Not Unix" to distinguish itself from Unix, a form of proprietary programming language popular in the 70s and 80s. In *Coding Freedom* (2013), Gabriella Coleman makes an anthropological study of the Free and Open Source (F/OSS) software movement and the growing demands for the protection of digital rights on the World Wide Web. She examines two developing but diametrically opposed legal trajectories on the early Internet: the F/OSS movement versus the expansion of intellectual property rights. Though initially following separate paths of development, these two very

different legal interpretations of the early programming language of the Internet would eventually begin to confront one another in the legal arena of the courts with greater and greater frequency. In the second chapter of *Coding Freedom* (2013a) Coleman refers to,

> two competing legal regimes, conceptualized here as two distinct trajectories that once existed independently but have come into direct conflict, especially over the last decade. The first trajectory pertains to free software's maturity into a global technolegal movement. The second trajectory covers the globalization of intellectual property provisions so famously critiqued in the works of numerous scholars. These partly independent trajectories intersected to become inseparable histories, with their horns locked in a battle over the future of the very technologies (the Internet and personal computer) that have enabled and facilitated the existence of both proprietary software firms and the free software movement (p. 62).

In addition to using the Internet and a variety of communicative tools to coordinate their protests, hacker/hacktivists practices have also included liberating information and sending it to repositories and databases like Public.Resource.org, WikiLeaks, and Cryptome. As already mentioned, Swartz's act of data activism in the PACER case led to his secret investigation by the FBI. Such acts of content liberation have been conducted by a wide range of hackers and whistleblowers over the past years including hacktivists like Chelsea Manning, Julian Assange, Edward Snowden, and Jeremy Hammond. These informers on the secrets of the powerful have precipitated world-wide political scandals with far reaching consequences that are not always recognized or appreciated. WikiLeaks has become synonymous with the practice of scientific journalism, a new style of investigative

journalism backed by massive amounts of data that has exposed the corruption of ruling elites from Tunisia to the United States. Such data activism has demonstrated the growing political power of hackers and hacktivists in the global discourse arena.

Hacktivist protests (a.k.a. reality hacking) can take a variety of forms including Distributed Denial of Service (DDoS) attacks, doxing, and raucous street protests. A definition of doxing is "the leaking of private information – such as social security numbers, home addresses, or personal photos" to the general public (Coleman, 2014, p. 7). On the other hand, a DDoS attack is one where large numbers of hackers engage with, and eventually overwhelm the normal operations of a website in order to crash it. Though Anonymous has successfully employed the latter technique, it has caused a great deal of handwringing among Netizens who struggle with the inherent contradictions that arise when a philosophy of information as a basic human right uses methods that undermine it such as DDoS attacks on major corporate and government websites.

One of the earliest cases of hacktivism is to be found in the anti-nuclear WANK worm that attacked a network of government computers in 1989. The WANK worm case shows how hacktivists employ humor, daring, and political messaging to get their point across. In an article appearing at Counterpunch on Nov. 25, 2006, WikiLeaks founder Julian Assange explains how computers at the U.S. Department of Energy and the NASA were "penetrated by the anti-nuclear WANK worm". There the computer virus installed a message written in ASCII text on government computers that announced, "WORMS AGAINST NUCLEAR KILLERS. \Your system has been officially WANKed/ You talk of times of peace for all and then prepare for war." Needless to say officials were not amused. Other examples of

hacktivist practices are further illustrated in the discussion that follows through a study of the different forms and functions of hacktivist collectives.

B. Hackers and Phone Phreakers

Early hacker culture can be traced back to the 1960s with the origin of the phone phreakers who often paid only cursory attention to political causes and social movements. Phone phreakers were known for manipulating telephone networks for a variety of aims including the securing of free phone services, access to the use of restricted phones, and fun pranks such as dialing up the Pope. A phone phreaker and pirate radio station creator who went by the alias "Captain Crunch" (a.k.a. John Draper, founding member of Apple computers) became famous for the latter prank (Draper, 2015). Draper got his nickname when he discovered that a kid's toy whistle in boxes of Captain Crunch breakfast cereal could produce the perfect tone for hacking AT&T phone systems.

In the early 70s, Abbie Hoffman was arguably the most well-known phone phreaker around having founded the anarchist-minded Yippie movement and the largely frivolous "Youth International Party." According to cyberpunk author Bruce Sterling in *The Hacker Crackdown* (2002), Hoffman and the Yippies "carried out a loud and lively policy of surrealistic subversion and outrageous political mischief. Their basic tenets were flagrant sexual promiscuity, open and copious drug use, the political overthrow of any power monger over thirty years of age, and an immediate end to the war in Vietnam, by any means necessary, including the psychic levitation of the Pentagon" (p. 45). Hoffman's most famous treatise, *Steal this Book,* has been described by Sterling, "as a spiritual ancestor of a computer virus" due to its promotion of all forms of "vaguely politicized varieties of rip-off"

(p. 46). In 1971, Hoffman and a phone phreaker by the alias of Al Bell began publishing the *Youth International Party Line*, a newsletter "dedicated to collating and spreading Yippie rip-off techniques, especially of phones, to the joy of the freewheeling underground and the insensate rage of all straight people" (p. 47).

Little wonder then that most hacktivists got their initial start by engaging in online pranks, tricks, and jokes. In this sense, the early hacker and hacktivist communities were the philosophical heirs of the avant-garde cultural movements of the Dadaists and Surrealists of the 1920s and 30s along with the anti-consumer Marxist ideologies of the Situationist International of the 1960s. Leah Lievrouw, in *Alternative and Activist New Media* (2011), has studied the history of activist artists to explore the relationship between the development of cultural and political forms of protest among the Dadaists of the 20s, the hippies of the 60s, and the mashup artists of the 90s.

> Cultural critics and scholars have long recognized the ties between today's "remix culture" – the sampling, fragmentation, juxtaposition, and recombination of disparate elements of text, image, and sound to create new works – and the availability of easy-to-use digital media technologies. But as numerous critics and historians have pointed out, the cultural sensibility of radical discontinuity and rupture of everyday experience that is commonplace in contemporary media culture can be traced as far back as Dada, which emerged in Europe at the time of World War I. In the in the 1950s and 1960s, a related sensibility – and some of the same tactics – were revived in France among the artists and writers of the Situationist International, in response to pervasive consumer culture, military/colonial powers, and the disabling,

> ideological “spectacle” generated by global systems of mass communication and cultural domination (p. 29).

These revolutionary social and cultural perspectives became the predecessors for free-spirited forms of reality hacking and cultural jamming that were the almost exclusive preserve of the early hacker and phone phreaker communities. For example, another exploit of Captain Crunch occurred in 1974 when he and a friend hacked Santa Barbara’s antiquated telephone lines in order to reroute all incoming calls to themselves. To the baffled bemusement of callers, they were informed that Santa Barbara had experienced a nuclear accident and that callers should leave phone lines open for emergency use only. The next day an LA Times article exposed the incident as a hoax.

Yet another example of the irreverent humor of hackers and hacktivists can be found in The Cult of the Dead Cow (cDc). The Cult of the Dead Cow and the Chaos Computer Club have the distinction of being some of the earliest hacker/hacktivists and DIY collectives in existence. cDc was formed in 1984 in Lubbock, Texas, and has stated that its mission is “Global Domination Through Media Saturation” (2014). The Chaos Computer Club, on the other hand, was founded in Berlin, Germany in 1981 with a mission to promote "a galactic community of life forms, independent of age, sex, race or societal orientation, which strives across borders for freedom of information" (Wikipedia, *Chaos Computer Club*).

Among its many exploits, cDc takes credit for using a blowgun dart to infect Ronald Reagan with Alzheimer’s disease. More ambitiously it has boasted that,

> In 1996, the cDc coined the term "hacktivism." Also in 1996, the Ninja Strike Force (cDc's elite cadre of cheerleader-assassins) was founded. In 1997, years before

> everyone and their dog had jumped on the file sharing bandwagon, it was distributing original mp3-format music on its website. In 1998 and 1999, the cDc's "Back Orifice" series was launched to open the eyes of consumers regarding the security of their computer operating systems. …Since 1999, Hacktivismo (a special projects group within the cDc) has been at the forefront of the ongoing struggle for human rights in and out of cyberspace (*Cult of the Dead Cow* website, n.d.)

Oscar Wilde has theorized, "Man is least himself when he talks in his own person. Give him a mask and he will tell you the truth." In an interview with Vanity Fair, founder of 4chan Christopher Poole has acknowledged that his online community is the philosophical antithesis of Facebook due to its protection of individual anonymity. While Facebook's CEO Mark Zuckerberg insists on the individual's online public face through authentic representation and non-anonymity, 4chan founder Christopher Poole insists on the protection of the individual's identity on the Web through anonymity.

4chan got its start when Poole created an imageboard and dedicated it to like-minded aficionados of Japanese manga, anime, and porn. It drew its inspiration from Japanese imageboards like Futaba and 2chan and quickly gained a reputation as one of "the largest active forums in the world, with 10 million unique visitors and 705 million page views a month". Nonetheless, reporters from Vanity Fair have characterized 4chan's "hive mind [as] a primordial soup of teenage-male angst and cute cat photos" (*Vanity Fair*, 2011).

The denizens of 4chan enjoy the site's special breed of trickery, sarcasm, and trolling, secure in their knowledge that "Anonymity is part of the culture of 4chan, a complex network of millions of trolls - (mostly) young men who are entranced with the notion of acting as one, as a 'hive mind,' and at the same time desperate to assert their individuality

apart from whatever pressures they feel in society, or 'I.R.L.' (in real life)" (Vanity Fair, 2011). The culture jamming proclivities of 4chan can be found in their endless stream of Internet memes. With Lolcats, Chocolate Rain, Pedobear, and Rickrolling to their credit, 4chan's online subculture actively encourages the proliferation of trolls, tricksters, and those in it for the lulz (a variant of "lol" – laugh out loud).

Figure 1. A Popular Culture Jamming Meme

Some of the earliest examples of 4chan's brand of chicanery and (some might even say sadistic) humor include its now infamous Habbo Hotel raid of a popular teenage social networking site from Finland. Habbo operates somewhat like Second Life insofar as it allows its users interact with one another in a virtual reality, this one in a series of hotels with a Lego-land motif. Habbo had already attracted the attention of other web tricksters before 4chan decided to make its move on it. Using African American avatars sporting giant afros, hundreds of 4chan trolls flooded the site with racist spam and other forms of provocations, including the blocking of the hotel swimming pool for alleged contamination by AIDS. Brashly unapologetic as ever, 4chan trolls declared themselves the victims of

racism when they were finally kicked out of Habbo Hotel (Stryker, 2011, p. 227 - 229).

Figure 2. Image from Habbo Hotel

Since posts to 4chan are ephemeral at best (most of them are erased each day and the site maintains no archives), "[i]t's one of the last places on the Internet where you really can say anything you want and it won't come back to haunt you. Anything posted on 4chan has generally disappeared by the end of the day, and there's no chance of Google finding it again" (Vanity Fair, 2011). In *Hacker, Hoaxer, Whistleblower, Spy* (2014), Coleman has noted that "On 4chan, … most post under the default name "Anonymous"" (p. 42). "Naturally, it was on this board where the collective idea and identity of Anonymous emerged" (p. 41). Given the typical troll's aversion to what 4chan denizens call "moralfagotry" (i.e. self-righteous indignation at perceived injustices) it does seem more than a little ironic that the infamous hacktivist collective known as Anonymous came into existence on 4chan.

C. Hacktivist Targets

What do many present-day hackers and hacktivists share in common other than the tools, practices, and motivation for doing things "for the lulz"? Surprisingly, Scientology – or

more specifically, a marked aversion for it. From discussants in the chat rooms of Suburbia in Australia, to the hackers of cDc in Texas, to the trolls of 4chan, a number of present-day hacker and hacktivist groups claim to have taken a shot at the Church of Scientology at some point in their initial career. Hacking the Church's website and trolling its responses seems to have almost become a rite of passage for many of them.

Originally founded in the 1950s by Navy Lieutenant officer and science fiction author L. Ron Hubbard, The Church of Scientology is based in Los Angeles, California, and touts the belief that the soul is immortal and has lived in reincarnated forms on other planets. According to John Carter (2004) in *Sex and Rockets*, Hubbard was a former friend of Jack Parsons, the Caltech rocket fuel scientist who died in a mysterious explosion at his house in Pasadena in 1952. There the two had led an occult group of practitioners in the Thelemic rituals of the Ordo Templi Orientis promulgated by master magician, Aleister Crowley. Not unlike Crowley himself, Hubbard had a long history as a Masonic charlatan who conned Parsons out of thousands of dollars and two of the boats they had invested in together as part of their Babalon Working project. Though it appears they were unsuccessful at conjuring the Thelemite goddess they had sought to invoke, the boats would eventually help Hubbard found the Church of Scientology, which sought jurisdictional freedom from its initial problems with world governments in the international waters of the ocean. The church developed notoriety for the cult-like behavior of its adherents and its harsh techniques for controlling every aspect of their lives – most notably their pocketbooks. Over the years, Scientology has been variously characterized as both a cult and an enterprise (Carter, 2004). When the Church began mounting an aggressive campaign to censor its critics in the late 80s, hackers and hacktivists went into action.

Former International Subversive hacker Julian Assange initially confronted the Church of Scientology as a system administrator for Suburbia, an Australian Internet service provider hosting online chat rooms on a wide variety of topics including the latest litigations of the Church. According to Andy Greenberg in *This Machine Kills Secrets* (2012), when one of Suburbia's members leaked documents about Scientologists' belief system to the server, the Church promptly sued for violation of copyright and had their computers seized. They contacted Assange demanding the release of the name of another of Suburbia's customers who was also an outspoken critic of the Church of Scientology. Assange refused. "We were the free-speech ISP in Australia," said Assange. "People were fleeing from ISPs that would fold under legal threats, even from a cult in the U.S. That's something I saw early on, without realizing it: potentiating people to reveal their information, creating a conduit. Without having any other robust publisher in the market, people came to us" (Greenberg, 2012, pg. 113). Assange would later credit his work at Suburbia as the inspiration for WikiLeaks.

Similarly, the denizens of 4chan also confronted the Church of Scientology but their decision to go after the Church stemmed in large part from their outraged sense of lulz. In 2008, a Tom Cruise Scientology video made the Internet rounds when journalists at Gawker, Radar, and other news groups linked up to reporter Mark Ebner's leaked copy of the video at YouTube. It was soon taken down again, but when Gawker reposted it along with a rating of ten on the scary scale, Scientologists swung into action. They demanded Gawker remove it or face legal repercussions. Alerted to this fact, the hive at 4chan did something that it had never done before; it put out a call for *principled action*. The following Anonymous post subsequently appeared on /b/ (or random bulletin board) at 4chan: "People need to

understand not to fuck with /b/, and talk about nothing for ten minutes, and expect people to give their money to an organization that makes absolutely no fucking sense. I'm talking about "hacking" or "taking down" the official Scientology website. Its time to use our resources to do something we believe is right" (Coleman, 2014, p. 55).

Thus Project Chanology was born.

Unlike other pranks played by the denizens of 4chan (for example, the Habbo Hotel raids, or their Fox News spoof), the attack on Scientology would also take action in the real world with organized street protests around the globe. "On February 10, 2008, over seven thousand people in 127 cities protested the Church of Scientology's human rights abuses and acts of censorship" (Coleman, 2014, p. 5). One of the largest of these protests occurred at the headquarters of the Church of Scientology in Los Angeles with over a thousand demonstrators participating. Protesters in Los Angeles, London, and Australia also wore the V for Vendetta/Guy Fawkes mask, the now public face of Anonymous.

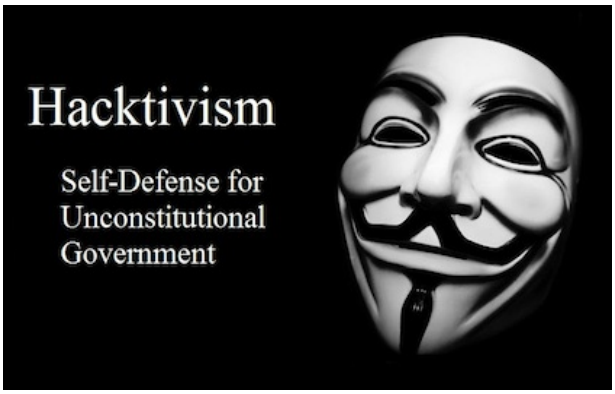

Figure 3. A Guy Fawkes Mask Used by Anonymous in Public Street Protests

D. Hacktivist Venues

Other venues for hackers and hacktivists include conferences and forums like Hackers on Planet Earth (HOPE), DEF CON, and the Chaos Communication Congress (CCC). HOPE is held in New York and is hosted by the rebel magazine, *2600: The Hacker Quarterly,* while DEF CON is hosted in Las Vegas and regularly includes government officials among its attendees. Additionally, the Chaos Communication Congress is held in Hamburg and is hosted by the Chaos Computer Club. Jacob Applebaum, who is widely known for his early work on Tor, has been a noteworthy cypherpunk at both HOPE and CCC conferences. Using encryption to remain undetected in order to facilitate online progressive campaigns, cypherpunks are the bane of governments and institutions around the world. A cryptography tool developed initially by the Naval Research Lab to provide anonymity for the transmission of online data, Tor is an acronym for The Onion Router, which describes the manner in which encrypted information is layered like an onion before being routed through a "mix network" that bounces the data between thousands of relays points making its origins difficult to trace (Greenberg, 2012, p. 146). Applebaum "joined the nonprofit as a staffer in 2008, [where] the young anarchist has served as one of Tor's primary coders as well as one of its international evangelists, preaching the gospel of anonymity wherever he goes" (Greenberg, 2012, p. 150).

At a HOPE conference in 2010, Applebaum surprised conference goers by replacing Julian Assange as the keynote speaker. He walked out on stage sporting a t-shirt that read "Stop Snitching", a reference to Adrian Lamo, the hacker who turned Bradley/Chelsea Manning over to U.S. military authorities after leaking thousands of classified military documents to WikiLeaks (including the now infamous "Collateral Murder" video). Applebaum spoke as the American representative for WikiLeaks because Assange had

decided it was too dangerous to travel to the U.S. "His talk contextualized WikiLeaks historically into what is now commonly called 'the fifth estate:' the hackers, leakers, independent journalists, and bloggers who serve the critical role that once fell to the "fourth estate," the mainstream media" (Coleman, 2014, p. 84). In the end, Applebaum revealed a revamped WikiLeaks submission site employing Tor to better protect the anonymity of future whistleblowers (Greenberg, 2012 p. 168). He closed by appealing to the audience to join the WikiLeaks crusade in order to - in the words of Assange - "reform every political system on the earth" (Greenberg, 2012, p. 96).

"Four years later, after the firestorms of Bradley/Chelsea Manning's alleged record-breaking, world-shaking releases, the science fiction writer Bruce Sterling wrote of WikiLeaks: 'At last – at long last – the homemade nitroglycerin in the old cypherpunks shack has gone off"' (Greenberg, 2012, p. 98).

E. Hacktivist Transformations

Just as the discussion boards at 4chan have spawned Anonymous, so too would Anonymous itself spin-off other hacktivist groups, perhaps the most well-known of these being LuzSec. Initially known as Internet Feds, Lulz Security (or LuzSec) got its start with the fallout from HBGary Federal when the president of the company, Aaron Barr, responded to a plea from Bank of America (BofA) to help plug its security leaks on pain of possible revelation of its misdeeds by WikiLeaks. HBGary Federal was a data security company that offered technical services to the government on issues of online corporate security, and had gotten word from the Department of Justice about BofA's concerns with WikiLeaks. Aaron

Barr, HBGary's CEO, met with his partners at Palantir and Berico to devise a plan of action to thwart WikiLeaks (Greenberg, 2012, p.183).

Their plan sought to undermine WikiLeaks credibility and sow dissension in its ranks using the tried and true COINTELPRO techniques of subterfuge, lies, and disinformation. One of Barr's chief targets was Glenn Greenwald, an internationally recognized American investigate reporter at The Intercept and well-known ally of WikiLeaks. Barr bluntly identified Greenwald as representing "the level of support we need to attack," describing him as a "professional with a liberal bent" who would cave under pressure. Barr concluded that, "Without the support of people like Glenn WikiLeaks would fold" (Greenberg, 2012, p.183).

But despite his best efforts, no lucrative government contract was forthcoming from this plan and Barr set his sights on another perceived security threat, one that he felt he could easily spy on using everyday social media. That security threat was Anonymous and Barr prepared another presentation on the subject entitled, "Who Needs the NSA When We Have Social Media?" (Greenberg, 2012, p.187). However, this plan ultimately proved to be Barr's downfall. When Anonymous discovered what he was up to, the hive went into action and subsequently hacked HBGary's company files and disseminated many of its most embarrassing emails to the public. Revelations of HBGary's dirty bag of tricks including surveilling enemies of the Chamber of Commerce, creating sockpuppets on social media to promote astroturf, and engaging in subterfuge to try to discredit well-known journalists and hacktivists, was enough to cost the company many of its most important contracts. Barr's career was over.

Out of the wreckage of Barr's career rose LuzSec (or Lulz Security), the group of breakaway Anonymous hackers who had precipitated his downfall and who had evidently developed a taste for government/corporate hacking. Though their meteoritic career lasted only fifty days (known as the "50 Days of Lulz"), they gained widespread notoriety with their spirited hijinks as well as their logo of "a stickman sporting a well-oiled, French-style, villainous mustache, replete with monocle, top hat, and three-piece suit – and sipping, naturally, a glass of fine wine" (Coleman, 2014, p. 239). LuzSec's targets comprised a veritable pantheon of government and corporate luminaries. "Sony Music Entertainment Japan, Sony Picture Entertainment, Sony BMG (Netherlands and Belgium), PBS, the Arizona Department of Public Safety, the US Senate, the UK Serious Organised Crime Agency, Bethesda Softworks, AOL, and AT&T": all became fair game for LuzSec (Coleman, 2014, p. 237).

Figure 4: LuzSec's Logo

Ever vigilant to perceived slights to WikiLeaks, PBS fell into LuzSec's crosshairs when its Frontline report on Julian Assange's website entitled *WikiSecrets* proved less than satisfactory. It "drew the ire of LuzSec members, notably Sabu [one of the groups' principals, later arrested and turned into an FBI informant] who disliked the film for how it skirted the pressing political issues raised by Cablegate in favor of a sensationalistic psychoanalyzing of the 'dark' inner life of Chelsea/Bradley Manning" (Coleman, 2014, p. 265). LuzSec retaliated for this transgression by hacking into PBS, stealing its staff data, and defacing its webpage. The latter drew titters around the Net for its tabloid depiction of Tupac Shakur with the headline "Tupac Still Alive in New Zealand" (Coleman, 2014, p. 266). Such epic pranks made LuzSec the unexpected darling of security types all over the Internet and its short but illustrious career lent rock star status to the hacktivist collective. When authorities finally caught up to them, the public was shocked to learn that two of LuzSec's key members were actually teenagers. Topiary was eighteen and T-flow was sixteen at the time of their arrests.

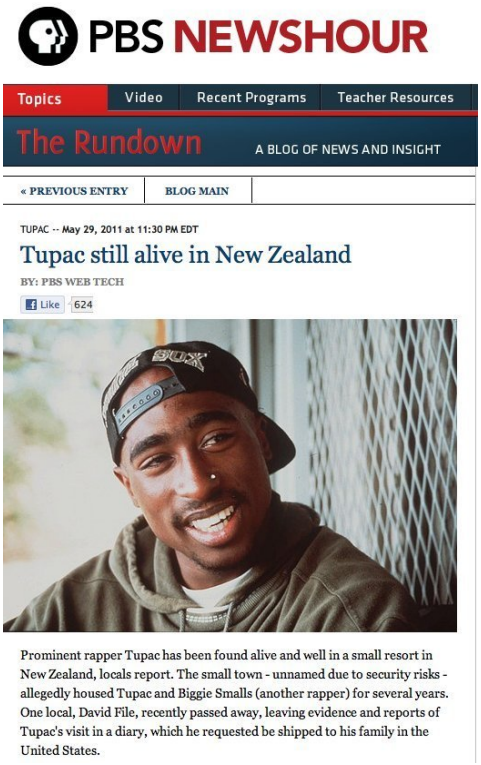

Figure 5. LuzSec Replaces PBS's Website with a Prank

Both Perelman and Lessig warn of a public discourse emptied of meaningful content due to government/corporate restrictions on free speech on the World Wide Web. In *The Realm of Rhetoric,* Chaïm Perelman (1982) has stated that,

> [Public debate] is intended to act upon an audience, to modify an audience's convictions or dispositions through discourse, and it tries to gain a meeting of minds instead of imposing its will through constraint or conditioning. We have seen that every argument presupposes a meeting of minds – a meeting which social and political institutions can facilitate or prevent. It is enough to think of the monopoly of the means of communication that characterizes totalitarian states, and of all the

means that are used either to protect or prevent this meeting of minds (1982, p. 11).

In the past three decades, a series of laws have gone into effect to ensure the protection of copyrighted materials over the Internet. Some of these include the Computer Fraud and Abuse Act of 1984, the Telecommunications Act of 1996, the Copyright Term Extension Act of 1998, and the Digital Millennium Copyright Act of 1998 – to name a few. While hacker/hacktivist efforts to ensure Internet accessibility has drawn support from other digital rights activists and civil liberty groups, it has conflicted with corporate and government institutions bent on securing and commercializing the content of the Internet.

For this reason, the hacker and hacktivist fight for freedom of information of the Internet has interesting historical parallels with the rise of an earlier form of writing technology: the printing press. Much as the printing press did in the medieval ages, the Internet has raised the specter of intellectual property rights at a time of burgeoning knowledge expansion. Just as medieval society struggled to quantify and commodify the development of modern books, periodicals, newspapers, and journals, the current commodification of digital information has created an economic resource that will either set the stage for the future meeting of the minds and the legitimate exchange of culture and learning or greatly control and inhibit it. In either case, the advent of both types of publication technology seized the imaginations of utopian visionaries who trumpeted declarations of the dawning of a new age of enlightenment. Like the seeds of a new world order of nations sown by Enlightenment ideas disseminated via the printing press, the possibility for a global new world order in cyberspace has been similarly heralded by utopianists espousing the evolution of human consciousness into an online global brain. However, utopian rhetoric necessarily brings with

it its opposite in the form of the dystopian, and the two different forms of communication technologies have elicited both prospects from their critics and admirers.

For this reason, the question of intellectual property rights has proven problematic in both epochs. In the medieval age, Church and State squared off against seditious and heretical texts printed by a small army of unregulated competing publishers. Medieval copyright law, like modern copyright law, confronted publishers with the problem of piracies and the spread of polemical ideas. This lead to the Licensing Act of 1662 in which the Church/state franchise granted large publishing houses exclusive publishing rights for promoted texts in exchange for the censorship of controversial ideas. With the Act of Queen Anne in 1710, the author was finally recognized as the legitimate holder of copyright, wresting control away from the patronage system of the arts that had previously dominated publication. Under the terms of the law, the author had the right to receive revenues from the sale of his/her book for fourteen years and this term could be renewed for another fourteen years. Texts automatically reverted to the public domain at the end of the copyright period (Febvre & Martin, 1997).

Modern copyright law, on the other hand, pits corporate and government authorities against hackers, hacktivists, and indymedia activists. Corporations have sought greater government control over *all* forms of copyright infringement including what had once been unregulated, non-commercial fair use of digital materials in the public domain. U.S. law governing intellectual property rights has developed concomitant with the growing trend toward the proprietization and commodification of information that signals the increasingly restrictive nature of the Information Age. Over time, the enhanced legislation and expanded scope of U.S. copyright law has resulted in the diminished availability of public works for a

future generation of scholars and artists. Indeed, Harvard law professor Lawrence Lessig (2005) has warned that, "the public domain is presumptive only for content from the Great Depression" (p. 25).

A brief overview of U.S. copyright law demonstrates Lessig's warning. For example, in 1909, the term of copyright in the U.S. was increased from fourteen to twenty-eight years and with a renewal of twenty-eight more years, copyright could be extended for a maximum term of fifty-six years. Legislation In 1976 extended copyright by another nineteen years and the term for renewal was dropped all together. Significantly, only the maximum term has been employed since 1992. In 1998, The Sonny Bono Copyright Term Extension Act (frequently called the Mickey Mouse Protection Act since Disney was one of the biggest lobbyists for the bill) increased the maximum term of copyright by another twenty years to give corporations copyright for ninety-five to one hundred and twenty years and authors a copyright term for the span of their life *plus* seventy more years. Lessig points out that "In the twenty years after the Sonny Bono Act, while one million patents will pass into the public domain, zero copyrights will by virtue of the expiration of a copyright term" (2005, p. 135).

It is perhaps noteworthy that in the middle ages only the lapse of half a generation was necessary before copyrighted materials were made available to the public, whereas in our own epoch an entire generation may go without being able to access the materials generated by its parents. The consequence of the expansion of copyright terms has been the loss of cultural works available in the public domain with the result that a culture of amnesia could well prove to be one of the inevitable by-products of the Information Age.

Another concern is the question of accessibility to new media material since copyright

has been expanded to include both *derivative and transformative* works. Whereas in the past, copyright infringement used to be the rather old-fashioned notion of making a direct copy of something, the growing prohibition against copying for derivative and transformative works means that any re-working of original materials may also be grounds for copyright violation. In the digital millennium, prohibitions against transformative and derivative works could include works produced through copypasta, sampling, mashups, remixes, fanfics, spoofs, parodies, and multimedia art to name just a few. Needless to say much artistic and intellectual innovation can be effectively curtailed under this application of the law.

One example of the far-reaching effects of such copyright infringements can be found in the case of mixed media artist Shepard Fairey. In altering a photograph taken of presidential candidate Barak Obama by an Associated Press (AP) reporter in 2008, Fairey succeeded in violating derivative copyright law. The fact that the AP reporter in question expressed approval of Fairey's work was not even a consideration in the case since the photograph was owned by the news company. The Associated Press sued Fairey for the rights to his famous Hope poster and he ended by settling out of court.

Figure 6. Shepard Fairey's Famous Poster was Sued by the Associated Press

In *Free Culture* (2005), Lawrence Lessig has summed up the situation thusly:

> For the first time in our tradition, the ordinary ways in which individuals create and share culture fall within the reach of the regulation of the law, which has expanded to draw within its control a vast amount of culture and creativity that it never reached before. The technology that preserved the balance of our history – between uses of our culture that were free and uses of our culture that were only upon permission – has been undone. The consequence is that we are less and less a free culture, more and more a permission culture (p. 8).

One has only to look as far as the controversy surrounding Biz Markie to get an idea of the nature of this problem. Ever since the ruling against the rap artist in 1992 for the sampling of a copyrighted song by Gilbert O'Sullivan, the original definition of what constitutes the fair use of materials for transformative purposes has grown far narrower. A New York court held that in the case of Grand Upright Music Ltd vs. Warner Bros Records Inc. (the latter Biz Markie's employer), all future Hip Hop and Rap artists would need to get permission or actually *purchase* the copyrights to the sampled songs they used in their compositions or risk being accused of copyright infringement. It perhaps goes without saying that Hip Hop is a musical genre typical of poor Black and Latino youths and like other forms of electronic music, relies heavily on sampling for its compositional scores. The prohibitive cost of purchasing the numerous samples necessary to create a typical Hip Hop piece has no doubt prevented many young artists of color from making it in the music world. This illustrates Lessig's caveat about the accessibility of digitized cultural materials in the

alleged Information Age:

> How free is this culture? How much, and how broadly, is the culture free for others to take and build upon? Is that freedom limited to party members? To members of the royal family? To the top ten corporations on the New York Stock Exchange? Or is that freedom spread broadly? To artists generally, whether white or not? To filmmakers generally, whether affiliated with a studio or not? (2005, p. 30).

III. Government and Corporate Responses to Hacktivists

In order to understand the relationship between the hacktivists and institutions that react to them in an adversarial manner, it is valuable to step back to contemplate broader theories of social structure and social organization for an examination of how they help us interpret power dynamics that are responsible for the evolution of political and social institutions in a global society. The adversarial government and corporate reactions to hacktivists and the corresponding counter-reactions to them by the civil rights community is one that according to Manuel Castells (2011) illustrates a network society of institutions and individuals in dialog with one another through digital media and advanced communication technologies. The purpose of the following discussion is to provide an overview of larger social theories at play in the online hacktivist community drawing on Castells and other authors that bear on the politics of the Information Age. Questions to keep in mind include: How are intellectual property rights and information security enforced by government and corporate interests and what does that signify for the hacktivist movement? How do government agencies and corporations respond to acts of cyber activism by hacktivist collectives? How has government surveillance and politically motivated responses to hacktivists modified the distributed information networks and social interactions of online hacktivist communities? How have hacktivists, in turn, responded to that?

Castells' works, *Communication Power* (2011) and *Networks of Outrage and Hope* (2012), are relevant because of his characterization of the nature of power and counter-resistance that create socio-political change over time. Castells' broad-ranging theory of social structure and social organization is based in part on the idea that modern society is a

network that mirrors the horizontal, non-hierarchical structures of the Internet itself. "In a certain way, the networking dynamics present in the [global justice] movement appears to bring to life the old anarchist ideal of autonomous communes and free individuals coordinating their self-managed forms of existence on a broader scale, and using the net as their global agora of deliberation without submission to any form of bureaucracy emerging from the mechanism of power delegation" (Castells, 2011, p. 345). He has noted that the online hacktivist community is an important part of the global justice movement: "The neo-anarchist current that has a strong presence in the movement against corporate globalization sees the expansion of global networks of communities and individuals as a political goal" (2011, p. 345). In *Crypto Anarchy, Cyberstates, and Pirate Utopias* edited by Peter Ludlow (2001), famed anarchist-syndicalist Noam Chomsky has defined the essence of anarchism as "The conviction that the burden of proof has to be placed on authority and that it should be dismantled if that burden cannot be met" (p. 436).

Castells has suggested that many hacktivists are also anarchists who embrace nonhierarchical, leaderless social structures as a matter of principle and who work in solidarity with worldwide social and environmental justice movements. He seems to harken back to older utopian ideals of alternative societies that flourished alongside the development of the printing press when he queries: "Could it be that the technological and organizational transformation of the network society provides the material and cultural basis for the anarchist utopia of networked self-management to become a social practice?" (2011, p. 346). Useful comparisons can be drawn between the development of a network society as outlined by Castells in general and the rise of hacktivism in particular.

For this reason, Castells' ideas pertain to my own research into hacktivism on several levels. First, they help me interpret the adversarial government and corporate reactions to hacktivists; second, they help me interpret the counter-reactions to authorities by hacktivists and the civil rights community; third, they help me understand the power dynamics that affect a social network of institutions and individuals in dialogue with one another through digital media and cybernetic technologies.

Also relevant to the discussion are Earl and Kimport (2011) in *Digitally Enabled Social Change* as well as Bennett and Segerberg in *The Logic of Connective Action* (2012). Both sets of authors are interested in whether or not decades-old theories of collective action drawing from sociology and political science apply equally to political action in the contemporary Information Age. These ideas bear on my research into hacktivism because they help me elaborate a critique of political institutions in order to arrive at an understanding of the larger question of the nature of modern political change on the World Wide Web.

Basso's (1997) *How Public Relations Professionals are Managing the Potential for Sabotage, Rumors and Misinformation Disseminated via the Internet by Computer Hackers* is also pertinent for its depiction of the corporate efforts to mitigate the negative public relations of hackers with regards to company products and services on the Internet. Basso explores how corporations create two-way communication channels with consumers on the Internet in a face-saving tactic to ameliorate the negative publicity generated by the hacktivist community critical of their poor business performance. In order to understand the reaction of civil rights, social justice, and grassroots organizations to hacktivism, it is also helpful to explore Nissenbaum's *Hackers and the Contested Ontology of Cyberspace* (2004)

for her discussion on the ontological shift in perception that has seen the increasing demonization of hackers over time.

In short, the purpose of my discussion is to examine how these authors' ideas of social structure and social organization can be used to discern far-reaching theoretical insights into the study of hacktivism and global socio-political movements in a digitally enhanced world.

A. Communication Power

This portion of my dissertation examines Manuel Castells's theories of power, counter power, and the function of ideologies in producing socio-cultural political change over time. At this juncture, I primarily look at *Communication Power* (2011), but later on, I also examine Castells' *Networks of Outrage and Hope* (2012). Castells has studied the digitally mediated world of communication in order to elucidate ideas of power and counter power in a global network society. Specifically, Castells has looked at information and communication technologies (ICT) in a networked society as a discursive setting for expressing the conflict of beliefs and values of powerful social actors in national and international politics. One of Castells's main points in *Communication Power* is the idea that a networked society will result in the total transformation of global power dynamics due to technological innovations in mass self-communication supporting individual political autonomy (2011, p. 58).

Castells has defined the exercise of power as one of two kinds of seemingly contradictory social forces: coercive and persuasive. He has stated that power is "the relational capacity that enables a social actor to influence asymmetrically the decisions of

other social actor(s) in ways that favor the empowered actor's will, interest, and values. Power is exercised by means of coercion (or the possibility of it) and/or by the construction of meaning on the basis of the discourses through which social actors guide their action" (2011, p. 10). Castells references Michael Foucault's idea of "disciplinary discourse" for its importance in understanding state power derived through violence. He has also referenced Weber (1919) who has observed that, "every state is founded on force" (2011, p. 15). Ultimately, it is the government's ability to regulate society through the punitive enforcement of rules carried out by violence upon the transgressor through confinement and capital punishment that is commonly understood to serve as the basis for the preservation of the social order.

Yet an equally important aspect of state power is discursive in nature and involves the framing of public opinion via verbal expressions of state power. After all, power that is internalized in the minds of its subjects as a just, necessary, or benign force for social control is more likely to succeed in the long run than power that is not accepted by its subjects. The manner in which the state frames its discourse is a basic means for exercising its power by constructing social ideology that manifests as social institutions. Legitimatization is key to the process for establishing the social acceptability of the power of social institutions and the main ingredient for its establishment is through persuasive appeals. "Legitimacy largely relies on consent elicited by the construction of shared meaning; for example, belief in representative democracy" (p.12). All told, the power exercised by the state and its social institutions requires it to be at once violent *and* discursive.

Interestingly, Castells has advanced the idea that state power is being fundamentally reconfigured via the Internet to usher in the development of a global order of networked states. He has called this "the network society," and has emphasized that "networks are communicative structures" (p. 20). Thus, Castells's elaboration on the global network state takes into account two powerful types of actors in a world-wide distributed information system: the programmers and the switchers. Programmers are those people who create the networks and switchers are those who coordinate the networks together. Castells has posited the idea that the networks themselves are the holders of power and that such "actor-networks" are not single individuals but groups of people networking with one another to carry out activities in coordination with other groups. He thus discounts entirely the idea of a power elite, which no doubt contributes to his often utopianist interpretation of the Internet. According to Castells, network switchers are most powerful at the nodes where business, finance, political, media and cultural networks connect up.

Yet wherever power is exercised, the possibility exists for the dissemination of its opposite message. "There is always the possibility of resistance that calls into question the power relationship, " contends Castells. He has described the relationship of state power to insurgent forces in society as one that predominates through human communication and, in modern network society, through digital network communication systems. Looked at within the context of Castells' theoretical concept of power versus counter-power, the U.S. government representing state power can be seen to be in dialogue with hacktivists representing counter-power in an argument over political realities on the Internet. This is particularly true with regard to the control and regulation of the network society itself as attested to by the recent government decision to greatly weaken the public protection

afforded by the Federal Communications Commission (FCC) and all but eliminate Net Neutrality. The fight for control of the Internet and digital media overall is a power dialectic that pits social reformists demanding freedom, equality, and social justice on the Net against government and corporate interests seeking to maintain and extend the hegemony of the current status quo.

Castells's discussion of communication on the World Wide Web is one about the expressions of social power, which, as already noted, is at once persuasive and coercive. The persuasive aspect of power is a function of global communication networks and such networks are central to the creation and maintenance of power. With the rise of digital and wireless technologies, the Information Age has heralded a revolution in human communication systems. Unlike older forms of mass media communication that conveyed a single text by a single author to multiple recipients, new mass media communications convey multiple texts by multiple authors to multiple recipients. Castells has dubbed this phenomenon "mass self-communication" and feels it plays a significant role in enhancing individual political autonomy (2011, p. 58).

While theoretically, anyone with access to a computer can broadcast themselves to the world via the Internet, Castells has nevertheless noted that problems of unequal educational access compounded by global inequalities in race, ethnicity, class, gender, and religion, are contributing to a digital divide. Needless to say, this digital divide between those possessing advanced communication and information technologies and those that do not is one abhorred by free data activists everywhere. Castells has also noted that two seemingly contradictory social forces – individualism and communalism – have been paralleled by the rise of a global culture in tandem with a multiple identity cultures. Somewhat paradoxically,

globalization favors both the branded consumerism of individualism as well as the cosmopolitanism of communalism. Identity politics favors both networked individualism as well as global multiculturalism. "These are the basic cultural patterns of the global network society [a]nd this is the cultural space in which the communication system must operate" (p. 121). As Peter Ludlow has posited in the opening of *Crypto Anarchy, Cyberstates, and Pirate Utopias* (2001), "not only is the Internet undermining the traditional media, but it is also reshaping the nature of our commercial infrastructure. If identity remains hitched to regular trade and commerce … then it is clear that our sense of identity is about to be unhitched from our national borders" (2001, p. 5).

The Internet is facilitating the transition from national identity to global identity. Traditional forms of mass media (newspaper, television, publishing, movies, and radio) remain important to communication networks especially since they have been concentrated into the hands of fewer and fewer owners. This has now reached the point where only seven transnational media companies dominate all media networks. These seven corporations are NBC, CBS, Viacom, Time Warner, Disney, NewsCorp, and Bertelsmann. At the same time, the rise of the Internet and wireless technologies has diversified media expression like never before with over 1.4 billion new Netizens and potential producers of content by 2008 alone (p. 62). Blogs, Vlogs, podcasts, social media, wikis, and file sharing represent just a few of the new forms of mass self-communication that proliferate on the Internet.

In recent years, new media giants have clashed with old media giants for the control of content shared over the Internet. Hacktivists coordinated with major websites to participate in an Internet Blackout Day that resulted in the dramatic shutdown of Wikipedia, Google, Twitter, Tumblr, and many more in a day of online protest against the Stop Online Piracy

Act (SOPA) and the Protect IP Act (PIPA). I will discuss this at greater length further on in my discussion when I delve into the life and times of Aaron Swartz, one of the principal organizers behind the protests despite his own prosecution by the government for alleged copyright infringement. Suffice it to say for now that "regulatory policies are in the hands of institutions that, in principle, are supposed to defend the public interest, but they often betray this principle, as in the past two decades in the United States" (Castells, 2011, p. 136).

Also of importance is the fact that individual cognition is social in nature and is greatly influenced by the discourse of political power in society. Therefore, another critical kind of network Castells has addressed is that of the brain's *cerebral* network. According to Castells, the brain's manner of processing information renders individuals akin to neural "networks connected to a network world" (2011, p. 139). "Since meaning largely determines action, communicating meaning becomes the source of social power by framing the human mind" (2011, p. 136). The role of emotions, thoughts, and beliefs is fundamental to motivating and communicating political action. The use of metaphors, narratives, and linguistic/cognitive frames activate "specific neural networks" that set into play patterns of association used in semantic fields to facilitate thinking processes in the real world. Framing is a way to present (and manipulate) discussion on a given subject by drawing attention to certain issues and making connections between them in order to support a favored outcome.

An important contributor to the field of linguistic framing and cognitive semantics, George Lakoff (2004), has observed that the manner in which the political right and political left frame their respective debates ends up creating a clash of values with the moral identity

of the right pitted against the empirical rationality of the left. Conservatives take a virtuous and moral-laden stance toward their political decision-making processes, while liberals take a rational and knowledge-laden stance toward their political decisions (2004). This is one reason why liberals are so frequently puzzled by the seemingly self-defeating behavior of poor, white working-class Americans who consistently vote for politicians bent on doing away with their rights as workers and citizens. "People do not necessarily vote in their self-interest. They vote their identity. They vote their values" states Lakoff (2004, p. 19). According to Lakoff, "Frames are mental structures that shape the way we see the world. In politics our frames shape our social policies and the institutions we form to carry out policies. When you hear a word, its frame (or collection of frames) is activated by your brain. Because language activates frames, new language is required for new frames. Thinking differently requires speaking differently" (2004, p. xv).

With reference to Castells's discussion of the neural nets of human brains, the individual's emotional world of hope and fear informs the values and attitudes that underlie the political ideology from which their frames arise. Just as anxiety leads to avoidance behavior, fear tends to paralyze action. Conversely, anger tends to lead to confrontational behavior while hope tends to motivate action (Castells, 2011). In order to manipulate feelings, politicians make emotional appeals to evoke popular sentiments directed toward specific campaigns. The skilled manipulation of such emotions by framing the issue is one of the key techniques of any politician (or demagogue) seeking to advance a political agenda. With this intent, the state communicates its political agenda through the media, which is used to prime and frame the public mind for favored initiatives and outcomes. "Power-making proceeds by shaping decision-making, either by coercion or by the

construction of meaning, or both" (p. 189). This then is the power of framing political debate in the public mind.

The late popular counter-culture figure Frank Zappa once opined that, "Politics is the entertainment division of the military industrial complex." The framers and programmers of communication networks are most often governments, corporations, and elite interests, and they frequently make use of the visceral appeal of what Castells has dubbed "scandal politics" to advance their agendas. As news increasingly becomes *infotainment*, scandal politics is used to simultaneously instruct and program the public. For this to happen, media networks and political networks must work in tandem together, a phenomenon Castells describes as "media politics." Media politics is the performance of scandals by high-profile personalities on the public stage of the media (Internet, newspapers, television, radio, etc.). This is necessary because "the most successful reporting is one that maximizes the entertainment effects that correspond to the branded consumerist culture permeating our societies….[F]or these issues (for example, the economy, the war, the housing crisis) to be perceived by a broad audience, they have to be presented in the language of infotainment in the broadest sense; not just laughing matters, but human drama as well" (p. 201). Thus, personality politics helps the public to discern, discriminate, and decide among often competing political possibilities by reducing them to simple narratives telling personal stories easily comprehended by all. It is perhaps noteworthy that the most popular narratives are often the most simplistic and typically involve a hero, a villain, and a damsel in distress.

Another important way to program communication networks and frame popular issues in the public mind is through think tanks and foundations. This is what Castells has called "informational politics." Think tanks are useful for disseminating carefully constructed

political messages that frame current events. "The production of the message has to proceed as an interface between the characteristics and values of the politician and the characteristics and values of the intended target audience" (p. 205). Major think tanks serve to create that interface. The construction of commonalities of interests in the public mind via big think tanks is one that has successfully shifted popular politics to the right in the past twenty years due to the dominance of the GOP in conjunction with the corporate and religious groups who have funded and disseminated their ideologies. Castells has attributed this to the Powell memo, a right-wing manifesto for advancing a reactionary political agenda in America: "The Powell memo is usually credited with launching the rise of right-wing think tanks and the "new right approach to American politics" (p. 207).

The simplest way to program communication networks is through direct government/ corporate intervention in the media by planting select stories while simultaneously censoring others. But indoctrination through propaganda comes at a price. Media control of social messaging through the promotion of scandal politics has contributed to a crisis of political legitimacy that bedevils the global network age and has all but destroyed public trust worldwide (Castells, 2011). The crisis of democracy is one that is exemplified by the "systemic disassociation between communication power and representative power" (p. 298). In other words, the increasing meaninglessness of scandal politics and what Castells has called the "killing of semantic fields" (p. 196) has overcome the citizenry's ability to engage in full participatory democracy anymore. Nowhere is this phenomenon more notable perhaps than in the 2017 presidency of former reality television star, Donald Trump.

"If power is exercised by programming and switching networks, counter-power, the deliberate attempt to change power relationships, is enacted by reprogramming networks

around alternative interests and values, and/or disrupting the dominant switches while switching networks of resistance and social change" (p. 431). In this sense, reprogramming networks through the expression of counter-power has much in common with the practice of guerilla semiotics, reality hacking, and culture jamming, all forms of subversion that try to disrupt commonplace expressions of neo-liberal consumeristic ideologies. In *Alternative and Activist New Media* (2013), Leah A. Lievrouw defines cultural jamming as a "genre which critiques popular/mainstream culture, particularly corporate capitalism, commercialism, and consumerism. Here, media artists and activists appropriate and 'repurpose' elements from popular culture to make new works with an ironic or subversive point - put another way, culture jamming 'mines' mainstream culture [in order] to critique it" (2013, p. 22).

The opposite of the programmers of communication networks are the *re-programmers* who are frequently the protesters who organize social movements. These are the individuals who fight to reform and revolutionize the system in order to put power back in the hands of the people. At their essence, "Social movements are formed by communicating messages of rage and hope" (Castells, 2011, p. 301). Because of the horizontal networks of communication that typify such insurgent politics, Castells opines that the Internet is particularly conducive for use by reformists and social justice organizers. He has looked with optimistic hope to the self-governing principles of autonomy the new networks enable due to "the potential synergy between the rise of mass self-communication and the autonomous capacity of civil societies around the world to shape the process of social change" (2011, p. 303). New cultures of hope and reform can be seen in the environmental movement – in particular the climate justice movement – as well as mass global movements

against the corporatocracy (for example the WTO Seattle protests, and ongoing protests against NAFTA/TPP). Additionally, the rise of the indymedia movement, the growth of the hacktivist community, and the hope for a utopian society founded in the principles of anarchy and civil liberties are also contributing to the enactment of social reform and renewal. "Enacting social change in the network society proceeds by reprogramming the communication networks that constitute the symbolic environment for image manipulation and information processing in our minds, the ultimate determinants of individual and collective practices. Reprogramming networks of meaning substantially affects the exercise of power throughout all of the networks" (2011, p. 412 - 413).

On a more cautionary note, it is perhaps worth pointing out again that the siren song of utopianism has been around since the beginning of the Internet with historical precedence even further back in time with the advent of the printing press. Peter Ludlow has quoted Mark Dery in the opening of *Crypto Anarchy, Cyberstates, and Pirate Utopias* to make this point: "[The Digerati] and the world they inhabit is a memory of futures past - the topdown technocracies of the 1939 World's Fair or Disney's Tomorrowland, socially engineered utopias presumably overseen by the visionary elites who 'basically drive civilization,' as Stewart Brand famously informed the *Los Angeles Times*" (2001).

B. The Digital Commons

The enclosure of the electronic creative commons is a very distinct possibility especially given the significant expansions of copyright laws since the 1980s. While Castells has recognized that "politically active hackers…have become a key component of the global

justice movement" nevertheless he cautions that all is not well in cyberspace (2011, p. 345). "As the potential of the industrial revolution was brought to the service of capitalism by enclosing land commons, thus forcing peasants to become workers and allowing landowners to become capitalists, the commons of the communication revolution are being expropriated to expand for-profit entertainment and to commodify personal freedom" (2011, p. 414). Castells has further noted that, "This is why perhaps the most decisive social movements of our age are precisely those aimed at preserving a free Internet, vis-a-vis both government and corporations, carving a space of communication autonomy that constitutes the foundation of the new public space of the Information Age" (2011, p. 415).

The hacker/hacktivists' belief that information is a basic human right, that censorship is an impediment to communication, and that digital privacy should be guaranteed – are all precepts of the alternative computing and online political dissident community. The government, on the other hand, balances such populist ideas against intellectual property rights for maximizing private corporate profits. It also seeks to censor some forms of content on the Internet such as pornography, as well as any and all information pertinent to national security interests. In an address to the Nuclear Age Peace Foundation in February of 2014 in Santa Barbara, Noam Chomsky discussed the rising U.S. surveillance state as evidenced by Snowden's exposure of the National Security Agency's (NSA) massive global spying program. The tensions between the conflicting interpretations over the socio-epistemic function of information by hacktivists and authorities have occurred against the backdrop of growing government secrecy, ongoing national security concerns, and the accelerating trend toward the privatization of the public domain by major corporations. The latter has resulted in the promotion of corporate interests over public in just about every

sphere of domestic affairs – from social programs, to public utilities, national parks, and cultural works to name just a few. Yet simultaneously, a growing global justice movement representing the people's interests in economic equity, open and transparent democracy, and social and climate justice has led to massive anti-corporate and anti-government protests around the planet in the past decade.

C. Networks of Outrage and Hope

Since the Tunisia revolt of early 2011, the desire for a more participatory democracy has ignited the imaginations of millions around the world. The Days of Rage that followed the Tunisian and Egyptian uprisings provoked sympathetic protests across the Arab world – Algeria, Syria, Lebanon, Jordan, Sudan, Oman, and Yemen, to name just a few. These were frequently met with violent state suppression. Outrage at state brutality in places like Egypt and Tunisia was what sparked the uprisings in the first place where people were able to overcome their fear in order to resist violent state suppression. Yet as Castells has cautioned in *Networks of Outrage and Hope* (2012), "When movements are determined enough to keep up relentless pressure on the state regardless of the violence they endure, and the state resorts to extreme violence (tanks against unarmed demonstrators), the outcome of the conflict depends on the interplay between political interests in the country and geopolitical interests related to the country" (2012, p. 97). Syria and the Ukraine are probably the most recent examples of this.

The Egyptian, Arab, and Spanish uprisings came to be known as the Arab Spring, which in turn became the inspiration for the political protests of the Occupy Wall Street (OWS) movement in the United States. The latter event was triggered in part by the labor union

protests in Wisconsin as well as the reaction to online cyber attacks against information posted by a website called AmpedStatus concerning the economic meltdown and banking crisis of 2008. When a group of hacktivists named Anonymous went to the website's defense, their struggles to protect the information on AmpedStatus eventually led to the alliance of the two groups for the creation of a 99% movement. With a concomitant call to protest Wall Street's economic practices put out by Adbusters – a cultural jamming website known for its anti-consumeristic ideologies – the occupation of Wall Street was decreed for September 17th. However, the Occupy Wall Street (OWS) movement was only successful in doing so because of the previous work of such dissident hacktivists as Anonymous and Bloombergville. Hacktivists were therefore instrumental in setting the stage for one of the biggest political protests in American history (Castells, 2012, p. 161).

There can be no denying the importance of social media in the rise of protests movements worldwide in 2011. One of the key features of the OWS movement was its use of social networking sites such as Facebook, Twitter, Tumblr, and Livestream to keep activists posted on developing events in Zucotti Park and across the United States. Ingenious methods for constructing wireless Internet connections despite the police crackdown on life in Zucotti Park's encampments led to an almost constant flow of information out of New York to a wired-in network of national activists. Castell's *Networks of Outrage and Hope* (2012) examines the rise of socially networked movements such as Occupy Wall Street and postulates that such expressions of counter-power portend serious challenges to entrenched institutions in the future.

For example, in Iceland's Kitchenware Revolution of 2008 – where protestors beat on pots and pans in protest of political and banking corruption – the new social democratic

government of the country decided to crowdsource the reform of its constitution by making what some observers have called the first ever "wiki-constitution." Iceland's reform-minded Constitutional Assembly Council (CAC) used Facebook to coordinate public debate on the new constitution while simultaneously using Twitter to publish its progress. "The CAC received online and offline 16,000 suggestions and comments that were debated on the social networks. It wrote fifteen different versions of the text, to take into consideration the results of this widespread deliberation" (Castells, 2012, p. 31). Thus, Iceland serves as a model for how the new "commons knowledge" facilitated by the Internet can serve a novel kind of radical, participatory democracy in an exercise of digitally enabled mass self-government (Lievrouw, 2011, p. 177).

In Egypt, where political protests took a particularly violent turn when state police retaliated against reformists, young Egyptians used mobile phone and social media like Facebook to amplify and send their messages of dissent to the international community. To a great degree, their efforts were facilitated by Al Jazeera (a traditional newspaper with anti-colonialist sympathies) since it allowed its media platforms to host the live-streams and tweets from the cellphones of activists when they clashed with police on the ground. In the process, Al Jazeera promoted the kind of citizen journalism that is perhaps the hallmark of networked mass self-communication and the indymedia movement.

In desperation, the Egyptian government tried to employ a kill switch to turn off all forms of networked communications with the result that once again the international Internet community – comprised of "hackers, techies, companies, defenders of civil liberties, activist networks such as Anonymous, and people from around the world for whom the Internet had become a fundamental right and a way of life" (Castells, 2012, p. 62) – came to the rescue.

This state of affairs lasted a couple of days before Internet communication was restored. Castells has reported:

> In fact, the revolution was never incommunicable because its communication platforms were multimodal. Al Jazeera played a crucial role in continuing to cover the protestors by reporting on the uprising against the regime. The movement was kept informed by images and news received from Al Jazeera, fed from reports by telephone on the ground. When the government closed its satellite connection, other Arab satellite television networks offered Al Jazeera the use of their own frequencies. Furthermore, other traditional communication channels like fax machines, ham radio, and dial-up modems helped to overcome the blocking of the Internet (Castells, 2012, p. 63).

In the case of the OWS movement, Occupiers used social media not only to send out the initial call to action via Twitter, but also to narrate personal accounts of the movement via Tumblr as well as to cover police crackdowns on Livestream, and to post actions and events on Facebook. The latter has usually gone hand-in-hand with Occupy websites to help less tech-savvy people communicate on the Internet. Nevertheless, Facebook in particular has come under criticism by Occupiers since it refuses to guarantee the privacy of its users and its "proprietary platform…[is] at odds with the openness valued within the movement" (Castells, 2012, p. 175).

Chilean poet Pablo Neruda has written about the eternal renewal of hope in each new generation: "Podrán cortar todas las flores, pero no podrán detener la primavera" (They can cut all the flowers, but they can't stop Spring). In examining how multimedia networks of

communication facilitate individual political autonomy, Castells has noted that just as social movements require the networked world of cyber space, they also need a physical location in the real world in order to permit organizers to meet and plan together face-to-face. In Egypt, demonstrators occupied Tahrir Square. In Spain, the Indignados camped out in the town center of Barcelona. In New York, the OWS movement occupied Zuccotti Park. In Iceland they took over Austrurvollur Square. Almost all were inspired by the economic meltdown of 2008 as the result of big banks invested in mass foreclosures, precipitating a world-wide economic downturn that has accelerated income inequality around the planet. This blending of spaces that occurred between virtual reality and physical places – what Castells characterizes as the space of flows and the space of places – contributed to the creation of a hybrid space that enabled communities of practice to imagine, plan, and collaborate together. It is perhaps one of the more noteworthy features delineating the differences between recent worldwide political protests from older social movements. While past social protests have occurred in distinct locales removed in space and time from their allies, rendering them unwieldy to coordinate, the new social movements enjoy the relative freedom of the collapsed space and time continuum afforded by the Internet. This makes them significantly easier and faster to coordinate due to the instant transmission of information through advanced communication technologies. As Castells has noted,

> The space of the movement is always made of an interaction between the space of flows on the Internet and wireless communication networks, and the space of places of the occupied sites and of symbolic buildings targeted by protest actions. This hybrid of cyberspace and urban space constitutes a third space that I call a space of autonomy. This is because autonomy can only be insured by the capacity to organize

> in the free space of communication networks, but at the same time can only be exercised as a transformative force by challenging the disciplinary institutional order by reclaiming the space of the city for its citizens (Castells, 2012, p. 222).

But what did the protesters want exactly? This was the subject of much old-school speculation in the mainstream media, which tended to paint the civil disobedience of protesters as the acts of rabble-rousers, anarchists, and malcontents, particularly in the case of the OWS movement in the U.S. "For many people in the movement, and for almost all external observers, particularly those intellectuals on the left always looking for the politics of their dreams, the lack of specific demands by the movement was a fundamental flaw" (Castells, 2012, p. 187).

Yet in the new media spheres of cyberspace, the revolution was being televised to a web of wired-in and connected political activists who had a very different take on the purposes, goals, and directions of the movement than those presented by older media spheres of influence in television, radio, newspapers, and magazines. "Indeed, the movement was popular to many precisely because it remained open to all kinds of proposals, and did not present specific policy positions that would have elicited support but also opposition within the movement as shown in the divisiveness that emerged in most occupations each time a committee put forward specific programs for reform" (Castells, 2012, p. 187). In some respects, the tale of the OWS movement and protests movements worldwide in 2011 is the tale of two media spheres – the 4th estate and the 5th estate – and their attendant clash of platforms, content, , values, and audiences as they have struggled to frame the political debate for an increasingly wired-in global community.

D. Digitally Enabled Social Change

Is there any significant difference between social movements of the past and the social movements of today? This question has been addressed by Earl and Kimport in *Digitally Enabled Social Change* (2011) as well as Bennett and Segerberg in *The Logic of Connective Action* (2012). Both sets of authors have addressed the issue of whether or not decades-old theories of collective action apply equally to political action in the contemporary electronic age. In *Digitally Enabled Social Change* (2011), Earl and Kimport have argued that the difference between past forms of organizing social protest and the new forms of organizing lies in the use of the Internet itself. These theoreticians view the Internet as an instrument for social reform. They have criticized past theoreticians of social movement protest for their failure to look at "who organizes and how organization takes place as well as who participates and their affiliation with a larger social movement" on the World Wide Web (2011, pg. 29). They have contended that digitally enhanced, networked communication creates two key benefits not realizable by earlier forms of social organizing: 1) the relatively cheap cost of online mobilizing and 2) the freedom to meet, work, and plan together in cyberspace outside of normal time and space (2011, p. 10). Earl and Kimport have questioned "the utility of well-honed theories such as resource mobilization when the costs fall low enough," claiming instead "that in some cases, what existing theories have always taken as a constant may in fact vary. For social movement scholars, [this] analysis helps to deepen [an] understanding of existing major theories and identify places where significant theoretical modifications or new developments are needed" (2011, p. 16). In self-reflexively engaging in a study of social movement theories, Earl and Kimport posit the idea of a need

for "theory 2.0" of "e-movements" which stands in contrast with a "Supersize" model of web organizing "where the web leads to faster, wider, cheaper, activism but without fundamental changes to the dynamics of contention" (2011, p. 13). Unlike the Supersize model of online organizing benefits, Theory 2.0 examines alterations in the fabric of social protest itself. It is the idea that "the use of Internet-enabled technologies changes the underlying processes of activism. Organization and participation, benefiting from the affordances of Internet-enabled technologies, are less expensive, quicker, and more convenient" (p. 29). One example of Theory 2.0 at play can be found in the online coordination of strategic voting among citizens during the struggle for U.S. presidency between Bush and Gore in 2000 (p. 8).

Earl and Kimport further break down online Internet organizing as "e-mobilization" (bringing activists together on a particular cause), "e-tactics" (signing online petitions, creating emailing campaigns and initiating online boycotts) and "e-movements" (direct action civil protest in real time and space) and they engage in an analysis of particular websites "to provide a population-level view of the use of these e-tactical forms on the web" (2011, p. 17). Yet Earl and Kimport insist that Theory 2.0 does not constitute "throwing the baby out with the bathwater" (p. 38). Rather, "social movement theory developed and tested over time is not rendered obsolete by emerging work on Web activism; indeed, even uses of the Web that strongly leverage affordances don't make existing social movement theory irrelevant" (2011, p. 38).

In *The Logic of Connective Action* (2012), Bennett and Segerberg have examined the difference between collective action versus connective action. They break this down into three subsets: organizationally brokered collective action (think labor unions, and

progressive movements of the 20th century) contrasted with organizationally enabled connective action (think Internet facilitated individualized action) and crowd-enabled connective action (think networked social activism á la Castells in *Networks of Outrage and Hope*). In the course of the book, they have focused on three main themes that serve to illustrate the nature of connective action. The first deals with the personalized nature of digitally mediated political engagement insofar as new forms of social movements are much more dispersed, individualistic, and identity-driven than earlier movements. "Various globalization-related changes have resulted in the separation of many (particularly younger) individuals from the integrative structures of modern society, such as class identification, church, party, union, and traditional family and career models" (Bennett and Segerberg, 2012, p. 6).

The second theme addresses communication in connective action and its role in forming social institutions and practices. Bennett and Segerberg state, "At the core of this book is thus an idea about c*ommunication as organization"* (2012, p. 8) and they point out how Twitter effectively coordinates meta-data that facilitates online mobilizations via hashtags. The third theme analyzes the logic of connective action in order to ascertain how different organizing principles may underlie different mobilization strategies (2012, p. 10). They argue that there is a world of difference between a *logic of collective action* (which is largely group oriented) and a *logic of connective action* (which is often more individually oriented).

In the finally analysis, both sets of authors conclude that older theoretical models of social movements are insufficient to account for the new digitally-enabled social movements of the World Wide Web. For purposes of my analysis of hacktivism, it may also be useful to explore how selective exposure to institutional ideologies shapes opinion and

participation in democracy in order to elucidate the framing of the larger public debate over hacktivism. A few of the government agencies reacting in an adversarial manner to hacktivists have included the National Security Agency (NSA), the Central Intelligence Agency (CIA), the Department Of Justice (DOJ), the Federal Bureau of Investigations (FBI), the Federal Communication Commission (FCC), and Congress. These institutions can be understood as social actors responsible for creating a social narrative that reflects dominant commercial and security interests.

The domination of government regulatory agencies by corporate lobbyists for the control of intellectual property rights on the Net in order to maintain bottom-line profits is a reality that hacktivists abhor. Unfortunately, the regulatory capture of government agencies by corporate takeover has become extremely pervasive. Specific laws aimed at Net Neutrality and the Digital Millennium Copyright Act (DMCA) – as well various incarnations of COICA (Combating Online Infringement and Counterfeiting Act), SOPA (the Stop Online Piracy Act), PIPA (Protect IP Act), and CISPA (Cyber Intelligence Sharing and Protection Act) – present some of the most recent examples of government regulations serving corporate interests to ensure intellectual property rights on the Internet. Such information policy often comes at the expense of the freedom of information so valued by hackers and hacktivists. The recent demise of Net Neutrality represents the political power of corporations in everyday life as big telecom giants like Verizon have finally succeed in putting a meter on the internet in order to charge variable rates to consumers depending on the amount of broadband width used. The creation of information toll roads in place of information freeways has yet to be ascertained for the extent of its damage to the right to access the Net though it is apparent that those with less money now have less access.

Likewise, the Trump administration's decision to cut programs to help maintain the affordability of the Internet for the poor will also increase the digital divide.

In the Digital Millennium, copyright poses a particularly thorny problem for big media giants due to the ease of duplicability of digital files over the Internet. Peer to peer (P2P) file sharing is an Internet feature that is a particular sore point for old media firms accustomed to traditional modes of publication and remuneration. Further complicating the problem, literacy in the digital age has come to increasingly signify not only knowledge and use of the printed word, but also video, audio, and graphics as well. This in turn poses a problem of epic proportions for media giants like the Recording Industry Association of America (RIAA), the Motion Picture Association of American (MPAA), and giant publishing conglomerates like Elsevier as they scramble to compete with new forms of web media like Google, YouTube, and Facebook, in addition to new types of literacy technologies like eBook. Unable to control distribution channels as they formerly have, old media giants have sought to control the Internet in order to maximize their traditional revenue sources. With equal fervor, new media titans maintain a vested interest in the freedom of expression and distributed information networks of the World Wide Web. The legal wrangling over the Stop Online Piracy Act (SOPA) and the Protect IP Act (PIPA) has proven to be acrimonious for at issue lies a question of open access and intellectual/artistic expression as a public good versus intellectual property right and the commodification of information for private profit. As might be expected, corporations seek expanded policies to control online piracy and ensure bottom-line profits. This has led hacktivists like Aaron Swartz to muse, "There's a battle going on right now, a battle to define everything that happens on the Internet in terms of traditional things that the law understands. Is sharing a

video on BitTorrent like shoplifting from a movie store? Or is it like loaning a videotape to a friend? Is reloading a webpage over and over again like a peaceful virtual sit-in or a violent smashing of shop windows?‟ (2015, p. 77).

Enter Digital Rights Management (DRM). A kind of digital lock placed on protected content, DRM is designed to regulate the distribution of copyrighted materials by encrypting protected digital materials and rendering them inaccessible to users without a key. What is more, restrictive licensing agreements (e.g., terms of service agreements or clickthrough contracts) such as those required before entering an online music store force the buyer to agree to the terms of use imposed by the seller of digital merchandise. Internet music stores such as Apple iTunes use DRM to restrict the number of times a file can be downloaded to registered computers and iPods, as well as the number of copies that can be burned from the download (even though the latter is still considered within the domain of fair use). Interestingly, Apple is being sued for anti-trust violation since it has been accused of using its DRM technology (dubbed "FairPlay") to prevent patrons of its iTunes store from being able to play their purchases on anything other than an iPod. Apple has since dropped the use of its FairPlay license from purchases of music from iTunes, but it still enforces it for purchases of video and iOS apps.

Overall, DRM has proven very unpopular with the wider public especially when applied to physically purchased CD's because it prevents encrypted CD's from being played on computers unable to recognize the DRM code. Companies like Sony BMG surreptitiously installed a form of DRM malware on users' computers when they played coded CDs, which had the effect of breaching the user's security systems. This resulted in several lawsuits against Sony, with the consequence that it, along with several other record labels, dropped

the sale of all audio CDs encrypted with DRM. Nowadays, recording studios and artists increasingly market their music as "DRM-Free." Nonetheless, DRM technology continues to proliferate among online music stores in a great variety of forms making it nearly impossible for the user to move easily between distribution platforms.

As has already been seen, entertainment industry groups such as the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) have often been diametrically opposed to the goals and objectives of hacktivists especially with regard to the access of digital media on the Internet. More recently, the Foreign Intelligence Surveillance Act (FISA) has also surfaced as relevant. The increasingly restrictive nature of laws governing intellectual property rights in tandem with laws enforcing national security, represent both moneyed opposition and perceived security threats to the freedom of online information.

E. Reaction of Big Corporations

In *How Public Relations Professionals are Managing the Potential for Sabotage, Rumors, and Misinformation Disseminated Via the Internet by Computer Hackers* (1997), Joseph Basso has addressed the corporate objective to mitigate negative public relations instigated by hackers on the Internet. Creating two-way communication channels to facilitate dialog with disgruntled consumers is probably the most important way to accomplish this. Basso uses a Systems Theory approach to the Internet which, "allows us to view public relations as an organizational linkage to the whole, facilitating communication both internally and externally" (Basso, 1997, p. 28). Basso has discovered that most public relation professionals employ a Web 1.0 approach to the Internet, meaning they view it more

as a one-way channel for disseminating information than as a two-way channel for engaging in communication. Furthermore, most of them are self-trained Internet users who do not appreciate the potential of hackers for sabotaging and misinforming the public about the performance of companies. This leaves them at a distinct disadvantage in terms of dealing with the online sabotage, misinformation, and rumors manufactured by hackers. Basso has suggested that public relations offices will need to evolve into more savvy users of the Internet if they want to survive in the ICT-dominated world of the future. "Public relations professionals must become more versed in electronic communication, recognize the two-way function of e-mail message dissemination, and carefully monitor and participate in the wired environment in order to maintain organizational credibility and communicate with constituent publics. In addition, public relations professionals must become more aware of the legal regulation of information via the Internet in order to monitor the potential for defamation" (Basso, 1997, p. 32).

Taking a much more sympathetic view of hackers, Nissenbaum's *Hacker's and the Contested Ontology of Cyberspace* (2004) lies at the other end of the spectrum from Basso. In her work, she has examined the ontological shift in perception that has seen the increasing demonization of hackers over the past thirty years, noting that simplistic models that suggest that both hackers and the public at large have merely "changed" does not take into account important shifting social contexts over time. Whereas early hackers were seen as slightly deviant, though lovable social curmudgeons who were obsessed with code and who delighted in high-tech pranks, present-day hackers are often depicted as malicious deviants who engage in criminal attacks on government and corporate websites. Nissenbaum and others attribute this new interpretation of hackers as one that serves the interests of

governments and corporations insofar as they are able to enforce "appropriate" Internet behavior on the Web, as well as justify the need for greater security and censorship of information. Like the depiction of the OWS movement and other non-mainstream groups of people, hackers are frequently associated with viruses, diseases, and social malaises that serve to rationalize the need for their control and regulation in the name of the greater good. "Cast as the 'bad guys' of computerized and computer-mediated social reality, they are sociopaths, thieves, opportunists, trespassers, vandals, peeping toms, and terrorists….To call a hacker good becomes virtually oxymoronic" (Nissenbaum, 2004, pp. 204 - 205).

The nature of riots, protests, and revolts ultimately represent paradigm shifts in the public consciousness and the established powers that be have no interest in allowing this to happen. This is another good reason to crackdown on hackers. Nissenbaum has concluded that:

> Hacking is now imbued with a normative meaning whose core refers to harmful and menacing acts, and as a result it is virtually impossible to speak of, let alone identify, the hackers that engage in activities of significant social value. Because the old hackers eschewed centralization of authority and invasive property boundaries, the ontological shift is convenient for those who seek to establish control in the new order and economy of cyberspace (2004, p. 213).

In this chapter, I have provided an overview of social theories at play in the online hacktivist community by examining how social theoreticians such as Manuel Castells, Joseph Basso, Helen Nissenbaum, Earl and Kimport, and Bennett and Segerberg have provided new, far-reaching theoretical insights into the study of hacktivism and global

political movements in the Digital Millennium. Through them, I have been able to achieve a broad overview of new trends in online social activism that contributes to a wider understanding of the strategic shifts in organizational principles of activists in a global network society. In the next chapter, I lay out a methodology for examining the arguments of the hacktivist movement using the lens of cognitive linguistics, critical discourse analysis, frame semantics, and metaphor theory.

IV. A Framework for Analysis

A clear understanding of the position of the hacktivist movement and the adversarial reactions to them by government and corporate authorities can benefit from a careful linguistic analysis of the communications produced by the relevant parties. In my work, the rhetorical and linguistic features of texts produced by hacktivists – along with their opposition by authorities, and their support by civil rights advocates – are essential to analyze in order to facilitate an understanding of the hacktivist movement and its wider social implications. In what follows, I lay out a framework that informs my approach to the linguistic analysis of the debate between hackers/hacktivists and government/corporations. Accordingly, I examine Cognitive Linguistics theory, Frame Semantics, and Critical Discourse Analysis (CDA) as tools for unpacking the construction of meaning arising from texts produced by and about hacktivists with a focus on linguistic framing and metaphor theory as a way to examine the ideologies that inform stances. It should be noted that my metaphor analysis has also included embedded metaphors because while hidden in nature, these covert metaphors nonetheless play a pivotal role in the linguistic framing of stances. I discuss how this methodology can help elucidate the political, ideological, and epistemological orientations of hacktivists and their detractors as each vies for social control of the digital symbolism of cyber space. Questions to bear in mind include: How do the linguistic framing practices of all parties reflect their conceptual and dialogic stances in public communications? In particular, how does the use of terminology and metaphor, as well as the rhetorical discourse posturing of stance, reveal assumptions and claims about the nature of issues at hand and their resolution?

A. Cognitive Linguistics and Frame Semantics

Cognitive Linguistics explores the relationship between language and thought. A fundamental tenet of Cognitive Linguistics is that because language expresses concepts, language and cognition overlap. Indeed, Cognitive Linguistics views language as *shaping* cognition because of its tendency to semantically categorize and associate concepts arising out of cognitive awareness and functioning. Due to its study of the relationship between linguistics and cognition, Cognitive Linguistics is fundamentally concerned with linguistic representations and the manner in which these representations influence human cognition (Lakoff, 1992), the latter drawing on other areas of study informing cognitive science including philosophy, psychology, artificial intelligence, and neuroscience (Evans & Green, 2006). Ideologically, Cognitive Linguistics is a reaction against the language-is-innate principle of Generative Grammar as well as the language-represents-truth idea of Truth-Conditional Semantics. Unlike Chomskian grammar, Cognitive Linguistics views syntax as learned rather than innate and adheres to Langacerk's slogan that "grammar is conceptualization." (Croft & Cruse, 2004). In this sense, it takes the view that syntax reflects semantics and that linguistic form and meaning are synonymous.

As mentioned before, one of the central tenets of Cognitive Linguistics is Frame Semantics. Charles Fillmore, who is considered the father of Frame Semantics, took classic grammar theory – or case grammar – and gave it a cognitive explanation. He described Frame Semantics as empirical semantics because it emphasizes "the continuities, rather than the discontinuities between language and experience" (2006, Geeraerts, ed.). Defining Frame Semantics as "any system of concepts related in such a way that to understand any

one of them you have to understand the whole structure in which it fits" (2006, p. 373), Fillmore has emphasized its use as a system encompassing the words, ideas, and understandings that are fundamentally relational and conceptual by nature (Fillmore, 1982, "Frame Semantics"). In other words, the denotative and connotative sense of vocabulary meaning constitutes the intricate system of interlocking concepts that make up a frame.

More narrowly, Frame Semantics is concerned with the organization and categorization of conceptual knowledge via the delineating relationship of domain/frames to profiles. This is largely a question of synecdoche, the relationship of the parts to the whole. For example, "*radius* profiles a particular line segment in the CIRCLE base/domain/frame" (Croft & Cruse, 2004, p. 15). In other words, the only way to understand the profiled concept of "radius" is by simultaneously evoking the domain concept of "circle". A radius is a part of a circle and can only be understood in this way, for without the concept of a circle first, a radius cannot make any sense. Ultimately, "the meaning of a linguistic unit must specify both the profile and its base" (2004, p. 15). Thus, an understanding of the organizing principles of domains and profiles – essentially, the synecdochic relationship of the part to the whole – serves as the basis for Frame Semantics.

Another important component of Frame Semantics is that of idealized cognitive models. Lakoff has defined idealized cognitive models as a species of frame (Croft & Cruse, 2004, p. 28). For example, a simple term like "bachelor" cannot account for the all the variety of social contexts to which this concept might apply. "The frame for BACHELOR represents an idealized version of the world that simply does not include all possible real-world situations" (p. 28). Much as Plato once theorized about idealized forms – the most common example being the perfect table – so too do idealized cognitive models suggest a perfect

reality. While this idealized reality does not exist, it nevertheless informs our ability to understand all the possible permutations of a concept. In this manner, idealized cognitive models are essentially kinds of idealized forms (or frames) in the Platonic sense of the word.

The fact that we need to bring encyclopedic knowledge to bear in order to understand even a single concept constitutes another important aspect of this line of thought. Since concepts evoke complex frames of association, even the simplest concept invites encyclopedic knowledge of all possible related frames and domains of understanding. "Once one begins to specify the conceptual structure of the frame that supports the concept profile for a word or linguistic expression, the semantic structure quickly expands to encompass the total (encyclopedic) knowledge that speakers have about the concept symbolized by the word or construction" (Croft & Cruse, 2004, p. 30).

Teun A. Van Dijk sees frames as epistemic by nature. In his paper entitled *Context and Cognition: Knowledge Frames and Speech Act Comprehension* (1977), Van Dijk begins with the premise that pragmatic theory is at once conceptual and empirical. In looking specifically at pragmatics and cognitive psychology, Van Dijk has stated that, "A cognitive theory of pragmatics has as one of its tasks to specify how we are able to perform and understand acts of language, and how we are able to act 'upon' such understanding as it is related to cognitive frames" (1977, p. 212). Van Dijk defines frames as organized conceptual systems and he asserts that speech acts are also a class of frames. Because frames serve as conceptual structures that guide the interpretation of social contexts – particularly with regard to those of an institutional nature – frames provide the theater for enacting pre-ordained speech acts that support the accomplishment of the social and cultural business at hand. A good example of a speech act in operation as a frame is, "I now

pronounce you man and wife." In making that speech act, an entire complex of frames, institutions, ideologies, beliefs, and values are evoked for the participants in order to enact the social contract of marriage.

The observation that speech acts occur as a matter of course in the function of institutions, policies, and their allied discourse patterns is perhaps best illustrated in that classic theatrical stage for meting out justice; the courtroom. A judge who pounds the gavel and declares, "You are hereby sentenced to life without parole" is making a speech act that draws upon a web of institutions and ideologies that implicate the social and cultural value of crime and punishment for the participants. Judgments, edicts, and eulogies are by their nature speech acts that serve as linguistic framing devices in discourse recognized as social contracts carried out in institutional settings.

B. Critical Discourse Analysis

The linguistic frames responsible for shaping and presenting ideology are areas of study for Critical Discourse Analysis (CDA). In *Cognitive Linguistics in Critical Discourse Analysis* (2007), editors Christopher Hart and Dominik Lukes sum up the development of CDA as something that "can be traced at least as far back as the Aristotelian study of rhetoric" (2007, Introduction, p. ix). They elaborate on the historical reach of CDA by noting, "In contemporary philosophy, the Marxist-influenced Critical Theory of the Frankfurt school, in particular that of Adorno and Horkheimer, later followed by Habermas, and Foucault's post-structuralist discourse analysis, should also be considered critical discourse analysis" (2007, Introduction, p. ix). Other early theoreticians in the emergence of Critical Linguistics and Critical Discourse Analysis include Chomsky for his idea of

Transformational Grammar, and Halliday for his theory of Systemic Functional Linguistics. In the field of CDA proper, Fairclough, Wodak, and Van Dijk are considered some of the primary theoreticians for the discipline. Unlike the descriptive and positivistic approach to language of Sociolinguistics, CDA is more concerned with a pragmatic analysis of language in operation as speech acts, debates, and ideological disputes over politics and power. Ultimately, CDA is about the deployment of power in civic discourse. When looked at in terms of its use for the framing of rhetorical stances, CDA is helpful for examining the persuasive aspects of the linguistic framing of the debate between ideological opponents.

In his classic work, *Language and Power* (2001), Fairclough provides an understanding of how language is situated in power and ideology. He has averred, "The gist of my position is that language connects with the social through being the primary domain of ideology, and through being both a site of, and a stake in, struggles for power" (2001, p. 15). Fairclough's position has much in common with Castells's view that state power can be deployed persuasively through appeals to logic and emotion. In *Cognitive Linguistics and Critical Discourse Analysis,* Dabrowska and Divjak describe discourse as existing in "dialectic with social situations and relations, both reflecting and reinforcing social structures" (2015, p. 1). They further state that, "The principle aim of CDA is to bring to the surface for inspection the otherwise clandestine ideological properties of text and talk and in so doing to correct a widespread underestimation of the influence of language in shaping thought and action" (2015, p. 2). Frames create the meta-narratives necessary for the maintenance of political ideology and thus point directly to the exercise of social power in political life. This theme will be addressed again as I begin to analyze the political rhetoric of hacktivists, their detractors, and civil rights mediators in the chapter that follows.

C. Linguistic Framing and Conceptual Metaphors

Linguistic framing as posited by Lakoff (2004) provides unity for an understanding of Cognitive Linguistics, Frame Semantics, and Critical Discourse Analysis, but it requires looking more carefully at how certain linguistic phenomena such as metaphor underlie the discursive practices of hacktivists and their opponents. Linguistic framing more generally, and the use of metaphors more specifically, comprise some of the more applicable ideas from Cognitive Linguistics that have facilitated my exploration of the political stances and epistemological attitudes of hacktivists and their opponents toward information.

Work in linguistic framing began with the study of institutions as social entities conducted by Ervin Goffman in 1974. In a presentation to the Commonwealth Club of California televised by FORA.tv, Lakoff (2008) has explained that "every institution is structured by a frame and has two parts: it is composed of roles and scenarios" (FORA.tv). He gives as an example the institution of a hospital which necessarily brings with it all the attendant concepts of its office: doctors, nurses, patients, operating rooms, ambulances, medicines, medical instruments, and so on. Since Charles Fillmore explains how words are always defined relative to frames, we can begin to understand that a frame elicits a complex association of words and concepts revolving around specific societal institutions.

"Linguistic framing is a deliberate strategic use of metaphor" that makes cognitive associations in our brains that become part of our neuro-circuitry through the association of emotions with knowledge gained through experience (2008, FORA.tv). Lakoff points to studies that reveal that, contrary to being an impediment to understanding, emotions and knowledge mutually reinforce one another by making the physical connections that become

part of the neurocircuitry of the brain. An example of this might be the metaphor of warmth associated with the notion of love and affection. Lakoff suggests that as a child is held in the arms of its mother, the child comes to associate the feeling of love with the physical warmth of the mother's body. A metaphoric connection is thus made between the sensation of warmth and the feeling of love and affection and Lakoff (1980) insists that our brains are actually hardwired for such primary metaphorical associations (*Metaphors we live by,* p. 255). Castells (2009) similarly discusses the role of emotions in creating political frames, asserting that, "fear-arousing situations attract the largest audience" (*Communication power,* p. 156). For this reason, political campaigns centered on the emotion of fear seem to have the greatest traction according to Castells.

Lakoff has likewise noted that, "metaphors and frames are thoroughly political" (2008). Frames are used in law and politics to debate ideas and stances. As mentioned previously, frames can occur as speech acts in institutional settings such as a court of law. In the institutional example of the courtroom, the gavel can be seen as a tool, the judge who wields it can be seen as the agent, and the oak-and-marble environs of the courtroom as the scene where this action is carried out. Words evoke frames and frames encompass the attitudes, values, and beliefs that accompany the stances associated with institutional and cultural narratives.

An example of a more obvious political instance of the use of frames and metaphors in action can be found in Lakoff's *Don't Think of an Elephant* (2004). In this work he has averred that, "people do not necessarily vote in their self-interest. They vote their identity" (2004, p. 19). He feels that this is one good reason progressives have failed to understand how to frame national debates more persuasively since they often view decisions as based

on rational choices rather than as decisions that stem from the adoption of complex interrelated frames that underlie political belief systems. Lakoff warns that until progressives begin framing the national debate to take into account the needs of their audience, they will continue to be unsuccessful at promoting liberal values.

In their discussion of the conceptual theory of metaphor, Croft and Cruse (2004) have maintained that Lakoff and Johnson's *Metaphors We Live By* (1980) is the definitive explanation of metaphors. "One of the most influential books to emerge from the cognitive linguistic tradition is Lakoff and Johnson's *Metaphors We Live By*" (2004, p. 194). They further explain, "Lakoff and his colleagues use evidence from everyday conventional linguistic expressions to infer the existence of metaphorical relations or mappings between conceptual domains … in the human mind" (2004, p. 194). They see the purpose of Lakoff's work as "to uncover these metaphorical mappings between domains and [to examine] how they have guided human reasoning and behavior" (2004, p. 194). According to Croft and Cruse, metaphors create circuit paths of meaning in the brain through descriptive associations that are reinforced over time. Metaphors and frames are fundamentally conceptual systems for organizing thoughts by explicitly inferring similarities between two or more distinct ideas and concepts. Like idealized cognitive models, conceptual metaphors can be thought of as a species of frames that categorize, organize and give coherence to our experiential reality. Croft and Cruse believe "that metaphor is the result of a special process for arriving at, or construing, a meaning" (2004, p. 194). Therefore, we can begin to appreciate how linguistic framing and Metaphor Theory share significant traits in common. Just as conceptual metaphors permit fruitful comparisons of our experiences across conceptual domains, so too does linguistic framing support our understanding of meaning

through the negotiation of associative networks of concepts. In short, metaphors may be thought of as linguistic framing devices for organizing conceptual domains.

In Lakoff and Johnson's magnum opus *Metaphors We Live By* (1980), they have provided a rigorous account of the systematicity of metaphors and their importance to human cognition. They believe that, "Our ordinary conceptual system, in terms of which we both think and act, is fundamentally metaphorical in nature" (1980, p. 3). They further clarify that "The same mechanisms of metaphorical thought used throughout poetry are present in our most common concepts: time, events, causation, emotion, ethics, and business, to name but a few" (1980, p. 244). In this regard, we can see that metaphors function to bridge the gap between the mental spaces or possible worlds associated with Frame Semantics and the tangible, prosaic world of real-life experiences. Lakoff and Johnson provide evidence for the functioning of conceptual metaphors in our thinking and reasoning processes and point out the basic nature of metaphors as a system of inference that maps one set of conceptual domains onto another. For example, knowledge drawn from the sensory domain typically gets mapped onto knowledge drawn from the reasoning domain. An instance of this can be found in the metaphor "hot water" to signify trouble because the sensation of intense heat is commonly associated with embroilment in social difficulties. Like Frame Semantics, metaphor is a conceptual system for organizing thoughts. Thus, Metaphor Theory can serve to link the idealized cognitive models discussed in Frame Semantics to the physical reality of quotidian experience. Lakoff and Johnson have dubbed this Experientialism (p. 226).

Dissatisfied with the western tradition for explaining meaning and understanding, Lakoff and Johnson have decried the fact that, "'[M]eaning' in these traditions has very

little to do with what people find *meaningful* in their lives" (1980, preface). For this reason, Lakoff and Johnson teamed up to write their treatise in order to offer a variant socio-epistemic explanation for human cognition and meaning-making. They point out that traditional explanations for truth, meaning, knowledge, and understanding, have been devoid of any significant attention to the important role of metaphor in philosophy and linguistics. The two have shared the idea that metaphor is "the key to giving an adequate account of understanding" (1980, preface) and that by challenging traditional assumptions of the role of metaphor in thought and meaning-making, they could revise "central assumptions in the Western philosophical tradition" in order to provide "an alternative account in which human experience and understanding rather than objective truth, played the central role" (1980, preface).

Accordingly, Lakoff and Johnson have laid out an examination of Metaphor Theory that challenges traditional assumptions of human cognition and reasoning ability. They dispute conventional ideas about language, cognition, and reasoning in order to conclude that "how we think metaphorically matters" (1980, p. 243). They believe that "the idea that metaphors can create realities goes against most traditional views of metaphors" (p. 145), and postulate that "it can determine questions of war and peace, economic policy, and legal decisions, as well as the mundane choices of everyday life" (p. 243). They argue that "metaphor has traditionally been viewed as a matter of mere language rather than primarily as a means of structuring our conceptual system and the kinds of everyday activities we perform" (p. 145). Indeed, they feel "the single biggest obstacle to understanding our findings has been the refusal to recognize the *conceptual* nature of metaphor" (p. 245).

Lakoff and Johnson have identified at least four major fallacies regarding metaphors that preclude a fundamental understanding of their importance in our conceptual systems. A significant one is the idea that metaphor is a figure of language and an embellishment of our thoughts, a belief that goes back to at least early Greek rhetoricians. They outline the fallacies surrounding metaphors thusly:

> The first fallacy is that metaphor is a matter of words, not concepts. The second is that metaphor is based on similarity. The third is that all concepts are literal and that none can be metaphorical. The fourth is that rational thought is in no way shaped by the nature of our brains and bodies (1980, p. 244).

In disputing these notions, Lakoff and Johnson demonstrate the systematicity of metaphor. "Because the metaphorical concept is systematic, the language we use to talk about that aspect of the concept is systematic" (1980, p. 7). The systematicity of metaphors is such that the selection of one concept necessarily precludes the selection of others: "a metaphorical concept can keep us from focusing on other aspects of the concept that are inconsistent with that metaphor" (1980, p. 10). Metaphorical systematicity means that correlated linguistic frames will or will not be realized depending on the specific metaphor chosen. Lakoff and Johnson elaborate on this point, observing that, "A far more subtle case of how a metaphorical concept can hide an aspect of our experience can be seen in what Michael Reddy has called the conduit metaphor" (1980, p. 10). This point will be returned to later on as I explore Reddy's notion of the significance of "dead" metaphors in the organization of our conceptual systems of communication.

Lakoff and Johnson have posited the idea that metaphors are structural by nature because they create cross-domain correlations "where one concept is metaphorically structured in terms of another" (1980, p. 14). For examples "time is money" structures a one-to-one conceptual correspondence between time and money. Two of the most important types of structural metaphors are orientational metaphors and ontological metaphors. While ontological metaphors tend to create one-to-one references between cross-domain concepts (e.g., "my love is like a red, red rose"), orientational metaphors "organize a whole system of concepts with respect to one another" (p. 14).

Ontological metaphors are "ways of viewing events, activities, emotions, ideas, etc., as entities and substances" by mapping cross-domain correspondences between disparate phenomena (1980, p. 25). Another example of an ontological metaphor is demonstrated in the idea of inflation. Though it is an abstract concept, we nevertheless talk about as though it were a physical entity due to the fact that ontological metaphors are ways of perceiving intangibles as tangibles, of concretizing non-corporeal reality. It is perhaps noteworthy that in describing such abstractions as mind, theory, or life, we do so as though they had actual material existence in our surrounding environments, often to the point of using our hands and bodies to enact, describe, and demonstrate them. Personification, reification, objectification, metonymy, and synecdoche are all classes of ontological metaphors that "allow us to make sense of phenomena in the world in human terms – terms that we can understand on the basis of our own motivations, goals, actions and characteristics" (1980, p. 34). For this reason, ontological metaphors allow us to talk about abstractions in a way that allows us to quantify and give coherence to our mental reality. As one example of this, a species of ontological metaphor called metonymy permits related concepts to substitute for

one another. When a waitress describes a customer as "the ham sandwich" in the sentence, "the *ham sandwich* is waiting for his check" (1980, p. 35), she is not referring to their perceived similarities so much as making an associative link between unlike objects to help give structural coherence to her mental world. Such cross-domain correlations are a function of perception, categorization, and association, but they are *not* about actual physical or conceptual similarities, a fact that too often gets forgotten. "[Metaphor] is typically based on cross-domain correlations…. which give rise to the *perceived* similarities between the two domains within the metaphor" (1980, p. 245 – emphasis added). The importance of this point will be discussed at greater length further on in a discussion on the significance of dead, hidden, or embedded metaphors.

The other important metaphor for our consideration is the spatial or orientational metaphor. Unlike ontological metaphors that map "one concept in terms of another," spatial metaphors map multiple concepts with respect to one another. Such metaphors "have to do with spatial orientation [like] up-down, in-out, front-back, on-off, deep-shallow, central-peripheral" (1980, p. 14). Spatial metaphors serve as the physical representation for embodied cognition and typically take the form of a preposition. An example of a spatial metaphor would be something along the lines of "he is feeling up today" where "up" corresponds to positive phenomena such as happiness. From this metaphor we get expressions like "Things are looking *up*" or "We hit a *peak* last year" (p. 16). Similarly the antonym "down" corresponds to negative phenomena such as sadness. For example, "He is feeling down" or "Things are at an all-time *low*" (p. 16). However, it bears reminding that metaphor is directly shaped by physical, social, and cultural contexts in the real world. Thus, spatialization metaphors "have their basis in our physical and cultural

experiences" (1980, p. 14). For this reason a western cultural tradition that associates upwardness with positivity is not necessarily the case in other cultures and some, in fact, may view it as the complete opposite.

Finally, the notion that thought occurs separately from our brains and bodies has been challenged throughout *Metaphors We Live By* in order to illustrate the importance of embodied cognition to the process of comprehension. The authors lay to rest the Cartesian duality dichotomizing the corporeal from the incorporeal (the objective from the subjective) that serves as the basis for modern ideas about human reasoning. Lakoff and Johnson critique the rationalist's epistemological orientation that views the acquisition of knowledge as acquired solely through reasoning as well as the empiricist's epistemological orientation that views the acquisition of knowledge as acquired solely through the senses (1980, p. 195). They contest the notion of an a priori, rationalist subjectivism that views truth as internal and dependent on meaning-making and an a posteriori, empiricist objectivism that views truth as external and independent of meaning-making. They buck both the rationalist and empiricist theory of knowledge for being either too subjective or too objective and dispute the idea that "truth is a matter of fitting words to the world," that "meaning is disembodied", and that emotion and imagination are suspect forms of meaning-making (pp. 191, 196).

Instead, they point out a third path they have dubbed Experientialism that navigates a middle ground between rationalism and empiricism. Because Experientialism views metaphors and conceptual gestalt systems as necessary to meaning-making, it synthesizes the seemingly insurmountable dichotomies posed by strict rationalism and strict empiricism to arrive at the conclusion that metaphor is in fact a function of Imaginative Rationality.

(1980, p. 193). The significance of Imaginative Rationality lies in its important role in helping us make sense of such abstractions as "feelings, aesthetics, morality and spirituality" (1980, p. 193). For example, in discussing the aesthetics of art, Lakoff and Johnson have noted that, "From the experientialist point of view, art is, in general, a matter of imaginative rationality and a means of creating new realities" (1980, p. 236). Experientialism has neither "the objectivist obsession with absolute truth or the subjectivist insistence that imagination is totally unrestricted" (1980, p. 228) and instead takes an epistemological orientation that views knowledge acquisition as the ability to reason about real-world sensory information through the use of cross-domain conceptual metaphors connected to the abstract world of thoughts and feelings. Kenneth Burke has described this as "the place where the dialectical realm of ideas is seen to permeate the positive realm of concepts" (*A Rhetoric of Motives*, 1963, p. 186). Indeed Burke, like Lakoff and Johnson, sees the poetic imagination and thus Imaginative Rationality, as a necessary precursor to scientific imagination. By all accounts, Lakoff and Johnson's Experientialism lays to rest the dualistic essentialism presented by the Cartesian split by hearkening back to the pre-enlightenment, scholastic notion of reading the world around us in an interpretive process of meaning-making that synthesizes mind, body, and spirit (Yates, 1966).

D. Paradigm Shift : Michael J. Reddy's Conduit Metaphor

We can see that metaphor theory is central to an understanding of linguistic framing, critical discourse analysis, and persuasive discourse overall. Metaphors may be thought of as the constituent elements of the linguistic framing devices that inform Critical Discourse Analysis. As previously mentioned, one of the metaphors that Lakoff and Johnson address

throughout their book is that of Michael J. Reddy's conduit metaphor. Lakoff and Johnson have acknowledged their debt to Reddy, stating:

> The contemporary theory that metaphor is primarily conceptual, conventional, and part of the ordinary system of thought and language can be traced to Michael Reddy's now classic essay [*The conduit metaphor: A case of frame conflict in our language about language*]. With a single, thoroughly analyzed example, he allowed us to see, albeit in a restricted domain, that ordinary everyday English is largely metaphorical, dispelling once and for all the traditional view that metaphor is primarily in the realm of poetic or 'figurative' language. Reddy showed, for a single, very significant case, that the locus of metaphor is thought, not language, that metaphor is a major and indispensable part of our ordinary, conventional way of conceptualizing the world, and that our everyday behavior reflects our metaphorical understanding of experience. Though other theorists had noticed some of these characteristics of metaphor, Reddy was the first to demonstrate them by rigorous linguistic analysis, stating generalizations over voluminous examples (Lakoff, 1992, p. 203).

Significantly, Lakoff and Johnson have analyzed Reddy's ideas to illustrate how fundamentally our metalanguage is structured by the conduit metaphor and its responsibility for producing the frame conflicts that give rise to misunderstandings and miscommunication. They distill the conduit metaphor in the following analysis:

> IDEAS (OR MEANINGS) ARE OBJECTS.
> LINGUISTIC EXPRESSIONS ARE CONTAINERS.

> COMMUNICATION IS SENDING.
>
> The speaker puts ideas (objects) into words (containers) and sends them (along a conduit) to a hearer who takes the idea/objects out of the word/containers. Reddy documents this with more than a hundred types of expressions in English, which he estimates account for at least 70 percent of the expressions we use for talking about language (1980, pp. 10, 11).

The relevance of this is that in trying to suggest that language *contains* meaning it "entails that meanings have an existence independent of people and contexts" (1980, p. 11). Lakoff and Johnson warn that the decontextualization of information that occurs with the conduit metaphor can have negative repercussions. This is illustrated in the example provided by Lakoff and Johnson below:

> "[T]here are cases where a single sentence will mean different things to different people. Consider:
>
> WE NEED NEW ALTERNATIVE SOURCES OF ENERGY.
>
> This means something very different to the president of Mobil Oil from what it means to the president of Friends of the Earth. The meaning is not right there in the sentence – it matters a lot who is saying or listening to the sentence and what his social and political attitudes are. The CONDUIT metaphor does not fit cases where context is required to determine whether the sentence has any meaning at all and, if so, what meaning it has" (1980, p. 12).

Though it might go without saying that communication requires more than the simple lexical decoding of words and sentences in order to permit genuine *understanding*, nevertheless Reddy's conduit metaphor suggests that social and political contexts are dismissed, ignored, or forgotten more often than not in any discussion of a social epistemology of meaning.

Another important entailment of the conduit metaphor is the idea that "more form is more content" (1980, p. 127). If we truly believe that words are containers for meaning, then it necessarily follows that just as we expect a container to limit the size of its contents, so too would we expect things like repetition and size (as with the phonological lengthening of words) to increase the *extent* of the meaning's significance. In rhetoric, this is a technique for creating presence – a polite way of describing the propaganda factor inherent in advertising through the sheer repetition or catchy rhythm of a slogan.

In studying our language about language – our metalangauge – Reddy claims that dead metaphors influence our referential frames of concepts so deeply that their prevalence in our metalanguage often goes entirely unrecognized. In his essay, *The Conduit Metaphor: A Case of Frame Conflict in our Language About Language* (1979), he points to the conduit metaphor as an example of a dead metaphor and exposes its hidden influence over our concepts of communication, meaning, and understanding.

He has observed, "if there are dead metaphors in [metalanguage] they all seem to involve the figurative assertion that language *transfers* human thoughts and feelings" (1979, p. 287). Reddy has dubbed the idea that language conveys thought "the conduit metaphor" and has provided an in-depth examination of how it gets addressed when communication breaks down. "I couldn't get my ideas across to him" or "She failed to get through to him"

are forms of metalangauge that suggest that when language fails to physically transmit thoughts to a recipient, it constitutes a failure of communication. The idea that words are containers for meaning, thoughts, and feelings is the gist of the conduit metaphor because it entails the physical transference of thoughts and emotions from one person to another via words from which the recipient extracts the meaning. Unfortunately the conduit metaphor tends to hide the cooperative aspects of communication and obfuscates the fact that language does not literally send thoughts from one mind to another. Again, Lakoff and Johnson's cautionary explanation about the misconceptions surrounding metaphors points up the fact that metaphors are NOT based on actual similarities between disparate phenomena and that their purpose is only as representational symbols for the facilitation of understanding. The embedded nature of "dead metaphors" (what Lakoff and Johnson call hidden metaphors) is important to my analysis of linguistic frames since these metaphors go largely unrecognized while nonetheless wielding tremendous influence over debates on freedom of information. I will come back to this point later as I delve into my thematic analyses to expose some of the embedded metaphors in each side's arguments concerning access to the Net.

Reddy suggests a thought experiment in order to point out problems with the conduit metaphor and to suggest an alternative he calls the toolmakers paradigm (1979, p. 292). The toolmakers paradigms suggests that rather than language transferring thoughts and feelings from one mind to the next, in fact, "language seems […] to help one person to construct out of his own stock of mental stuff something like a replica, or copy, of someone else's thoughts – replica which can be more or less accurate, depending on many factors" (1979, p. 287). While the conduit metaphor suggests a simple one-to-one physical transference of thoughts and ideas via words between individuals, the thought experiment

posed by the toolmakers paradigm suggests that people living in disparate environments with very different materials at their disposal must communicate their toolmaking methodologies to one another via a machine that transmits written instructions across a barrier. The conduit metaphor objectifies meaning by implying that it is contained in words easily transferred from one person to the next, while the toolmakers paradigm *subjectifies* it by implying it is worked out with great difficulty by people working in radically different environments under radically different conditions.

Hence, the toolmakers paradigm posits a radical subjectivity in which each individual lives in a walled-off compound with vastly different environments and resources to use in the construction of the tools necessary for survival. The wall between each compound prevents any other form of communication than written messages conveyed between individuals. Successful communication entails solitary yet nevertheless *cooperative* efforts to decode meaning in order to understand the messages sent between the walls of the compound. For example, one person may live in an environment that has a great many trees and so learns to make a rake out of wood, which he finds useful for raking leaves. He may send instructions to the person in the compound next to him about how to make a rake but the recipient happens to live in an environment that is very stony and so is puzzled by the purpose of a rake. Eventually the recipient makes something similar to the rake but uses it instead as a pick for digging up rocks, something he finds more useful in his particular environment. As each individual tries to help the other fashion the tools they have found useful for their respective environments, each must struggle to understand and reconstruct their messages in a way that makes sense within their surroundings (1979, p. 292). Such is the radical subjectivity of the toolmakers paradigm in contrast to radical objectivity of the

conduit metaphor.

Lakoff and Johnson mull over the political and social implications of the conduit metaphor observing that,

> Communication theories based on the CONDUIT metaphor turn from the pathetic to the evil when they are applied indiscriminately on a large scale, say, in government surveillance or computerized files. There, what is most crucial for real understanding is almost never included, and it is assumed that the words in the file have meaning in themselves – disembodied, objective, understandable meaning. When a society lives by the CONDUIT metaphor on a large scale, misunderstandings, persecution, and much worse are the likely products (1980, p. 232).

In this regard, Reddy's conduit metaphor gives pause for second thought since it directly implicates government whistleblowers such as Snowden, Manning, and Assange and throws into sharp relief the overarching metaphor of the Internet itself as a *conduit* for communication. This is evinced by the state's desire to control the Internet in order to regulate the flow of certain kinds of information for ostensible purposes of national security and public safety. It goes without saying that the state's wish to regulate and control information is directly at odds with the hacktivists' metaphoric stance that information is a human right, censorship impedes communication, and online personal privacy should be guaranteed for all. In examining the conduit metaphor, we can begin to see that the nature of the conflict between hackers/hacktivists and government/corporations comes down to a question of linguistic framing via metaphors to determine who gets to define the legitimate form, meaning, and function of the Internet. "As Charlotte Linde (in conversation) has

observed, whether in national politics or in everyday interaction, people in power get to impose their metaphors" (1980, p. 157).

E. Metaphors in Action

Take for example one of the fundamental precepts of the hacktivist community: *information wants to be free*. This phrase was originally attributed to Stewart Brand, one of the early developers of the Internet, who uttered it during the first Hackers Conference in 1984 when making a neutral observation about the economic value of information to his colleague, Steve Wozniak (Wikipedia, n.d., "Information wants to be free"). But the other part of Brand's quote included the idea of the polarization of opposing economic forces: "Information also wants to be expensive. That tension will not go away." Only the first half of Brand's quote got adopted by hackers, hacktivists, and cypherpunks, those early software programmers and computer-code writers who also helped forge the Internet. These early hackers initiated the free and open source software (F/OSS) movement that later evolved into the idea of computer code as protected speech. Brand's quote would morph from its original value-free meaning to eventually become a cherished tenet of the hacker ethic dedicated to free speech and open access to the Net. Historian Adrian Johns points out that the perspective that information wants to be free is not a unique idea since it was also held dear by earlier developers of the Web such as Norbert Wiener, Michael Polanyi and Arnold Plant. Like later hacker and hacktivists, these individuals similarly advocated for open access to information (Wikipedia, n.d., "Information"). This hacker ethic is discussed at length in Gabriella Coleman's *Coding Freedom: The Ethics and Aesthetics of Hacking* (2013).

This idea of the free exchange of information pervades just about every aspect of the hacktivist movement and is a notable theme in John Perry Barlow's "A Declaration of the Independence of Cyberspace" (1996). Barlow made his declaration in response to the Telecommunications Act of 1996, a measure to deregulate the burgeoning telecommunications industry in order to permit the ownership of multiple media forms by a single company or individual, something that had been forbidden as an unfair monopoly in the past. With much metaphoric fanfare, John Perry Barlow had this to say about the implications of greater government and corporate control of the World Wide Web:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. ….
>
> We are creating a world where anyone anywhere may express his or her beliefs no matter how singular, without fear of being coerced into silence or conformity. …
> Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are based on matter. There is no matter here. …
> Your increasingly obsolete information industries would perpetuate themselves by proposing laws, in America and elsewhere, that claim to own speech itself throughout the world. These laws would declare ideas to be another industrial product, no more noble than pig iron. In our world, whatever the human mind may

> create can be reproduced and distributed infinitely at no cost. The global conveyance of thought no longer requires your factories to accomplish. ….
>
> These increasingly hostile and colonial measures place us in the same position as those previous lovers of freedom and self-determination who had to reject the authorities of distant, uninformed powers. We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts. ….
>
> We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before (Barlow, 1996, pp. 27 – 30).

While a bit florid, nevertheless I believe Barlow's metaphoric-rich declaration captures the essence of the hacker attitude toward government and corporate control of the Internet. The Telecommunications Act of 1996 and The Copyright Terms Extension Act of 1998 were measures to proprietize and monetize information through the enhanced protection of corporate interests on the Web by ensuring their established intellectual property rights through stricter enforcement of copyright laws. Given the desire of government and corporate interests to rein in and commercialize the proliferation of information on the Internet, it is little wonder that Barlow's manifesto is fundamentally a call for freedom of expression on the Net.

However, another ostensible reason for the control and regulation of information on the Internet is that of the metaphor of *national security*. National security is the metaphor increasingly used by government and corporate interests in support of laws and policies to control the channels of information in cyberspace. When Chelsea Manning exposed the Pentagon's war policies in the Middle East in 2010, releasing sensitive videos and documents to WikiLeaks (including the now infamous Collateral Murder video), the U.S. government promptly arrested her. According to Reporters Without Borders, she has been seen ever since as a prime example of the vulnerability of whistleblowers in the United States (Wikipedia, n.d., "Bradley Manning").

The fact that WikiLeaks has been at the epicenter of all five alleged security breaches in the past decade is testament to the power of the Internet to rapidly disseminate information to the world by transcending national borders in the blink of the eye. Assange, Manning, and Snowden have been catapulted onto the international stage for their revelations of government and military improprieties much to the chagrin of U.S. Pentagon and government authorities. Like Daniel Ellsberg before them, these three individuals have risked their lives in order to make available secret government and military documents held by U.S. officials. As a result of their digital activism, they are wanted by the U.S. government. Attempts to bring Assange and Snowden to the United States to face trial for violations of the espionage act have so far failed since the international community has stubbornly resisted U.S. pressures to extradite them.

The metaphor of national security can be seen in the following press release from Jane Holl Lute of the Department of Homeland Security (DHS) concerning the roles and responsibilities of the DHS in maintaining cybersecurity in America.

I can think of no more urgent and important topic in today's interconnected world than cybersecurity, and I appreciate the opportunity to explain the Department's mission in this space and how we continue to improve cybersecurity for the American people as well as work to safeguard the nation's critical infrastructure and protect the Federal Government's networks...

The United States confronts a dangerous combination of known and unknown vulnerabilities in cyberspace and strong and rapidly expanding adversary capabilities. Cyber crime has also increased significantly over the last decade. Sensitive information is routinely stolen from both government and private sector networks, undermining the integrity of the data contained within these systems. We currently see malicious cyber activity from foreign nations engaged in espionage and information warfare, terrorists, organized crime, and insiders. Their methods range from distributed denial of service (DDoS) attacks and social engineering to viruses and other malware introduced through thumb drives, supply chain exploitation, and leveraging trusted insiders' access.

We have seen motivations for attacks vary from espionage by foreign intelligence services to criminals seeking financial gain and hackers who may seek bragging rights in the hacker community. Industrial control systems are also targeted by a variety of malicious actors who are usually intent on damaging equipment and facilities or stealing data. Foreign actors are also targeting intellectual property with the goal of stealing trade secrets or other sensitive corporate data from U.S. companies in order to gain an unfair competitive advantage in the global market.

> In addition to these sophisticated attacks and intrusions, we also face a range of traditional crimes that are now perpetrated through cyber networks. These include child pornography and exploitation, as well as banking and financial fraud, all of which pose severe economic and human consequences. For example, in March 2012, the U.S. Secret Service (USSS) worked with U.S. Immigration and Customs Enforcement (ICE) to arrest nearly 20 individuals in its "Operation Open Market," which seeks to combat transnational organized crime, including the buying and selling of stolen personal and financial information through online forums. As Americans become more reliant on modern technology, we also become more vulnerable to cyber exploits such as corporate security breaches, social media fraud, and spear phishing, which targets employees through emails that appear to be from colleagues within their own organizations, allowing cyber criminals to steal information (Website of the Department of Homeland Security. Accessed Oct. 13, 2014).

Typical of the bloodless language of bureaucrats, this DHS press release makes frequent use of the metaphor of security to legitimize a broad spectrum of policies for the regulation of information on the World Wide Web. "Sensitive information is routinely stolen from both government and private sector networks, undermining the integrity of the data contained within these systems," declares Lute. She has talked at great length about the perceived vulnerabilities of U.S. government and corporate computer systems in cyberspace, and paints them as at the mercy of "foreign agents of espionage" bent on "information warfare" and "social engineering." She describes hackers as being motivated in their attacks for their "bragging rights in the hacker community," a reduction of those

who might presumably be adults to the status of errant children and all around miscreants. This reinforces her paternalistic attitude toward Netizens.

Perhaps one of the more noteworthy arguments Lute has made is when she conflates child pornography with banking fraud. She attests that both "pose severe economic and human consequences" though it might be pointed out that the sexual exploitation of a child is a particularly heinous crime many would see as sadistically distinct from robbing a bank. In fact, the most noteworthy crime the press release addresses over and over again is the idea of the theft of intellectual property by the hands of hackers and "foreign agents of espionage." While she does make allusions to domestic welfare now and again – she mentions hackers who targeted "natural gas and pipeline companies" or those "adversaries [who] are seeking to sabotage our power grid, our financial institutions, and our air traffic control systems" – nevertheless, the DHS's overriding concern with protecting banking interest and industry trade secrets is suggestive of a much more pecuniary motive for government regulation than the protection of the public good.

These two conflicting metaphors – the freeing of information versus the securing of information – are prime examples of the ontological nature of metaphors that give rise to ideological stances. Recall that ontological metaphors are "ways of viewing events, activities, emotions, ideas, etc., as entities and substances" (1980, p. 25). The metaphors for a social epistemology of information used by hackers/hacktivists and government/corporations are grounded in the idea that human characteristics and values can be found in non-corporeal concepts. "[Personification] allows us to comprehend a wide variety of experiences with nonhuman entities in terms of human motivations,

characteristics, and activities" (1980, p. 33). A few more examples of personification in ontological metaphors are:

> His *theory explained* to me the behavior of chickens raised in factories.
>
> This *fact argues* against the standard theories.
>
> *Life has cheated* me.
>
> *Inflation is eating up* our profits.
>
> His *religion tells* him that he cannot drink fine French wines.
>
> The *Michelson-Morley experiment gave birth to* a new physical theory.
>
> *Cancer* finally *caught up with* him. (Lakoff & Johnson, 1980, p. 33).

Similarly, hacktivists and governments and corporations create the personification and objectification of information when they say things like "*information wants to be free*" or "*information should be guarded for the sake of national security.*" The attributing of human motivations and values to the concept "information" would lead us believe that information desires freedom or that it needs to be safeguarded, two modalities that directly implicate the ideological stances of the disputants making the claims. To all accounts, each side must provide a rational basis for their arguments appealing to the epistemological dispositions of the general public.

The personification of information is understandable insofar as it can be difficult to separate human concepts from human intentions. Likewise, the objectification of information is understandable in terms of the value we often place on abstract ideas and concepts. But while the reification of an abstraction provides a convenient shorthand mode for conceptualizing ideas, it also invests it with physical properties that may or may not be

true. Anthropomorphizing or commodifying ideas can lead to a logical fallacy that perceives such reifications as though they were real objects in the real world. That is to say, the idea that information is a security risk that should be safeguarded is a perception that does not take into account the shared nature of thoughts and ideas. Indeed, the proprietarization and commodification of information problematizes the communal nature of thoughts and ideas. We might ask ourselves: Can information be bartered, protected or secured? Can it be sold, rationed, or liberated? Can it be manufactured, monetized, or exploited? The fact that we frequently talk about information in these terms directly implicates the far-reaching socio-political ramifications of linguistic framing through metaphors. To no small extent, the future of the Internet will be determined by the epistemological orientation toward the social construction of knowledge expressed through the metaphors of the antagonists in this debate.

In the next chapter, I provide a fine-grained analysis of a particular instance of hacktivism that resulted in the persecution of Internet prodigy Aaron Swartz.

V. Social Epistemology in Cyberspace

The tension over conflicting interpretations of the form, meaning, and function of the Internet is essentially a struggle over competing metaphors for quantifying it. Lakoff and Johnson have shown how metaphors play an important role in linguistic framing through the mental organization of key concepts that facilitate easy cross-referencing of ideas. Because metaphors analogize related ideas, they provide a system for indexing thoughts that supports the building of encyclopedic knowledge. For this reason, metaphors not only play a fundamental role in human cognition and knowledge building, they also reflect the values, attitudes, and intentions of antagonists struggling to define the purpose of the Internet.

In the thematic analysis that follows, I examine six texts in order to elucidate the metaphors employed by the disputants reflective of their respective stances over freedom of information on the Net. As I delve into my analysis, questions to keep in mind include: How has the Internet as a medium of publication and communication changed the notion of intellectual property rights and basic precepts about materials available for fair use in the public domain? How have laws enacted by government and corporations to combat hacktivists further restricted the free exchange of information so important to the open access and free culture movements?

While Teun A. Van Dijk and other linguists have long posited that frames are epistemic by nature, Lakoff and Johnson (1980) have expanded that notion to also include metaphors. For this reason, metaphors and linguistic frames are a species of heuristics that signify the epistemological stance of hacktivists and their opponents toward online freedom of information. Conflicts arise because the epistemological attitude toward knowledge favored by hacktivists is at odds with government and corporate interests for the control and

commercialization of it. On a broader scale, narrative is another important feature of the debate since texts are constructed with the frames and metaphors that support the narratives of the disputants. The significance of linguistic frames lies in their structuring of the meta-narratives necessary for the maintenance of political ideology. In turn, metaphors impart frames with important attitudes and perspectives that provide clues to the intentions of the antagonists concerning the social epistemology of the Internet.

Grand narratives captivate their audiences. Philip Eubanks has stated that "Postmodernists argue that the very prevalence of some narratives makes them largely invisible and, at the same time, inescapably intermingled with institutions, practices, and texts" (2004, p. 33). One of the unexamined narratives of the U.S. justice system as exemplified by the case of Aaron Swartz is its creation of what some psychologists have dubbed Legal Abuse Syndrome. Legal Abuse Syndrome is a form of post-traumatic stress disorder (PTSD) stemming from fraud and ethical misconduct in a court of law. As his case wore on, Swartz became increasingly depressed and this was to become a source of contention between Swartz's lawyers and federal prosecutor Stephen Heymann. When Swartz's initial lawyer, Andrew Good, tried to appeal to Heymann about the suicide-inducing affects the prosecution was having on the young Internet prodigy, Heymann was dismissive (Cullen, 2013). By the end, Swartz was reading Franz Kafka's *The Trial* and finding many similarities between the situation of the principle character, Josef K., and his own (Peters, 2016).

Swartz's short life is a classic narrative of David versus Goliath, of a boy-genius standing up to an institutional behemoth in order to speak truth to power. It is the story of a whiz kid who inadvertently takes on the U.S. Department of Justice (DOJ) in a fight for free

culture and open access to the Internet. The story has a hero, a villain, and a tragic ending and it centers on the hacker precept that information is a human right. The fact that this precept has become the ideological battleground over the struggle to define information policy on the Internet is clearly demonstrated in the case of Aaron Swartz.

For this reason, his narrative is intertwined with other contemporary champions of cyberspace freedom, including Chelsea Manning, Edward Snowden, Barrett Brown, Jeremy Hammond, and Julian Assange (who has referenced one of Swartz's articles, *Squaring the Triangle,* in his own book, *When Google Met WikiLeaks*). In the past seven years all of them have challenged the U.S. government's information policies as each has fought for freedom of speech and preservation of the knowledge commons on the World Wide Web. All of them have been free data activists and whistleblowers of one stripe or another who have questioned the government's control of national security information, as well as its privatization of public domain materials. Their cases must be examined within the context of the global mass movements of 2011 and the larger socio-historical currents of the Information Age. It is no doubt significant that Swartz committed his alleged theft of intellectual property the year of worldwide social justice uprisings that were facilitated by new information and communication technologies (ICT) in conjunction with new forms of social media. From the Arab Spring in the Middle East, to the Indignados in Spain, and the Occupy Wall Street Movement in the United States, all these social movements engaged hackers and hacktivists in maintaining the flow of online information to a wider global audience. The possibility that Swartz was a government target due to his hacktivism has been addressed by his friends and family who have continued to defend him from his detractors to this day. In an article appearing in the *New Yorker* a few months after his

suicide, Aaron's first girlfriend, Quinn Norton, wrote:

> If you look at 2011 to the present, there's an incredible emotional rollercoaster about Internet freedom and the Arab revolutions. The Internet was going to change everything, and at the end of 2011 you had Occupy. And then everything just got destroyed. 2012 was the year, globally, for the heightening of censorship and the heightening of surveillance, and then Aaron killed himself. Aaron was so much the Internet's boy, and that so much exemplified this machine crushing our hopes (Macfarquhar, 2013).

There can be little doubt that the worldwide populist uprisings of 2011 greatly alarmed the U.S. government. This is evinced by the State Department's reaction to Cablegate and the severity of the Department of Homeland Security's (DHS) crackdown on the Occupy Wall Street movement as the government took a hardline stance toward the social justice movements of 2011. The reaction of the government may have been due to the surprising interconnectedness of these movements, but what seems more probable is that it was because of the unexpected role of the Internet and social media as tools for mobilizing them.

Indeed, Swartz was able to effectively maintain the momentum of the Occupy Wall Street movement when he dovetailed it with his campaign to defeat the Stop Online Piracy Act (SOPA) and the Protect IP Act (PIPA). These measures were introduced in the legislature to grant lawmakers broad power to shut down websites accused of intermediary copyright infringement on the Net. While ensuring the commercial profit of intellectual property holders, the laws also disproportionality punished file-sharing sites by taking them offline whenever their clients exchanged copyrighted materials with one another. In support

of the mass protest culminating in the worldwide slow-down of the Internet, Swartz and his fellow hacktivists set up an electronic petition at Demand Progress that called on protesters to support freedom of information and open access to the Internet. On January 18, 2012, Swartz and other hackers, hacktivists, and free media advocates initiated Internet Blackout Day in which popular websites such as Wikipedia, WordPress, Twitter, Reddit, Boing Boing, and Craigslist shut down in protest of the proposed anti-piracy legislation. Many more popular websites went black that day in a show of solidarity with hacktivists. This cowed lawmakers and the measures were withdrawn.

Swartz was triumphant but there is significant evidence that his victory may have contributed to the government's decision to double-down on its efforts to prosecute him. Certainly many of his friends and family believed this to be so. In a post appearing on her Tumblr blog shortly after his death, Swartz's girlfriend, Taren Stinebrickner-Kauffman, averred, "The DOJ has told Congressional investigators that Aaron's prosecution was motivated by his political views on copyright. […] Many people speculated throughout the whole ordeal that this was a political prosecution, motivated by anything/everything from Aaron's effective campaigning against SOPA to his run-ins with the FBI over the PACER database" (Stinebrickner-Kauffman, Feb. 26, 2013).

Whether or not he meant to, Swartz has ended up a martyr for the hacker principles of free culture and open access on the Internet.

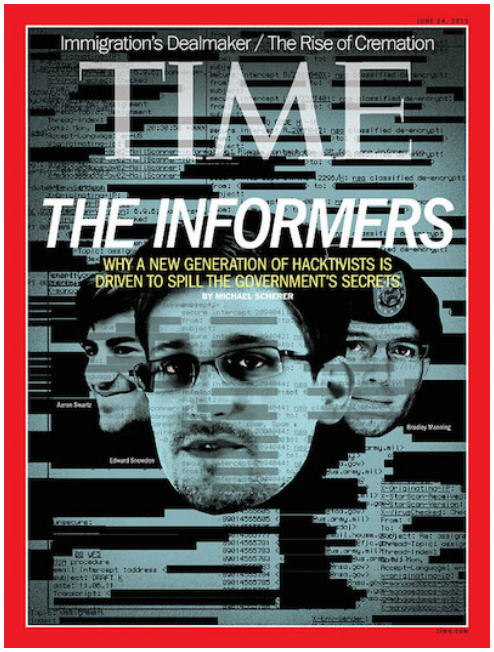

Figure 7. A Time Cover Story of Data Activists

What follows is a selective thematic analysis of six cited texts that create a narrative account of the life and times of Aaron Swartz, and the debate over freedom of information on the World Wide Web. Each analysis begins with an overview of the text's background followed by an introductory look at their main arguments that situates them in a dialog with one another. A contrastive analysis of the hacktivists, government, corporations, and social justice activists involved in the debate will further elucidate the thematic elements arising from the texts. My analysis examines the key discussion points of each text for their use of linguistic framing that reveal how the epistemological stances of the protagonists are represented through metaphor.

The texts follow in roughly chronological order starting with Swartz's *Guerilla Open Access Manifesto* in 2008 and moving next to his FBI files from the PACER case. The

MIT's special investigation into its handling of Swartz's case continues my analyses followed by the DOJ's public statement on his suicide in its press release. Next, an examination of the memorials installed by Anonymous on the MIT and the United States Sentencing Commission (USSC) websites are followed by a study of the legislation to reform the Computer Fraud and Abuse Act used to prosecute Swartz.

Some of the important embedded metaphors under consideration include hacker principles of transparency, free speech, and the preservation of the knowledge commons on the Web. This stands in marked contrast to the embedded metaphors of secrecy, restrictedness, and commercialization of the knowledge commons by authorities.

A. Guerilla Open Access Manifesto

Although he is known for being a gifted and talented computer programmer, Swartz was also a bibliophile who thought of himself first and foremost as a writer. In one of his essays from *The Boy Who Could Change the World* (2015), Aaron declares, "I don't want to be a programmer. …Perhaps, I fear, this decision deprives society of one great programmer in favor of one mediocre writer. Even so, I would make it. The writing is too important, the programming too unenjoyable" (p. 125).

A prolific blogger on his personal webpage, one of Swartz's most well-known posts is a piece entitled *Guerilla Open Access Manifesto.* This is the subject of my first thematic analysis. Written in 2008 while he was attending a conference of librarians in Eremo, Italy, there is evidence that he may have written it in collaboration with others who did not wish to have their names associated with it due to fears for their professional careers (Swartz, 2015). Though there is a good chance that Swartz's former girlfriend, Quinn Norton, also

participated in writing the manifesto, nevertheless she recommended it to prosecutors when they pressured her to give them something to use against him. Once they had it, prosecutors saw it as clear evidence of his intention to violate copyright law by copying and uploading academic texts to the Internet.

From his computer abilities to his writing abilities, from his hacktivism to his social theorizing, there is little doubt that Swartz was a multi-faceted wunderkind who by age fourteen had already received accolades from Internet digerati. In *Communication Power* (2011), Castells has identified the struggle for power as one that necessarily arises out of institutions and individuals engaged in communications that are socio-political by nature. As was already discussed in chapter three, Castells sees the power of the government as at once coercive and discursive. Governments around the world expend great energy in the discursive realm of persuasion in order to get their point across, appealing to and manipulating the ideas and values of their citizenry in order to convince them of the legitimacy of their laws and policies. Discursive measures are far less risky to deploy than coercive ones since the latter requires greater mobilization of forces, a situation which is always functionally unstable.

In the discursive realm, Castells also talks about the power of the programmers and the switchers in a network society. Swartz was one of those rare individuals who was both. According to Castells, "networks are communicative structures" that are created to fulfill certain goals and objectives by their programmers. Programmers are individuals who build the networks, and the Internet itself is one of their greatest accomplishments. Switchers, on the other hand, are those individuals who coordinate different sets of networks together. Examples of interconnected networks in society include financial, business, political, and

communication networks (Castells, 2011). The fact that Swartz was both a network programmer *and* a network switcher in the realm of politics and communications rendered him a particularly powerful individual on the World Wide Web.

As already mentioned, there is significant evidence that the DOJ prosecuted Swartz for his hacktivism. The following article on the congressional investigation into the DOJ's handling of his prosecution appeared on the Electronic Frontier Foundation (EFF) website. It reports, "At the briefing, prosecutors admitted that Aaron's political speech, specifically his *Guerilla Open Access Manifesto,* a document collaboratively written years before his alleged crime, was a main motivator in pursuing a case against Aaron. Of course, prosecuting someone, or prosecuting them more severely, because of their speech should raise red flags for Congress" (Higgins, Mar. 7, 2013). Significantly, when Anonymous shut down MIT's website and installed a memorial to Swartz in its place, they featured the entirety of his manifesto.

In one of the few books written about the life of the young hacktivist, *The Idealist,* (2016) Justin Peters has characterized Swartz's choice of title for his manifesto as unfortunate. According to Peters, "*Manifesto* connotes instability and political upheaval, the rise of people with nothing to lose but their chains; *guerilla,* for its part, brings to mind barbate insurgents in berets, toting Kalashnikovs through some fetid jungle. The title certainly suggested that Swartz stood for anything but peaceful, law-abiding resistance" (2016, p. 180). Whatever Peters' misgivings, it is clear that Swartz's manifesto functions as a powerful statement of his principles based on his belief that information is a human right. His manifesto is a testament to the hacker ethic of information freedom on the Internet and a clarion call to action for its liberation. As such, it identifies a problem – restrictions on

knowledge on the Internet – and proposes a solution – freeing knowledge so that everyone can share it.

Lawrence Lessig was the Harvard law professor and director of the Edmond J. Safra Center for Ethics where Swartz was on internship at the time he was arrested by MIT and federal secret service agents. As previously mentioned, Lessig (2004) has contended that the struggle to define legal notions of property and piracy on the Internet is having unforeseen and far reaching consequences for the sharing of human culture. The travails of the open access movement is one Lessig attributes to the problem of "eras[ing] the divide" between commercial and non-commercial intellectual and creative property (2004, p. 8). For this reason, Lessig has been critical of the Recording Industry Association of America (RIAA), the Motion Picture Association of America (MPAA), and Elsevier publishers among other corporations for their role in the growing proprietization of knowledge and culture.

In the Digital Millennium, copyright violations pose a significant problem for big media giants due to the ease of duplicability of digital files on the Net. Lessig has argued that, "the internet [is] a distributed digital network where every use of copyrighted work produces a copy" (2004, p. 145). The file sharing networks that host peer-to-peer file sharing have become a particular sore point for giant media firms and international trade associations. When Napster launched MP3, a new peer-to-peer file sharing technology to allow its subscribers to easily share music over the Internet, it was promptly sued by the RIAA for copyright infringement. Napster made modifications to its program to block copyrighted music from its site with 99.4% accuracy, but the judge in the case ruled that it was still insufficient. This prompted Lessig to declare, "If 99.4 percent is not good enough, then this is a war on file-sharing technologies, not a war on copyright infringement….Zero tolerance

means zero P2P" (p. 74).

Yet the digital circulation of electronic copies is the essence of the Internet's vital processes. There is no doubt that the perpetually replicating nature of file transfer protocols (FTP) is a function of the very form and function of the Internet. Like blood flowing in the body's arteries, FTP ensures the constant stream of digitized duplicates around the Net rendering their control and regulation extremely problematic. Internet security expert Bruce Schneier has noted, "trying to make digital files uncopyable is like trying to make water not wet" (Schneier, 2006).

But that is precisely what corporate copyright holders seek to do. In trying to extend their dominion over intellectual property rights on the Internet, they have introduced a host of legislation that strips the public domain of significant intellectual and cultural works in digital form. A brief rundown of some of these laws include the following:

- Prioritizing Resources and Organization for Intellectual Property Act of 2008
- Digital Millennium Copyright Act of 1998
- Copyright Term Extension Act of 1998
- United States No Electronic Theft Act of 1997
- Telecommunications Act of 1996
- Copyright Act of 1995
- Computer Fraud and Abuse Act of 1984

A *New York Times* editorial on the Sonny Bono Act has warned that it is "… the beginning of the end of public domain [and] the birth of copyright perpetuity" (Lessig, 2003, p. 246).

There is little doubt that the advent of the Internet is significantly modifying our basic ideas about the fair use of copyrighted materials on the digital commons. The reification of information for commodification is facilitated by the developing architecture of the Internet as a commercial vehicle for transacting business. The consequence of this is that access to cultural and intellectual works in cyberspace is increasingly limited to those of means. This further contributes to the digital divide between the haves and the have-nots in the alleged Information Age.

Under these circumstances, Swartz wrote his *Guerilla Manifesto.* It is written in a problem/solution expository style that ends with a clarion call to action. As a hacker and hacktivist, it is only natural that Swartz would have taken an epistemological stance toward information favoring research. Therefore the gist of his manifesto promulgates a hacker ethic dedicated to the pursuit of unfettered knowledge and free inquiry. Since the manifesto is short, it has been included it in its entirety here.

> *Guerilla Open Access Manifesto*
>
> Information is power. But like all power, there are those who want to keep it for themselves. The world's entire scientific and cultural heritage, published over centuries in books and journals, is increasingly being digitized and locked up by a handful of private corporations. Want to read the papers featuring the most famous results of the sciences? You'll need to send enormous amounts to publishers like Reed Elsevier.
>
> There are those struggling to change this. The Open Access Movement has fought

valiantly to ensure that scientists do not sign their copyrights away but instead ensure their work is published on the Internet, under terms that allow anyone to access it. But even under the best scenarios, their work will only apply to things published in the future. Everything up until now will have been lost.

That is too high a price to pay. Forcing academics to pay money to read the work of their colleagues? Scanning entire libraries but only allowing the folks at Google to read them? Providing scientific articles to those at elite universities in the First World, but not to children in the Global South? It's outrageous and unacceptable.

“I agree,” many say, “but what can we do? The companies hold the copyrights, they make enormous amounts of money by charging for access, and it's perfectly legal — there’s nothing we can do to stop them.” But there is something we can, something that's already being done: we can fight back.

Those with access to these resources — students, librarians, scientists — you have been given a privilege. You get to feed at this banquet of knowledge while the rest of the world is locked out. But you need not — indeed, morally, you cannot — keep this privilege for yourselves. You have a duty to share it with the world. And you have: trading passwords with colleagues, filling download requests for friends.

Meanwhile, those who have been locked out are not standing idly by. You have been sneaking through holes and climbing over fences, liberating the information locked

up by the publishers and sharing them with your friends.

But all of this action goes on in the dark, hidden underground. It's called stealing or piracy, as if sharing a wealth of knowledge were the moral equivalent of plundering a ship and murdering its crew. But sharing isn't immoral — it's a moral imperative. Only those blinded by greed would refuse to let a friend make a copy.

Large corporations, of course, are blinded by greed. The laws under which they operate require it — their shareholders would revolt at anything less. And the politicians they have bought off back them, passing laws giving them the exclusive power to decide who can make copies.

There is no justice in following unjust laws. It's time to come into the light and, in the grand tradition of civil disobedience, declare our opposition to this private theft of public culture.

We need to take information, wherever it is stored, make our copies and share them with the world. We need to take stuff that's out of copyright and add it to the archive. We need to buy secret databases and put them on the Web. We need to download scientific journals and upload them to file sharing networks. We need to fight for Guerilla Open Access.

With enough of us, around the world, we'll not just send a strong message opposing

> the privatization of knowledge — we'll make it a thing of the past. Will you join us? (Swartz, 2015, pp. 26 - 27).

Swartz begins his manifesto with a structural and ontological metaphor: "Information is power." As already noted, structural metaphors make one-to-one relationships between disparate concepts. In this case, knowledge corresponds to power. The epistemological stance of Swartz and other computer engineers toward knowledge reflects a hacker ethic that values freedom and open access to the Internet. To Swartz and other hackers and hacktivists, access to information is fundamentally a question of human rights where those with entree to the "banquet of knowledge" are obligated to share it with those who don't. Swartz has used a metaphor analogizing information to intellectual repast that reveals how hackers and hacktivists imbue knowledge with properties of sustenance and nourishment. Just as food nourishes our bodies, knowledge provides the "food for thought" that feeds our minds and empowers our lives. The idea that knowledge is power in the sense that it sustains us on a basic human level is probably one of the most important embedded metaphors employed by Swartz and other subscribers to the hacker ethic. From the hacktivist point of view, denying information to another human being would be as morally repugnant as denying someone food and shelter. Sharing information, then, becomes a moral responsibility in the hacker worldview.

Naturally, information that is hoarded and paywalled is anathema to hacktivists. Yet governments and corporations value security and property on the World Wide Web. For this reason, Swartz has identified the problem of access to information as one where those in authority "want to keep it for themselves." Swartz has criticized the fact that "the world's

entire scientific and cultural heritage, published over centuries in books and journals, is increasingly being digitized and locked up by a handful of private corporations" (2015, p. 26). He affirms that the purpose of the open access movement is "to ensure that scientists do not sign their copyrights away but instead ensure their work is published on the Internet, under terms that allow anyone to access it" (2015, p. 27).

From an epistemological point of view, metaphors and linguistic frames are heuristic devices because they help us comprehend and resolve problems. Once invoked, the logic of the metaphor demands a methodology that Lakoff and Johnson call "the systematicity of metaphorical concepts" (1980, p. 2). Therefore the systematicity of a structural metaphor equating knowledge to sustenance would provide for a heuristic frame that draws on associated frames and concepts. Such a heuristic frame of reference would necessarily privilege academic freedom over information restriction. Though prosecutors sought to use Swartz's manifesto as a sign of his motive to illegally distribute academic articles over the Internet, there is evidence that Swartz was actually engaged in academic research when he downloaded articles from JSTOR's academic database. Swartz's former girlfriend, Quinn Norton, has suggested as much. In an article appearing in *The Atlantic* on March 3, 2013, she recounts her involvement with Aaron during his prosecution and the intimidating interrogation she underwent by federal agents seeking to find evidence of his criminal intent. After she had revealed his *Guerilla Manifesto* to government authorities, she remembers her dismay at overhearing Swartz speak on the telephone about his data collection methods to a reporter shortly thereafter.

> Later I listened to Aaron on the phone as he described to a journalist how he had downloaded 400,000 law journal articles to do text analysis, revealing what kind of

> legal research was being funded by what kind of companies in 2008, and publishing an academic paper at Stanford about it, all as explanation of why he might have downloaded the JSTOR articles. It was the best answer legally to the question I'd been asked in that small fluorescent room surrounded by big men. Listening to him say that I felt my insides collapse. Why didn't he tell me? Things could have been different (Quinn, 2013).

Using a programmer technique called scraping, Swartz deployed computer scripts to robotically harvest scholarly articles from JSTOR for analysis at a later date. It is a common technique among computer-savvy researchers. In an era of Big Data, scraping generates the large data sets necessary for the sifting of information to conduct detailed analyses of the developing structure of the Net. Though scraping is a method for compiling the meta data that fuels corpus linguistics and other broad-based studies, it is also often a violation of the terms of service (TOS) required to access computer networks, websites, and other online information sources. Science fiction author Cory Doctorow has been another of Swartz's friends critical of federal prosecutors in his case. In a post appearing at Boing Boing on June 30, 2016, Doctorow provided the following legal analysis of the epistemological facts of Swartz's case:

> The [Computer Fraud and Abuse Act] CFAA is the statute under which Aaron Swartz was prosecuted; Swartz had used a script to download scholarly papers from the MIT network. Though he was allowed to access and download these papers, the network's terms of service required him to access them by manually clicking on links, instead of using a script. Because Swartz violated these terms, a US federal

prosecutor argued that he should spend 35 years in prison. Swartz hanged himself in 2013, as his case was taking a turn for the worse.

….

Given the severe penalties for CFAA violations, it's not surprising that researchers are leery of running afoul of its provisions. A group of researchers – academics and journalists – say that they are unable to scrape websites in order to determine whether the companies behind them are engaged in illegal discrimination (for example, to see whether men are showed higher-paying jobs than women on job-search sites, or whether people of color are "steered" to high-interest loans when they qualify for cheaper, better forms of credit).

…

Courts and prosecutors have interpreted a provision of the CFAA – one that prohibits individuals from "exceed[ing] authorized access" to a computer – to criminalize violations of websites' "terms of service." Terms of service are the rules that govern the relationship between a website and its user and often include, for example, prohibitions on providing false information, creating multiple accounts, or using automated methods of recording publicly available data (sometimes called "scraping").

The problem is that those are the very methods that are necessary to test for discrimination on the Internet, and the academics and journalists who want to use those methods for socially valuable research should not have to risk prosecution for using them. The CFAA violates the First Amendment because it limits everyone,

> including academics and journalists, from gathering the publicly available information necessary to understand and speak about online discrimination (Doctorow, 2016).

For hackers, hacktivists, and the academic community as a whole, copyright law is stifling important research. As Doctorow points out, it prevents research into unfair computer algorithms that may be guiding Netizens toward certain kinds of information based on discriminatory criteria of gender, race, and class. Additionally, it stifles research into how computer scientists can improve online security systems because copyright law deems this kind of investigation as itself a security violation. The case of a computer scientist, Ed Felten, demonstrates the latter point.

Felten had been invited to a forum to expose weaknesses in encryption programs designed to protect copyrighted material transmitted over the Internet. When he and his team easily broke the encryption code and prepared a conference paper about it, the Secure Digital Media Initiative (SDMI), the Recording Industry Association of America (RIAA) and the Verance Corporation threatened him with a lawsuit for violating the Digital Millennium Copyright Act (DMCA). Among its many other proscriptions, the DMCA prohibits revealing information about how to circumscribe Digital Rights Management (DRM) technologies even for conference papers designed to improve them.

A kind of digital lock placed on protected content, DRM is designed to regulate the distribution of copyrighted materials over the Internet. Lessig has insisted that "enabling technology to enforce the control of copyright means that the control of copyright is no longer defined by balanced policy." The DMCA serves to buttress existing DRM

technology by criminalizing the manufacture and distribution of any device created to circumvent DRM control measures. This law has had unexpected consequences for computer scientists like Felten. Under threat of lawsuit by corporate interests, Felten withdrew his paper from the conference though he issued a statement of protest.

In a similar case, a Russian computer programmer named Dmitry Sklyarov was arrested during an eBook conference in the U.S. for alleged copyright violation under the terms of the DMCA. Complaints by Adobe that the Russian had developed an eBook reader violating Adobe's copyrighted book content led to his arrest following the presentation of his paper entitled "eBook Security - Theory and Practice." He spent several months in an American prison before being permitted to return to Russia in 2001. These and other cases have put cryptographers and innovators on high alert with regard to the possibility of prosecution under the anti-circumvention measures of the DMCA and have had a chilling effect on the overall cryptanalysis research community. All told, such cases illustrate how copyrighted knowledge can block academic inquiry and prevent open discussion on developing information technologies.

B. Swartz's FBI Files

The second text I look at is the FBI file on Swartz**.** Swartz ordered his FBI file when he discovered the Bureau had begun surveilling him after he hacked into public court documents kept at the Public Access to Court Electronic Records (PACER) website maintained by the federal judiciary. It is no doubt significant that this act of hacktivism occurred the same year Swartz published his *Guerilla Manifesto.* Public records at the PACER website are secured behind a digital pay-wall, and Swartz's hacktivism was an act

of content liberation in which he copied federal court documents and delivered them to Internet archivist, Carl Malamud, at his website, Public.Resource.org. Malamud had already gained a reputation as a free data activist with the founding of his non-profit organization. As such, Public.Resource.org is dedicated to recovering public documents from behind commercial paywalls and returning them to the public domain. A longstanding admirer of Malamud and his website, Swartz had responded to Malamud's call to liberate documents locked behind the paywall of the Administrative Office of the United States Courts. The federal judiciary had been charging a fee for copies of electronic court documents housed at PACER even though federal documents are not covered under copyright laws and so – at least in theory – freely available to the public. In a memorial tribute to Swartz called *Aaron's Army* (2013, Jan. 24), Malamud has recalled the episode thusly:

> When we brought in 20 million pages of U.S. District Court documents from behind their 8 cent-per-page PACER pay wall, we found these public filings infested with privacy violations: names of minor children, names of informants, medical records, mental health records, financial records, tens of thousands of social security numbers.
>
> We were whistle blowers and we sent our results to the Chief Judges of 31 District Courts and those judges were shocked and dismayed and they redacted those documents and they yelled at the lawyers that filed them and the Judicial Conference changed their privacy rules.
>
> But you know what the bureaucrats who ran the Administrative Office of the United States Courts did? To them, we weren't citizens that made public data better, we

were thieves that took $1.6 million of their property.

So they called the FBI, they said they were hacked by criminals, an organized gang that was imperiling their $120 million per year revenue stream selling public government documents (Malamud, 2013).

Using a free trial account offered through the Sacramento Public Library, Swartz hacked into PACER where he copied more than two million public court records and turned them over to Public.Resource.org. The FBI took immediate notice. Federal agents visited Swartz on April 19, 2009 requesting to talk with him but he refused because he did not have a lawyer present. Malamud remembers how the FBI conducted a secret investigation into their digital activism:

The FBI sat outside Aaron's house. They called him up and tried to sucker him into meeting them without his lawyer. The FBI sat two armed agents down in an interrogation room with me to get to the bottom of this alleged conspiracy.

But we weren't criminals, we were only citizens.

We did nothing wrong. They found nothing wrong. We did our duty as citizens and the government investigation had nothing to show for it but a waste of a whole lot of time and money.

If you want a chilling effect, sit somebody down with a couple [of] overreaching federal agents for a while and see how quickly their blood runs cold (Malamud, 2013).

Swartz filed a Freedom of Information Act (FOIA) for his FBI records later that year in August of 2009. When he received them, he posted them to his web blog in October that same year. (It is worth noting that FOIA requests for Swartz's FBI file have been ongoing ever since, as Muckrock and others have continued to seek copies of his files from the FBI and U.S. Secret Service.) Black Vault's website appears to have the most comprehensive compendium of FBI and Secret Service documents released on Swartz to date. Altogether, the pages of these documents number in the hundreds of thousands due to the extensive computer records compiled by the U.S. Secret Service of his JSTOR downloads. The Secret Service file alone constitutes over 14,500 pages of material (Wachtler, Nov. 8, 2015)

FOIA requests archived at Black Vault's website come in four batches: 1) Swartz's initial FBI file following his brush with federal authorities after the PACER incident; 2) documents released after he was indicted for downloading JSTOR articles; 3) documents released by the U.S. Secret Service; 4) documents released after his suicide.

In particular, the second batch of documents is revelatory of the depth and breadth of interest the FBI showed in Swartz after he had hacked MIT's computer networks in order to download academic articles. When the FBI and U.S. Secret Service agents first raided Swartz's apartment at 950 Massachusetts Avenue (as well as his basement storage locker and his office in the Safra Center for Ethics at Harvard) on February 11, 2011, they took a breathtaking amount of his personal property. The haul included what appeared to be a complete inventory of his computer equipment, in addition to pay stubs, electrical cords, notebooks, papers, and books. This was assiduously detailed in their report. After the FBI raid, the first version of this interview has Swartz mentioning the loss of a book he was writing while the second does not.

Swartz posted the FOIA documents released by the FBI at his personal website in order to demonstrate the extent of the government's surveilling of his private activities. The overall tone of his web blog appears to be one of bravado. FOIA documents from the first batch of records stored at Black Vault showed that not only had Federal agents identified Swartz's IP address and physical home address, they also conducted a Naval Criminal Investigative Services (NCIS) records check on him in addition to record checks with the State of Illinois and the Department of Labor. What is more, the FBI sent disguised agents to his family home to photograph cars, license plates, and people, and to note the layout of the Swartz family home. They documented his profile at LinkedIn and Facebook (also making note of the locale for each of his associates), and they perused his personal website at www.aaronsw.com. They downloaded articles he had written for the *New York Times* and his personal weblog, compiled all his PACER court records, and swept up a huge amount of his personal emails, telephone calls, and text messages.

For purposes of my thematic analysis, I have decided to focus on the first batch of documents at Black Vault's website that comprise the FOIA documents Swartz requested from the FBI after he was cleared of any wrong doing in the PACER case. Though this batch of documents is twenty-six pages long and heavily redacted, they nevertheless provide valuable insight into the reasons the FBI monitored and investigated Swartz after he and Malamud downloaded court records from the Administrative Office of the United States Courts. The FBI file also summarizes the federal government's legal perspective with regard to the consequences of copyright violations.

The first sentence of the FBI report provides a legal overview of the PACER case: "The U.S. Courts implemented a pilot project offering free access to federal court records through

the PACER system at seventeen federal depository libraries" (U.S. Dept. of Justice, 2009). In doing so, it makes use of a number of metaphors that are so deeply embedded in the bureaucratic language of the report as to go almost undetected. Those metaphors include the previously mentioned themes of freedom of information versus security of information. Additionally, it includes the idea of the monetary value of information, which it estimates at close to $1.5 million dollars in federal court records. It also addresses the appropriate manner of access to information and the role of federal repositories in providing public access to information. To set up the frame for the latter idea, the report claims that federal court records are kept at "federal depository libraries" through PACER. Noteworthy here is the implied idea that federal depository libraries function as vaults of information akin to federal reserve vaults of money. The safeguarding of valuables in government repositories begs the question of what items constitute value, why is it necessary to secure them, and why the government is the appropriate agency for doing so. The FBI report also objectifies information in a manner similar to Reddy's conduit metaphor. Recall that the conduit metaphor posits the idea that words are containers for meaning, thoughts, and feelings and that this tends to conceal the cooperative aspects of communication. In doing so, the FBI report points to the deeply embedded metaphor of capitalism as its associated conceptual framework since it assumes that government institutions are the natural administrators for economic business. The metaphorical theme of capitalism is embedded throughout the report's opening paragraph implying that information is a commodity like any other.

The FBI report continues. "Library personnel maintain login and password security and provide access to users from computers within the library" (U.S. Dept. of Justice, 2009). Again, the idea of informational security points to the kind of objectification of information

that implicates Reddy's conduit metaphor. The idea that information can be locked up like any other physical object neglects the fact that information arises out of communicative processes between people engaged in the social construction of meaning and knowledge. Information is not an actual object in space that can be secreted away and secured in strongboxes since it only actually exists at the moment it arises through discussion. But since most people understand communication in terms of the conduit metaphor, it is frequently the default setting for any discussion of knowledge sharing. This means that the objectification of information implicit in the conduit metaphor goes largely unrecognized even though it is an embedded metaphor that greatly influences our understanding of social epistemology. Through its depiction of Swartz's manner of access to libraries with PACER accounts, the FBI report succeeds in unconsciously objectifying information. "The login information was compromised at the Sacramento County Public Law Library (SCPLL) and the Seventh Circuit Court of Appeals Library (SCCAL). The two accounts were responsible for downloading more than eighteen million pages with an approximate value of $1.5 million." The FBI's use of the metaphor "compromise" connotes acts of espionage not normally associated with borrowing materials from a public library. Likewise the metaphor of $1.5 million to entail the value of public court records is one that objectifies information by assigning it capital value. The fact that these court records were once freely available in the public domain is completely disregarded in such an economic framework of commodified data.

What is perhaps noteworthy about this opening paragraph is that by taking as a given the embedded metaphors of capitalism and the objectification of data, the report succeeds in framing the PACER case in such a way as to conceal the debate over freedom of

information lying at the heart of it. It assumes its own premises, a rhetorical ruse of bureaucracies everywhere. This points up another important aspect of the frame structure of government: because the operational logic of society is that government is the primary actor for the benefit of all, we tend to assume its greater beneficence as compared to individual acts by ordinary people. This allows government institutions to achieve an ontologically stable, almost agentless state of being that is always GOOD, even when acting against the interests of the people. It also conceals the individuals who comprise the prosaic operations of day-to-day government. In doing so, it can create the impression that government is a moral reasoning entity capable of acting like an independent rational human being. Institutional frame conflict arising from this kind of synecdoche is an issue that will be examined at greater length in the next thematic analysis.

Looked at from the point of view of government/corporate desire to control and limit information for purposes of security and commodification – what functionally comes down to secrecy – the associated frame and embedded metaphor of secrecy must also be examined for its import in the debate over freedom of information. Secrecy draws on metaphors connotative of the confidential, the hidden, the unknown, and the mysterious. Secrecy also draws on associated linguistic frames of deceit and deception. A revolutionary practitioner of its opposite frame through radical transparency, the notorious founder of WikiLeaks, Julian Assange, has addressed the subject of government secrecy in his short essay entitled *Conspiracy as Governance* (2006, Dec. 3). According to Assange, "We must understand the key generative structure of bad governance". He identifies this first and foremost as conspiracy. According to Assange, a cabal of conspirators is seldom beneficial for the people it claims to govern since it must first vow allegiance to its fellow conspirators before

the interests of its citizenry. Exploitation of those not in the know is usually the objective of such a cabal. Assange theorizes that if left unchecked, governance through conspiracy induces debilitating social passivity:

> Everytime we witness an act that we feel to be unjust and do not act we become a party to injustice. Those who are repeatedly passive in the face of injustice soon find their character corroded into servility. Most witnessed acts of injustice are associated with bad governance, since when governance is good, unanswered injustice is rare. By the progressive diminution of a people's character, the impact of reported, but unanswered injustice is far greater than it may initially seem (Assange, 2006).

It perhaps goes without saying that another one of the tools of bad governance are secret courts and investigations. Secret courts called star chambers had become such an odious tool of political repression by the monarchy of medieval England that the Habeas Corpus Act of 1640 abolished them altogether. The fact that Swartz had been the subject of a secret FBI investigation despite not having broken any laws no doubt contributed to the kind of unhappy cognitive dissonance that would eventually lead to his suicide. Certainly the fact that he was reading Franz Kafka's *The Trial* by the end would suggest as much. To all accounts, Aaron Swartz's case illustrates how the embedded metaphor of secrecy entailed in the commodification of information is one that should be seriously scrutinized for its impact on the growing digital divide in the alleged Information Age.

C. The MIT Report

After Aaron Swartz's suicide on January 11, 2013, MIT president L. Rafael Reif called for an internal investigation of the school's involvement in his case. The *Report to the President: MIT and the Prosecution of Aaron Swartz* (2013, July 26) was authored by Professor Harold Abelson, an MIT professor of computer science and engineering, Peter A. Diamond, an MIT economist and professor emeritus, Andrew Grosso, a former assistant US attorney, and Douglas Pfeiffer, MIT assistant provost for administration. Together the team interviewed 50 people and reviewed close to 10,000 pages of documents. Their report is the subject of my third text analysis.

MIT conducted the self-review with the intent to learn from the events that transpired and to justify its actions. Six months after the death of Swartz, it issued a 182-page report to president L. Rafael Reif, the MIT community, and the public at large. From these pages, I have selected key parts of the report in order to address its overarching theme of neutrality with a particular focus on pages sixty-two through seventy. These pages shed light on MIT's avowed stance of neutrality and subsequent discussions about it with Aaron's father, Robert Swartz. I have also examined the university's self-reflection in the latter part of the report.

MIT's role in the affair began when Swartz was on research fellowship at Harvard University's Edmond J. Safra Research Lab on Institutional Corruption. Swart was under the tutelage of Lawrence Lessig, a renowned lawyer, author, and activist on the issue of digital rights and open access to the Internet. The young research fellow had a guest user account at MIT's library that allowed him to access JSTOR's digital database of academic journals, books, and articles. Using a utility closet to plug into MIT's computer networks, Swartz hooked up a laptop and began downloading millions of JSTOR articles.

When his computer was discovered, two MIT police officers and a U.S. Secret Service

Agent arrested Swartz on January 6, 2011. Swartz was initially charged by the state of Massachusetts with two felony counts of breaking and entering. In the meantime, a federal indictment released by grand jury on July 14, 2011, charged him with "four felony counts, these being one count of wire fraud and three counts of violating the Computer Fraud and Abuse Act (CFAA)" (Abelson, et. al, 2013, p. 36). On Nov. 6, 2011, he was subsequently indicted by the state on three additional counts "of accessing a computer without authorization; and one count of larceny—stealing the electronically processed or stored data of JSTOR—in an amount over $250" (Abelson, et al., 2013, p. 35). This was added to the previous breaking and entering charges for a total of six felony counts against him by the state of Massachusetts. Not to be outdone, a federal superseding indictment issued on Sept. 12, 2012, replaced the state's case and "charged Aaron Swartz with thirteen felony counts, these being two counts of wire fraud and eleven counts of violating the CFAA" (Abelson, et al., 2013, p. 38). According to the MIT report, "Essentially, the superseding indictment took the four counts from the initial [federal] indictment and broke each of them into multiple counts, by charging Aaron Swartz's alleged conduct (as related to each of the four legal theories of liability) as discrete events in place of being merged into single allegations of liability. Also, the theory of liability for the final count, alleging damage to a protected computer, was expanded" (p. 38).

While JSTOR was apparently satisfied with a settlement reached with Swartz on June 3rd of 2011 and refused to participate in further litigations against him (p. 42), MIT was not. Instead MIT chose to insist on its neutrality, which meant that the university fully cooperated with prosecutors. At one point, according to Swartz's second lawyer, Marty Weinberger, JSTOR had agreed to negotiate a plea bargain to prevent Swartz from serving

jail time but MIT refused to do likewise.

The ostensible purpose of MIT's report was to "to determine facts and to consider what can be learned from this tragedy" (p. 14). In the opening of the report, its author, Professor Abelson, states that "We hope this report, by laying out a full history of MIT's involvement, will put people in a better position to judge for themselves the plausibility of the various comments and positions taken, and to evaluate MIT's conduct" (p. 12). Toward that end, Abelson goes on to ask readers to "limit the effects of hindsight" when reading the report so as to interpret it from a "perspective uncolored by the shock and tragedy of Aaron Swartz's suicide, or…by the realization that he was the person who did the downloading and who was then arrested" (p. 12). In his opening letter to Professor Abelson, the MIT president concludes that, "On behalf of MIT, I thank you in advance for the objectivity, analytic skill, and high sense of responsibility that you will bring to the task" (p. 3). Metaphors of objectivity, factuality, authority, and synecdoche recurred throughout the report and are addressed again in a more detailed examination of the thematic elements of the texts.

The gist of MIT's 182-page report was its stance of neutrality. "Early in the prosecution by the U.S. Attorney's Office in Boston, MIT adopted a position of remaining neutral, with limited involvement" (p. 13). MIT officials maintained that private conversations with the prosecution lead them to believe that anything they said in defense of Swartz would make no difference to the government and in fact, could actually harm Swartz (pp. 14, 46). They also maintained that since Swartz was not a student, faculty, staff, or alumni of MIT, he was not a part of the MIT community per se and therefore did not warrant its intervention in his case. This despite the fact that Aaron's father was an alumnus of the institute and worked as a consultant for MIT's Media Lab while two of Aaron's brothers had interned there.

Furthermore, the rest of the MIT community "paid scant attention to the matter" (p. 14) and "the MIT community did little to draw the administration more deeply into the case" (p. 54). All in all, "MIT took the position that *U.S. v. Swartz* was simply a lawsuit to which it was not a party" (p. 14). This feat of existential legerdemain – the idea that MIT was at once a party involved in a case as the victim of a "break-in" and NOT a party involved in the case because of its purported indifference to it – is also worth a closer examination, especially with regards to its claims of impartiality, objectivity, and fairness.

At many points throughout the report, MIT adapts a stance of non-involvement and neutrality in the affair. For example on page 13, it declares, "MIT never requested that a criminal prosecution be brought against Aaron Swartz." On page 21, "We note that no one from MIT called the Secret Service." On page 35, "MIT was not involved in the state prosecution." And again on page 54 it insists, "MIT had not pressed for criminal charges against Aaron Swartz."

But it turns out that MIT's protestations of neutrality and disinterestedness were nuanced and prone to change. According to the report, the nature of MIT's stance of neutrality included two stages: an initial phase in which it refused to make any public statements about the case or take an official position on it (p. 52), and after the prosecution began, a second stage in which MIT decided to treat both sides the same in terms of providing documents and interviews for legal proceedings.

That was MIT's position of neutrality in theory. But in reality, MIT cooperated fully with the government, fulfilling many of the Secret Service's initial requests for documents of Swartz's laptop without a subpoena though it was not similarly cooperative with Swartz's lawyer (p. 49). In the case of the defense, MIT actively stonewalled to requested meetings

by Aaron's attorney and "did not produce to the defense, even though requested by subpoena, documents that the defense sought from MIT but that MIT had already provided to the government" (p. 76). To the latter charge, MIT maintained that it "did not want MIT to engage in duplication of effort regarding document production" since it assumed that the requested documents would be provided to the defense by the prosecution (p. 76).

According to Swartz's former girlfriend, Taren Stinebrickner-Kauffman, MIT was not at all neutral in its stance against Swartz. "MIT's lawyers gave prosecutors total access to witnesses and evidence, while refusing access to Aaron's lawyers to the exact same witnesses and evidence," she said. "That's not neutral." (Abel, 2013, July 30). Robert Swartz corroborated Stinebrickner-Kauffman, stating that in a meeting with MIT's Chancellor on September 14, 2011, "the defense could not get any assistance from MIT, particularly access to persons, documents, or answers to questions about the network or logs" (Abelson, et al., 2013, p. 63).

When the lobbying efforts on behalf of Aaron by his father proved unsuccessful, Swartz's legal team went on the offensive. Swartz's new defense attorney, Martin Weinberg (replacing Andrew Good), filed a motion to suppress evidence. Since the motion to suppress was based on the principle of Swartz's fourth amendment right to privacy which had been violated by the university and the government when they seized and opened his computer MIT was unhappy at the possibility of the besmirchment of its good name (Abelson, et al., 2013, p. 74). Reversing course entirely, "MIT decided that it would not be fully neutral with regard to defending anticipated possible attacks on MIT's employees or the Institute's integrity" (p. 76).

Anyone who has dealt with bureaucracies will note the shifting stances they frequently

assume when describing the nature of their operations. Sometimes bureaucracies present themselves as a coalition of autonomous units operating at cross-purposes to each other, and at other times, as a unified whole acting with a single will. For this reason one of the more noteworthy embedded metaphors at play throughout the MIT report is that of synecdoche. Synecdoche is a class of referential metaphors where the part can represent the whole and the whole can represent the part. Since metaphors are linguistic framing devices for organizing concepts, synecdoche is the domain/profile aspect of frame semantics in cognitive linguistics. For example, a wheel is one part of a vehicle, but when used in the sentence "I've got a new set of wheels," it refers to a car or motorcycle as a whole (Lakoff and Johnson, 1980, p. 36). Nuanced connotations for the entity "MIT" expressive of either its profile or its domain (its wholeness or partialness), allowed officials at the Institute to effectively manipulate synecdoche in order to elude responsibility for cooperating with Swartz's lawyers. For example, at certain critical points, the authors of the MIT report express the idea of the university as an entire sentient organism capable of independent rational thought. As convenient as this metaphor may be for providing a neat account of its administrative functions and decisions, it fails to acknowledge the many individuals who actually compose MIT and who bear responsibility for its daily operations. At other points, MIT officials characterized the university as one made up of autonomous offices operating with varying degrees of cooperation. The MIT report thus vacillated in its representation of itself, sometimes appearing to recognize the fact that it is an institution composed of individuals and their attendant offices, and at other times representing itself as though it were a self-contained rational being in its own right. These permutations of the entity "MIT" – who or what constituted it, what its functions were, and how it conducted its

operations – were ongoing throughout the affair. Such frame conflicts led to considerable miscommunication among the involved parties. In this manner, MIT officials kept Swartz's legal team off balance and on the defensive.

In *Context and Cognition: Knowledge Frames and Speech Act Comprehension* (1977), Teun A. Van Dijk has stated that frames are "not arbitrary 'chunks' of knowledge… they are knowledge units organized around a certain concept." Frames help create the meta-narratives necessary for the maintenance of political ideology and directly implicate the importance of social power and cultural capital in political life. The latter is a field of linguistics called pragmatics, of which critical discourse analysis is a subset. A study of the political rhetoric of hacktivists and their detractors demonstrates how the use of metaphor is necessary for the construction of linguistic frames that support a social epistemology of the Internet. In the case of MIT, the framing of its position of "neutrality" drew on its long-standing reputation as an academic institution of science and engineering that placed stress on its dispassionate attitude in worldly affairs. Teun A. Van Dijk views pragmatic theory as one founded on conceptual and empirical principles and defines frames as organized conceptual systems. In presenting the meta-narrative of its impartiality and non-involvement in Swartz's case, MIT played up its institutional frame of scientific rationality and objectivity. MIT's depiction of its neutrality drew on linguistic frames valuing impartiality and fairness, a fact that greatly upset Robert Swartz who could not be reconciled with MIT's disinterestedness in his son's case especially given his family's long-standing service to the institution. Robert Swartz sought to get the university to agree to a settlement with his son similar to the one that JSTOR had negotiated, but MIT officials maintained that, "it did not want anything from Aaron Swartz and had no intention of filing any lawsuit against him,

and saw no point in a settlement" (2013, p. 63). The grieving father accused the university of attempting to destroy his son.

Nevertheless, the institution had pause for reflection on its responsibilities as an educator in the latter part of its report. In the close of MIT's report to the president, the authors have included a chapter in which they present a series of critical questions about MIT's leadership as a research institute. Labeled "Questions for the MIT Community," the university considers what it can do to prevent future tragedies by perhaps more clearly asserting its epistemological mission in the future. It begins by asking, "What are MIT's institutional interests in the debate over reforming the computer fraud and abuse act?" In the ensuing discussion, the authors of the report muse over the difficulties of conducting research at a time of rapidly evolving communication technologies, exacerbated by vacillating information laws and policies.

> MIT is not a legislature: it does not hold open debates about how its Terms of Service (TOS) should be crafted, defined, provided with "safe harbors," and otherwise applied; and it cannot foresee how rapid advances in technology and social uses of technology may make its TOS obsolete, unclear, or a dangerous and unintended trap for the unwary. Does MIT want to be in the position of determining what is and is not a felony? The application of this clause can criminalize even minor violations of TOS, and expose violators to civil and criminal penalties. In an intensive environment of exploration, it is not uncommon for researchers to conduct experiments that arguably violate the broad terms of service often associated today with websites and services. As one example, research involving collection and

> analysis of data about Internet services is vital to scholarly understanding of this medium (Abelson, et al., 2013, p. 94).

In this regard, MIT is in agreement with Doctorow's analysis of the laws governing the rules of access to the internet and their potentially chilling effect on research, particularly with regard to studying the workings of the Internet itself. The MIT report goes on to speculate about Swartz's motive for downloading JSTOR articles and the importance of the right to access academic articles on the Internet.

> Aaron Swartz's downloading of the JSTOR database may have been motivated by the ideal of open access to scholarly works. Many commentators on the Swartz case have criticized MIT for not taking this into account in responding to his prosecution, given that MIT is itself a leader in advocating for open access. Should MIT be doing even more in support of open access to scholarly publications? At present, the MIT Open Access Working Group is considering possible proactive initiatives in light of recent push-backs, by some publishers, against open-access policies. These include publicly advocating pro–open access positions with professional societies, increasing MIT's support for open-access journals, and strengthening MIT's commitment to the Faculty Open Access Policy (p. 95).

In its "Questions for the MIT Community," MIT has explicitly recognized its celebrated hacker culture and its attraction for "students who are driven not just to be creative, but also

to explore in ways that test boundaries and challenge positions of power" (p. 98). The authors of the MIT report have engaged in a little bit of soul searching when they acknowledge this aspect of MIT's research reputation.

> [T]here has been a persistent undercurrent of concern over the past several years that MIT's hacking tradition is being vitiated by a perceived increasing tendency to interpret hacking as a criminal activity…. More than once, in our interviews, the Review Panel heard members of the MIT community express a feeling that there has been a change in the institutional climate over recent years, where decisions have become driven more by a concern for minimizing risk than by strong affirmation of MIT values. Several people interpreted the Institute's response in the Swartz case in that light. And some critics have chided MIT for playing such a passive role when Swartz's actions were motivated by principles that MIT itself champions (p. 99).

Eventually, MIT's self-reflection led it to conclude that its stance of neutrality in Swartz's case was morally reprehensible. "A friend of Aaron Swartz stressed in one of our interviews that MIT will continue to be at the cutting edge in information technology, and, in today's world, challenges like those presented by the Swartz case will arise again and again. With that realization, 'Neutrality on these cases is an incoherent stance. It's not the right choice for a tough leader or a moral leader'" (p. 101).

MIT's conclusion in favor of open access to the Internet, while belated, was nevertheless heartfelt. The question of access to information will be further examined in the upcoming thematic analyses.

D. The DOJ's Press Statement

The fourth text I examine is the press release of the Massachusetts U.S. Attorney's Office. The gist of its message is its attempt to legitimate its role in the prosecution of Aaron Swartz. While the MIT report justified its actions through its stance of neutrality, the DOJ's press release insisted on its responsibility to prosecute cyber criminals. Nevertheless, Aaron's mentor, Lawrence Lessig, derided the DOJ in his personal blog in 2013. He wrote:

> From the beginning, the government worked as hard as it could to characterize what Aaron did in the most extreme and absurd way. The "property" Aaron had "stolen," we were told, was worth "millions of dollars" — with the hint, and then the suggestion, that his aim must have been to profit from his crime. But anyone who says that there is money to be made in a stash of ***ACADEMIC ARTICLES*** is either an idiot or a liar. It was clear what this was not, yet our government continued to push as if it had caught the 9/11 terrorists red-handed.
>
> Aaron had literally done nothing in his life "to make money." He was fortunate Reddit turned out as it did, but from his work building the RSS standard, to his work architecting Creative Commons, to his work liberating public records, to his work building a free public library, to his work supporting Change Congress/FixCongressFirst/Rootstrikers, and then Demand Progress, Aaron was always and only working for (at least his conception of) the public good. He was brilliant, and funny. A kid genius. A soul, a conscience, the source of a question I have asked myself a million times: What would Aaron think? That person is gone

> today, driven to the edge by what a decent society would only call bullying. I get wrong. But I also get proportionality. And if you don't get both, you don't deserve to have the power of the United States government behind you.
>
> For remember, we live in a world where the architects of the financial crisis regularly dine at the White House — and where even those brought to "justice" never even have to admit any wrongdoing, let alone be labeled "felons" (Lessig, n.d.).

Under a barrage of criticism, federal prosecutors sought to deny any culpability for their role in his suicide and all charges against Swartz were subsequently dropped. U.S. Attorney for Massachusetts, Carmen Ortiz, who oversaw the case, "expressed sympathy for Swartz's family but said she was 'terribly upset' they're blaming her office" (McConville, & Cassidy, 2013, Jan.). Ortiz insisted:

> This office's conduct was appropriate in bringing and handling this case.... This office sought an appropriate sentence that matched the alleged conduct—a sentence that we would recommend to the judge of six months in a low security setting (Department of Justice, 2013, Jan. 16).

In an interview for *The Boston Globe* shortly after his death, another of Swartz attorneys, Andy Good, has gone on record stating:

> The thing that galls me is that I told Heymann the kid was a suicide risk. His reaction was a standard reaction in that office, not unique to Steve. He said, 'Fine, we'll lock him up.' I'm not saying they made Aaron kill himself. Aaron might have done this

> anyway. I'm saying they were aware of the risk, and they were heedless (Cullen, 2013, Jan. 15).

Swartz wasn't Heymann's first victim. As a specialist in cybercrime, prosecutor Stephen Heymann is the director of U.S. Attorney Carmen Ortiz's Internet and Computer Crimes Unit. In 2000, Heymann convicted the youngest hacker in U.S. history with the case of Jonathan James who at age fifteen hacked his local school district in Miami-Dade county Florida. From there he went on to hack the Department of Defense. It was later discovered that he had also succeeded in hacking into the NASA's International Space Station. He plea-bargained his way down to six months of house arrest followed by probation until age eighteen. Then Attorney General Janet Reno and U.S. attorney Guy Lewis vowed to prosecute youthful hackers more vigorously in the future (Stout, 2000, Sept. 23). It should be pointed out that at least since the Sentencing Reform Act of 1984, there has been a legal trend in the U.S. judicial system to grant prosecutors greater power to prosecute youths as adults by letting the prosecutors determine juvenile sentencing rather than judges. When it was discovered that James had used drugs in violation of his probation, he was sentenced to six months in an Alabama federal correctional facility, one of the worst in the country with a long litany of human rights abuses.

James came under suspicion by Heymann again in 2007 for his association with some of the computer hackers involved in the TJX identity scam. It was the largest case of identity theft of its kind and thousands of credit card numbers and customer information were stolen from the international department store chain. Heymann was involved in the investigation of several of James's friends in the affair. Though James maintained his innocence, Secret Service Agents raided his house looking for evidence to connect him to the cybercrime.

None was found. Worried that the feds were using one of his recently freed friends to trick him into incriminating himself, Jonathan James shot himself in the head two weeks after the raid, ending his young life at age twenty-five. He left behind a note that read:

> I honestly had nothing to do with TJX. I have no faith in the 'justice' system. Perhaps my actions today, and this letter, will send a stronger message to the public. Either way, I have lost control over this situation and this is my only way to regain control. Remember, it's not whether you win or lose, it's whether I win or lose, and sitting in jail for 20, 10, or even 5 years for a crime I didn't commit is not me winning. I die free. ("Prosecutor pursuing Aaron Swartz linked to suicide of another hacker," 2013, Jan. 15).

Heymann would go on to receive the Attorney General's Award for Distinguished Service for his prosecution of the TXJ case.

A career federal prosecutor, many of Heymann's critics have pointed to his personal ambitions in his relentless pursuit of Swartz. In an article for the Huffington Post, "Swartz's attorney Elliot Peters accused Massachusetts assistant U.S. attorney Stephen Heymann of pursuing federal charges against Swartz to gain publicity". Peters felt that Heymann was hunting for "some juicy looking computer crime cases and Aaron's case, sadly for Aaron, fit the bill " (Reilly, et al., 2013, Jan. 14).

In 2013, Congressional investigators Darrell Issa and Elijah Cummings sent a letter to the DOJ asking, "Was Mr. Swartz's opposition to Sopa or his association with any advocacy groups considered?" (McVeigh, 2013, Jan. 29). Apparently the DOJ's response was less than satisfactory because a year later in 2014, a follow-up letter from U.S. Senators John

Cornyn and Al Franken charged Attorney General Eric Holder with inconsistencies in his account of the case when compared with the MIT Report. They pointed out that "The MIT Report indicates that Assistant U.S. Attorney Stephen Heymann considered other factors in advance of the return of the superseding indictment" (Sledge, 2014, Jan. 25).

Indeed, the MIT Report made clear that its own attorneys were intimidated into compliance with Heymann. In a conversation using outside counsel to communicate with Heymann on August 9, 2012, MIT told the prosecutor that it was not interested in punishing Swartz with a prison sentence and that the institution did not look forward to the stress and hassle of pursuing a case against him. Much like Department of Homeland Security official Jane Holl Lute, the DOJ prosecutor employed a metaphor of rape to liken MIT to a victim of sexual assault. While Lute conflated child pornography with financial fraud, Heymann tried to compare Swartz's activism to rape in order to imply that MIT was the victim of his transgressions (Wright, 2013, Aug.). In this manner, Heymann sought to persuade MIT lawyers of the need to prosecute transgressive cyber criminals like Swartz to the full extent of the law. Nevertheless,

> MIT's counsel noted that no one at the Institute was looking forward to the time, disruption, and stress involved in testifying at hearings and trial.
> The prosecutor's response was that it disturbed him whenever a defendant "systematically re-victimized" the victim, and that was what Swartz was doing by dragging MIT through hearings and a trial. He analogized attacking MIT's conduct in the case to attacking a rape victim based on sleeping with other men (Abelson, et al., 2013, p. 67).

Yet MIT's outside counsel continued to resist the idea of imprisoning Swartz, stating at one point that "while the government might believe that jail time was appropriate in this case, the government should not be under the impression that MIT wanted a jail sentence for Aaron Swartz." MIT stressed the fact that its mandate was educational not punitive and made clear that it "did not want to act as an intermediary between the parties" (Abelson, et al., 2013, p. 68).

Heymann responded by insisting that though he had originally intended to have leniency with Swartz, the hacktivist crossed a line when his friends at Demand Progress put up a post about his case at the same time they were leading a campaign against the Stop Online Piracy Act and the Protect IP Act (SOPA/PIPA). As mentioned before, the measures were designed to punish copyright offenders on the Internet by shutting down their websites. According to the MIT Report:

> The prosecutor said that, pre-indictment, he had wanted to approach the case on a human level, not punitively. To this extent he made an extremely reasonable proposal, and was "dumb-founded" by Swartz's response.
>
> The prosecutor said that the straw that broke the camel's back was that when he indicted the case, and allowed Swartz to come to the courthouse as opposed to being arrested, Swartz used the time to post a "wild Internet campaign" in an effort to drum up support. This was a "foolish" move that moved the case "from a human one-on-one level to an institutional level." The lead prosecutor said that on the institutional level cases are harder to manage both internally and externally" (Abelson, et al., 2013, p. 68).

Evidently the fact that Swartz alluded to the political nature of his prosecution on the Demand Progress website after Heymann's first indictment greatly incensed the government prosecutor (Demand Progress, 2011, July 19). As already discussed, Swartz had been leading a battle charge against the government's proposed PIPA/SOPA legislation via Demand Progress and when he and his allies successfully defeated SOPA/PIPA in January of 2012, Heymann followed up with a superseding indictment that significantly expanded the scope and severity of the initial charges against Swartz. While the first indictment against Swartz in July of 2011 included four felony counts of wire fraud, computer fraud, unlawfully obtaining information from a protected computer and recklessly damaging a protected computer, Heymann's superseding indictment in September of 2012 added nine more felony counts to the original four to bring it up to a total of thirteen felony charges.

Robert Swartz roundly castigated government and university officials at his son's funeral stating bluntly, "Aaron was killed by the government, and MIT betrayed all of its basic principles" (Sandra, 2013, Jan. 15). IBM executive Tom Dolan, husband of Carmen Ortiz, responded via Twitter, "Truly incredible that in their own son's obit they blame others for his death and make no mention of the six month offer." This lead Charlie Pierce of *Esquire* magazine to muse, "the glibness with which her husband and her defenders toss off a 'mere' six months in federal prison, low-security or not, is a further indication that something is seriously out of whack with the way our prosecutors think these days" (Pierce, 2013, January 17).

In her press release, U.S. Attorney Carmen Ortiz opens her statement on the death of Aaron Swartz by expressing her sympathy to his family and friends. She calls attention to her relationship with her own family and asserts that she can therefore imagine the pain of

those who were close to Aaron. The major theme in the first paragraph of Ortiz's press statement is that of family, community, and the bonds of love. She tries to establish her humanity to others by assuring her audience of her "heartfelt sympathy" and she briefly mentions the emotions of pain, sympathy, love, and anger (Department of Justice, 2013, Jan. 16).

From there she goes on to assert that the role of her office was appropriate and reasonable in conducting the prosecution of Aaron Swartz. She points out that she and other prosecutors have taken an oath of office (a speech act of great institutional significance) to uphold the law and insists on her duty, responsibility, and moral obligation to prosecute Swartz. While acknowledging that there was no evidence to support the claim that Swartz committed theft for financial gain, she nevertheless defends her office's attempt to reach what she perceives as an equitable punishment for Swartz by suggesting that he serve six months in a low-security prison rather than the maximum sentence suggested by law. Furthermore, she insists that at "At no time did this office ever seek – or ever tell Mr. Swartz's attorneys that it intended to seek – maximum penalties under the law," a statement that is, unfortunately, contradicted by Swartz's attorney, Elliot Peters (Department of Justice, 2013, Jan. 16). Peters's account of his interactions with federal prosecutors has painted a picture of prosecutorial overreach motivated by personal ambition. In an article appearing in the Huffington Post in 2013, he scathingly denounced the federal prosecutor for his career ambitions. "Heymann, Peters believes, thought the Swartz case 'was going to receive press and he was going to be a tough guy and read his name in the newspaper'" (Reilly, et al., 2013, Jan. 14).

Peters would go on to write a formal letter of complaint to the DOJ's Office of

Professional Responsibility accusing Stephen Heymann of threatening Aaron with up to seven years imprisonment if he did not accept a plea bargain. He also detailed other instances of Heymann's professional misconduct such as his failure to turn over relevant evidence in a timely manner and his initial misrepresentation of the extent of the government's involvement in the case (Peters, 2013, January 28).

Ortiz's dissembling on Heymann's lack of ethical professionalism did not go unnoticed. A blog by Scott Horton at Harper's has remarked:

> Ortiz's refusal, even at this late point, to come to terms with her gross misconduct is hardly surprising. She is after all a political figure with political aspirations, and the rules of American politics dictate that one should never admit a mistake, instead pushing blame onto others — here, an Internet prodigy who can no longer defend himself. But it does reinforce her image as a bully who has abused her power and is incapable of reexamining serious mistakes. Past experience suggests that the DOJ itself will behave the same way — closing ranks behind her, hiding the identities of those who collaborated in the tragedy, and concealing vital evidence. For all these reasons, an aggressive, thorough, and public congressional probe with bipartisan support is the necessary next step. Ortiz and her collaborators in this tragedy have serious questions to answer (Horton, 2013, Jan. 18).

In defense of her actions, Ortiz establishes her office within a web of government bureaucracies by pointing out that it was Congress – not her – who mandated the harsh sentencing guidelines for computer fraud and abuse and that the final decision would have

been out of her hands anyway since a judge would have rendered the final verdict. "Ultimately, any sentence imposed would have been up to the judge" (Department of Justice, 2013, Jan. 16).

In this manner, Ortiz sought to exculpate herself by shifting the blame to other decision-makers in the justice system including congress, judges, and the United States Sentencing Commission (USSC). The latter would become the subject of Anonymous's attacks when the hacktivist collective installed memorials to Swartz at the MIT and USSC websites. As already mentioned before, the embedded metaphor of synecdoche provides the domain/profile structures necessary for the linguistic framing of institutions that in turn allows the individuals within them to conveniently shift decision-making responsibility onto others. When bureaucrats cooperate with one another in order to dodge responsibility for their actions, the total effect is one for the obfuscation of the problem to the point of total irrelevancy. As Horton predicted, when called to task by legislators a year later, Attorney General for the DOJ, Eric Holder, defended Ortiz and Heymann and maintained the soundness of their decisions as "good use of prosecutorial discretion" (Masnick, 2013, March 7).

Ortiz continues her justification for her actions in her press release by next reminding her audience of her mission to enforce "the law as fairly and responsibly as possible" by "protecting the use of computers." Implicit in this argument is an appeal to authority – notably her own. As mentioned earlier, the purportedly benign and ethical nature of those who take an oath of office to protect the public good – as in the case of officials with the FBI, MIT, and DOJ – gives bureaucrats recourse to the embedded metaphors of duty and responsibility to support their decisions and justify their actions. As holders of public office,

bureaucrats rely on the ontological frame of their oath of duty to support the appropriateness of their actions as public servants ministering on behalf of the public good. It is a tautological argument encouraging passivity and uncritical acceptance of the organs of state, a necessity for the maintenance of the hegemony of the status quo.

The text of the press release is dense with such metaphors as family, love, law, crime, profit, punishment, mission, and protection. Putting aside her attempt to humanize herself at the outset, what is perhaps most noteworthy about Ortiz's press release are the conceptual metaphors of crime, punishment, and law. In particular, her notion of the laws governing intellectual property is in agreement with the FBI's own ideas about it as demonstrated in its initial investigation of Swartz and Malamud for the alleged theft of public court records. Such "thought crimes" entail the proprietary nature of acts of cognition. In keeping with the embedded metaphor of capitalism, intellectual property is analogous to private property and can be "stolen" just like houses, cars, or gold. According to a capitalistic framework, ideas are as marketable as any other commodity. "Stealing is stealing whether you use a computer command or a crowbar, and whether you take documents, data or dollars," stated Ortiz in a preliminary press release on Swartz's indictment (Day, 2013, June 1).

As previously noted, the problem with metaphors analogizing thoughts to property is that it creates a frame conflict in much the same manner as the conduit metaphor does: by reifying an abstraction. And while the objectification of an abstraction provides a convenient shorthand mode for conceptualizing ideas, it also invests them with physical properties that may not be true. For instance, the frame conflict of the conduit metaphor results from the fact that meaningful communication is dynamically constructed through mutual interactions with others and not simply through the passive decoding of language for

meaning. This fact is hidden by the metaphor's associated linguistic frame entailing language as a "container" for meaning. Likewise, the frame conflict inherent in the notion of "intellectual property rights" results from the objectification of thoughts and ideas that ignores the social interactions that produce them. The embedded metaphor within "intellectual property rights" is one entailing thoughts as marketable commodities. But as Lakoff and Johnson have already pointed out in *Metaphors We Live By* (1980), "a metaphorical concept can keep us from focusing on other aspects of the concept that are inconsistent with that metaphor" (p. 10). In other words, selecting a metaphor that entails thoughts as marketable commodities and securities necessarily *deselects* a metaphor that entails thoughts as shared culture. The proponents of open access and fair use of copyrighted materials in the public domain realize that if copyright becomes too restrictive it will also inhibit the innovation of new forms of digital culture. More importantly, hackers and hacktivists have recognized that as social life become more and more digitized, the potential for the draconian regulation of *all* forms of intellectual and cultural exchange is greatly enhanced.

Under cover of law, the metaphor for the commodification of information conceals how the Internet as a medium of publication has resulted in the significant expansion of intellectual property rights by traditional media giants bent on privatizing the knowledge commons. Yet the ideological roots of the free software movement that nurtured the burgeoning form of the Internet have given hackers firm ground on the electronic commons where all are free to share information (Coleman, 2013, *Coding Freedom*). Recognizing the trend toward the criminalization of the social construction of knowledge on the Internet, Swartz and other Netizens have sought to resist government and commercial encroachments

in cyberspace by promulgating a hacker ethic of cooperation, collaboration, and free inquiry. Anonymous went to the defense of Aaron Swartz because they considered him an ideological brother. Their heartfelt eulogy to him is ample demonstration of their deep-rooted hacker ethic and mutual respect for Swartz's views on open access to the Internet. Such hacker principles are the topic of discussion in the next thematic analysis.

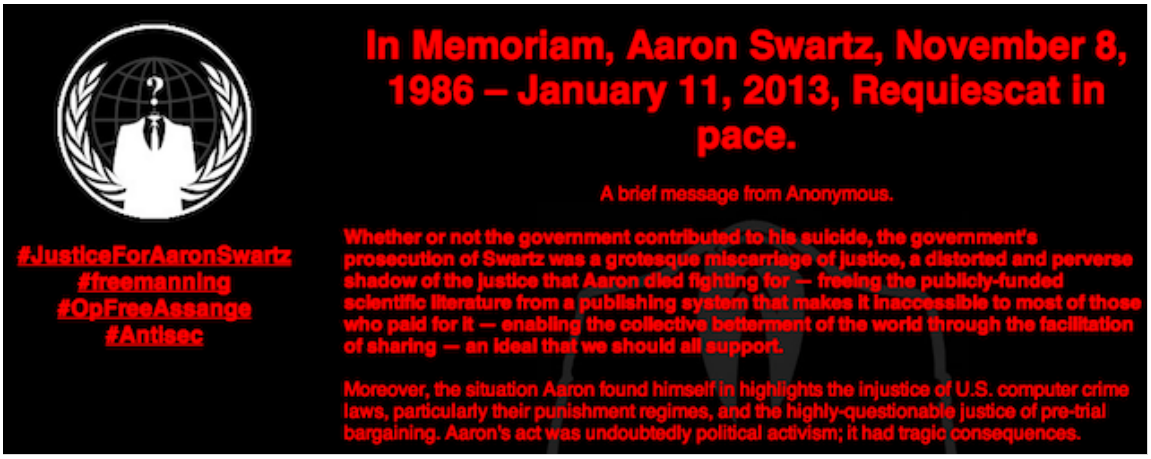

Figure 8. Memorial Tribute to Aaron Swartz Posted by Anonymous

E. Anonymous's Memorial to Swartz

A fifth set of critical communications is comprised of interconnected texts produced by Anonymous in defense of Aaron Swartz. Anonymous hacked the official websites of MIT and the United States Sentencing Commission (USSC) in order to replace their webpages with memorials to Swartz. The hacktivist collective also rallied Swartz's supporters to defend his funeral services from protesters and initiated a broad campaign to expose corruption in the judiciary. For my analysis, I will look primarily at the memorial sites dedicated to Swartz at the MIT and USSC websites. Secondarily, I will reference related

announcements posted at Pastebin where Anonymous coordinated its online operations with on-the-ground volunteers in defense of Swartz.

The Harvard fellow committed suicide on January 11th, 2013, and two days later, Anonymous took down MIT's website and dedicated a tribute to Swartz in its place. This installation shut down campus Internet access for over three hours Sunday evening and interrupted campus email for over ten hours. Additionally, MIT's backup emergency site was taken offline (McVeigh, 2013, Jan. 14). Entitled "In Memoriam, Aaron Swartz, November 8, 1986 – January 11, 2013, Requiescat in pace," Anonymous began its eulogy to Swartz thusly:

> Whether or not the government contributed to his suicide, the government's prosecution of Swartz was a grotesque miscarriage of justice, a distorted and perverse shadow of the justice that Aaron died fighting for — freeing the publicly-funded scientific literature from a publishing system that makes it inaccessible to most of those who paid for it — enabling the collective betterment of the world through the facilitation of sharing — an ideal that we should all support (In memoriam, 2013, Jan. 14).

In this first half of the first sentence, Anonymous makes use of many interesting metaphorical themes including justice, prosecution, and government. Probably the most easily recognizable metaphor here is the anthropomorphization of justice, a cultural phenomenon stemming from the oft-seen statue of a blindfolded woman holding aloft the scale of justice. This statue of "blind justice" is found at just about every courthouse around the country and is meant to symbolize the impartiality, objectivity, and fairness of justice.

The second half of the sentence makes reference to Swartz's activism and employs conceptual metaphors like freedom, scientific literature, publishing system, financial inaccessibility, and collective betterment. This is a direct response to the government's prosecution of Aaron Swartz for his alleged theft of digital data.

Next, Anonymous enumerates a list of demands for reforming copyright laws and calls for the return of the populist principles of the pre-digital era. The hacktivist collective makes an appeal for help for hackers suffering from similar political persecution (for example, Barrett Brown and Jeremy Hammond) and demands the overall reform of the judicial system, particularly the United States Sentencing Commission (USSC). Perhaps the gist of Anonymous's argument can be found in its last demand: "We call for this tragedy to be a basis for a renewed and unwavering commitment to a free and unfettered Internet spared from censorship with equality of access and franchise for all" (In memoriam, 2013, Jan. 14).

Hacker ethics for the prevention of online censorship and the right to freedom of information are once again on full display here. At the conclusion of its memorial on MIT's website, Anonymous paid open homage to the Internet prodigy: "Aaron, we will sorely miss your friendship, and your help in building a better world. May you read in peace. You were the best of us; may you yet bring out the best in us" (Ferenstein, 2013, Jan. 13).

But Anonymous did more than simply coordinate online political protests through its usual DDoS attacks on official websites. When the Westboro Baptist Church (WBC) announced that it would picket Swartz's funeral on January 15, Anonymous launched Operation Angel (#OpAngel). Never an organization to mince words, the WBC had entitled its press release "GOD H8S Cyber Criminal THUGS" and proclaimed, "Cyber criminals

are the latest face of this nation's and this world's raging at God and His Servants at WBC. Now the gloves are off, cyber rebels! ... We will picket the funeral, the LORD willing, so that in that Great Day of His Wrath, your blood is not on our hands" (Sieczkowski, 2013, Jan. 16). Despite rallying volunteers to defend Swartz's funeral in what could have potentially developed into a fractious confrontation, Anonymous remained heedful of his friends and family. They issued a preliminary apology at Pastebin:

> Before discussing the operation, there is something that needs to be said to Aaron's family and his friends: We're sorry. It is likely that our continuous condemnation and attacks against this cult is the very reason Aaron is being targeted by them. We would do anything to stop them from attending Aaron's services. Aaron deserves peace and we will not allow this cult to overpower what should be the media's focus, the monsters at DOJ who ruthlessly targeted your son.
>
> We encourage organizations who would like to form protective human shields near Aaron's funeral to listen closely for any announcement by the family on this action and respect their wishes (Anonymous, 2013, Jan. 13).

When Operation Angel volunteers showed up at Swartz's funeral to protect funeral-goers from picketers, WBC officials contacted police to inform them that they would not be in attendance at Swartz's funeral after all (Sieczkowski, 2013, Jan. 16).

The first phase of Operation Angel had been a success. The second phase of the operation was more ambitious: "Anonymous is now preparing for a longer and more extensive battle within the U.S. legal system" (Anonymous, 2013, Jan. 17). Toward that end,

Anonymous promised to hack the United States Sentencing Commission's website in order to draw attention to its harsh sentencing guidelines and to demand reform of the Computer Fraud and Abuse Act (CFFA). Dubbed Operation Last Resort (#OpLastResort), the second phase of their attack included other hackers within its scope, in particular Barrett Brown who, like Swartz, was a hacktivist prosecuted by the federal government for possession of information that violated its prescription for data security (McAfee Labs, 2013, Jan. 27). In Brown's case, he was implicated along with other hackers (including Jeremy Hammond) for disclosing Stratfor as a private intelligence agency subcontracted by the NSA. Hammond hacked the information from Stratfor's site and uploaded it to WikiLeaks. For this he received a ten-year prison sentence. Brown linked to Hammond's information via a chat room and received a four-year prison sentence. Brown was released to a halfway house in his home state of Texas in 2016 and has since signed a lucrative book deal with Farrar, Strauss, and Giroux. (Greenberg, 2016, Dec. 16). However, he was picked up by authorities again on April 27, 2017, a day before a scheduled interview with PBS (Emmons, 2017, April 27). Interestingly, both Brown and Hammond have been accused of being members of LulzSec though Brown denies it.

Hacker ethics fueled Anonymous' campaign to expose the unjust sentencing of Swartz and Brown. In the case of Swartz, this was due in part to his efforts to defeat SOPA/PIPA, a campaign promoted by Anonymous and many other hackers and hacktivists. Swartz and his colleagues at Demand Progress played a significant role in spearheading the SOPA/PIPA campaign, but it was a broad coalition of hacktivists who eventually took part in the bill's defeat including Anonymous itself. In an article entitled "Geeks are the New Guardians of our Civil Liberties" (2013, Feb. 4) appearing in MIT's *Technology Review*, Coleman has

observed that, "The [SOPA/PIPA] victory hinged on its broad base of support cultivated by hackers and geeks. The participation of corporate giants like Google, respected Internet personalities like Jimmy Wales, and the civil liberties organization EFF was crucial to its success. But the geek and hacker contingent was palpably present, and included, of course, Anonymous" (Coleman, 2013, Feb. 4).

In *Coding Freedom* (2013), Coleman has defined hackers as "computer aficionados driven by an inquisitive passion for tinkering and learning technical systems, and frequently committed to an ethical version of information freedom" (p. 3). She looks at how the free and open source software (F/OSS) of the 70s and 80s furthered the development of the Internet in the 90s. Under the banner of a General Public License (GPL) mandating that non-proprietary software like Unix, GNU, and Linux be made freely available to all, hacker ethics originate with the Internet itself, thus putting them on a collision course with commercial interests on the Net.

Swartz's hacker ethics meant that he was recognized as the ideological brother of Anonymous and so it was only natural that the hacktivist collective would have targeted the United States Sentencing Commission (USSC) in his defense. An independent branch of the judiciary appointed by the president and the legislature, the USSC was created under the Sentencing Reform Act and Comprehensive Crime Control Act of 1984. Its significance lies in the fact that not only is it an unelected position, it has essentially replaced the indeterminate sentencing model previously practiced by judges and parole boards with a determinate sentencing model controlled by prosecutors. More than one hacker has been a victim of the punitive dictates of the sentencing guidelines and this probably accounts for the reason that the USSC's guidelines were brought up repeatedly by different individuals in

the Swartz case including his mentor Lawrence Lessig and Anonymous itself.

As previously mentioned, Anonymous decried the USSC and called for an all-out war against it. In order to back Operation Last Resort, Anonymous planned in-the-street protests in Washington D.C. and Boston, and offered congresswoman Zoe Lofgren a chance to speak about her measure to reform the CFFA at the Washington protest (Anonymous, 2013, Jan. 17). Accordingly, on Friday, January 25, 2013, Anonymous hacked into the U.S. Sentencing Commission website and replaced its homepage with a YouTube video (KevinTx., 2013, Sept. 23). The video, entitled *Anonymous Operation Last Resort* (@OpLastResort), harshly criticized DOJ prosecutors and questioned the merits of an American judicial system based on mandatory minimums for convicted hackers, a direct reference to the USSC's sentencing guidelines. Authorities regained control over the website on Saturday, but the website was hacked a second time on Sunday, January 27. For the second attack, Anonymous posted instructions for how to use a flash-based, Konami-coded game (similar to an earlier video game called Asteroids) in which people could launch cartoon missiles at the DOJ's online text in order to reveal a Guy Fawkes mask – the signature face of Anonymous (Limer, 2013, Jan, 26). Natasha Lennard of Salon has reported, "In targeting the Sentencing Commission site, hackers symbolically took aim at a justice system wherein minimum sentencing laws put undue power in the hands of government prosecutors, who can exact guilty pleas from suspects afraid of facing hefty jail sentences at trial" (Lennard, 2013, Jan. 28).

But the crux of Operation Last Resort was its intention to release "warheads" containing sensitive information about the DOJ. In its video post on the DOJ's website, Anonymous outlined its plan for Operation Last Resort.

We have enough fissile material for multiple warheads. Today we are launching the first of these. Operation Last Resort has begun...

Warhead - U S - D O J - L E A - 2013 . A E E 256 is primed and armed. It has been quietly distributed to numerous mirrors over the last few days and is available for download from this website now. We encourage all Anonymous to syndicate this file as widely as possible.

The contents are various and we won't ruin the speculation by revealing them. Suffice it to say, everyone has secrets, and some things are not meant to be public. At a regular interval commencing today, we will choose one media outlet and supply them with heavily redacted partial contents of the file. Any media outlets wishing to be eligible for this program must include within their reporting a means of secure communications.

We have not taken this action lightly, nor without consideration of the possible consequences. Should we be forced to reveal the trigger-key to this warhead, we understand that there will be collateral damage. We appreciate that many who work within the justice system believe in those principles that it has lost, corrupted, or abandoned, that they do not bear the full responsibility for the damages caused by their occupation.

It is our hope that this warhead need never be detonated (Kessler, 2013, Jan. 26).

On February 3, 2013, Anonymous also hacked the Alabama Criminal Justice

Information Center where it posted the contact information for over 4,000 U.S. banking officials. Anonymous claimed to have gotten the information from Federal Reserve computers, which greatly alarmed authorities. On February 18, it hacked the website of George K. Baum and Company and doxed many of the investment company's clients. Anonymous also revealed the company's ties to Stratfor, the previously mentioned intelligence firm that has been dubbed "the shadow CIA" (Blue, 2013, Feb. 19). It should be noted that the ongoing collusion of private investment firms with intelligence agencies had already been revealed in 2012 when WikiLeaks exposed the connections between Goldman Sachs and Stratfor - not to mention Bamford's revelation of the NSA spying on French airline companies competing with American firms for European contracts in the 1970s (Bamford, 1982, *The Puzzle Palace*).

Figure 9. Anonymous's Logo

Swartz and others in the hacker brotherhood have recourse to a shared cyberculture replete with philosophical principles. Perhaps the embodiment of hacker ethics can be found in the person of Richard Stallman, writer of the *GNU Manifesto* and founder of the Free

Software Foundation. Based on the golden rule "that if I like a program, I must share it with other people who like it" (Coleman, 2013, p. 18), Stallman championed the populist ethos of "cooperation, community, and solidarity" so valued among hackers (p. 44). These ideals would eventually evolve into the hacker tenet that computer code is free speech, the ideological antithesis of international trade associations bent on enforcing intellectual property rights on the World Wide Web (Coleman, 2013, p. 71).

In order to demonstrate the importance of hacker ethics, a little background history on their role in developing the original Internet is in order. The Bulletin Board System (BBS) was an early form of the Net where hackers chatted, played games, shared programming tips, and formed DIY collaboratives. Out of such early online communities arose hacker conferences like Hackers on Planet Earth (HOPE), which was founded in 1994 in part to promote awareness of the legal travails of Kevin Mitnick (Coleman, 2013, p. 16). Even though the hacker never profited from his sojourns onto restricted computers, Mitnick had hacked too many of them to avoid serving time. When he wasn't behind bars he was on the run from authorities. In one of his early Robin-Hood style escapades, Mitnick used a hole-puncher to distribute free bus transfers from the Los Angeles Rapid Transit District. Stories of such hacker transgressions are common fare at conferences like HOPE and Swartz would have been no stranger to them.

Indeed, the same month Swartz committed suicide another hacker was being similarly prosecuted under the terms of the CFAA. Arrested in November of 2012 for doxing the email addresses of over 114,000 AT&T customers, notorious hacker and troll, Andrew "Weev" Auernheimer, had committed his act of content liberation with the goal to embarrass the telecommunications giant into fixing its security leaks. In response, the

government charged Auernheimer with breaking into a protected computer and stealing customer identities, a crime carrying up to ten years in prison. He was commanded to apologize.

> In a 'statement of responsibility' published on Monday in a response to a request from the government that he accept responsibility before sentencing, Auernheimer wrote: 'Ivy-League educated and wealthy, Aaron dealt with his indictment so badly because he thought he was part of a special class of people that this didn't happen to. I am from a rundown shack in Arkansas. I spent many years thinking people from families like his got better treatment than me. Now I realize the truth: The beast is so monstrous it will devour us all. None will be spared' (McVeigh, 2013, Jan. 24).

F. Aaron's Law

The sixth and final text I will look at is a bill known as the Aaron's Law Act of 2013. Introduced by a bipartisan group of congressional Representatives, the legislation sought to reform the Computer Fraud and Abuse Act (CFAA) used to prosecute Swartz. Representative Zoe Lofgren (D-CA), the chief sponsor for H.R. 2454, was joined by Representatives James Sensenbrenner (R-WI), Mike Doyle (D-PA), Yvette Clarke (D-NY), and Jared Polis (D-CO) in presenting the bill to the House Judiciary Committee (*Wikipedia*, n.d., "Representative Zoe Lofgren").

According to Dr. Gabriella Coleman, "the US has historically been tougher on hackers than other countries" (McVeigh, 2013, Jan. 24). In an article appearing in *MIT Technology Review* (2013), Coleman points out that despite the hacktivist victory over SOPA/PIPA,

"federal authorities orchestrated the takedown of the popular file-sharing site Megaupload [in the same month]. The company's gregarious and controversial founder Kim Dotcom was also arrested in a dramatic early morning raid in New Zealand" (Coleman, 2013b). Using the Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO-IP Act) – legislation that created a new executive arm for the enforcement of intellectual property rights along with expanded punishment for secondary data theft – the Department of Justice (DOJ) charged Kim Dotcom with copyright violation, racketeering, and money laundering.

Figure 10. The FBI Takes Down Megaupload's Website

Following as it did on the heels of the defeat of SOPA/PIPA, suspicions abounded over the timing of Kim Dotcom's high-profile arrest.

> But the decision by the Justice Department to net such a big, obvious fish at this time raised eyebrows among the internet cognoscenti, who posited that it was meant as a retort to populist digital forces that amassed in protest of the fast-tracking of two anti-piracy bills, the Stop Online Piracy Act (SOPA) and Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA) (Jonsson, 2012, Jan. 21).

The saga of Kim Dotcom (a.k.a. Kim Schmitz, a German citizen) and his company Megaupload illustrates the increasingly expansive nature of U.S. copyright laws especially in regards to non-U.S. citizens. Megaupload was a Hong Kong-based file sharing website similar to Napster. With millions of subscribers from all over the world, users of the site enjoyed cloud storage services for their digital files. At the height of its popularity, Megaupload accounted for 4% of all web traffic (Wikipedia, n.d., "Kim Dotcom"). Nevertheless, The FBI and DOJ indicted Dotcom in his home country of New Zealand and seized millions of dollars of his assets for alleged copyright infringement. When it was revealed that the government had been illegally spying on him prior to his arrest, Dotcom sued for damages. A friend of fellow hacker and hacktivist, Julian Assange, Kim Dotcom has since accused the Obama administration of teaming up with New Zealand prime minister, John Key, and CEO of the Motion Picture Association of America (MPAA), Chris Dodd, to target him for his early career as a hacker and hacktivist (Bennett, 2012, Oct. 2).

Much like the DOJ's prosecution of Swartz, the U.S. government's case against Dotcom hinges on the question of intention. The DOJ has charged Megaupload with knowingly allowing its subscribers to share copyrighted materials over its site in order to garner profits.

Lawyers for Megaupload have responded that the terms of the Digital Millennium Copyright Act (DMCA) do not hold Internet companies liable for the contents of their subscriber's accounts and that all subscribers are required to sign a terms and conditions of use contract agreeing not to share copyrighted materials over the site. They also point to privacy laws that protect customer's accounts. In 2015, Kim Dotcom lost an appeal to keep his case in New Zealand and now faces extradition to the U.S. Speculation abounds concerning the fate of the file-hosting site and the conventional wisdom holds that Dotcom's case will drag on for years before winding up before the U.S. Supreme Court.

Like the DMCA, the CFAA is a law governing the user's connection to the Internet. While it might seem like a trivial point, the question of *connection* lies at the heart of the debate over authorized access to computers and the Internet, and it was pivotal to the development of the prosecution's case against Swartz. Nevertheless, the "Prosecuting Computer Crimes" manual published by the Office of Legal Education Executive Office has acknowledged that it can be very difficult to prove whether someone with authorized access can be accused of unfairly connecting to a computer after the fact.

> A more difficult question is whether a person with some authorization to access a computer can ever act "without authorization" with respect to that computer. The case law on this issue is muddy, but, as discussed below, there is growing consensus that such "insiders" cannot act "without authorization" unless and until their authorization to access the computer is rescinded (Office of Legal Education, n.d., pg. 6).

It boils down to a question of access versus *manner* of access and this issue was critical in the prosecution's attempt to build a case against Swartz (Abelson, et al, 2013, p. 138). Indeed, it can be seen that the tension between conflicting interpretations over manner of access to the Internet is one that stems from the evolution of the metaphors used to describe digital connections in the past forty years. For example, one of the first metaphors for the Internet is contained within its name – the "Net" – since it was at first primarily perceived as a network of computer connections. The original idea of computers as connections to networks had much to do with the fact that early computers were linked through a system of telephone lines. Bruce Sterling's description of the emergent Internet in *The Hacker Crackdown* (1992) draws attention to this fact:

> Cyberspace is the 'place' where a telephone conversation appears to occur. Not inside your actual phone, the plastic device on your desk. Not inside the other person's phone, in some other city. The place between the phones. [...] in the past twenty years, this electrical 'space,' which was once thin and dark and one-dimensional—little more than a narrow speaking-tube, stretching from phone to phone—has flung itself open like a gigantic jack-in-the-box. Light has flooded upon it, the eerie light of the glowing computer screen. This dark electric netherworld has become a vast flowering electronic landscape. Since the 1960s, the world of the telephone has cross-bred itself with computers and television, and though there is still no substance to cyberspace, nothing you can handle, it has a strange kind of physicality now. It makes good sense today to talk of cyberspace as a place all its own (Introduction to *The Hacker Crackdown*, 1992).

As Sterling notes above, the metaphor of connectivity evolved into the notion of the

Internet as a form of cyber "space" where digital information could be shared and stored in data banks and data clouds. From there the metaphor for the Internet has gone on to be regarded as a "pipeline" for conveying digital content sold as broadband width by cable providers. Former Vice President Al Gore further transmogrified its terrain with the debate over Net Neutrality and the introduction of the possibility of tollbooths on the "information superhighway". The most recent metamorphosis of the Internet's linguistic frame is one that entails information as "intellectual property" secured behind paywalls. This latter metaphor has been used to question whether or not Swartz had authorized access to MIT's computer networks.

According to the DOJ's manual for prosecuting computer crimes, the CFAA has developed in response to the growth of computer and Internet fraud. "As computer crimes continued to grow in sophistication and as prosecutors gained experience with the CFAA, the CFAA required further amending, which Congress did in 1988, 1989, 1990, 1994, 1996, 2001, 2002, and 2008." (Office of Legal Education Executive Office, n.d., p. 2). However, the CFAA also charts the trajectory of the increasingly harsh penalties of the U.S. government for intellectual property theft. An example of the expansion of the legal theory for copyright infringement can be found in the casebook study of David LaMacchia, an MIT student accused of copyright violation in 1994. Like Swartz, LaMacchia had been caught downloading copyrighted materials on MIT computers. In LaMacchia's case, he had downloaded copyrighted computer games and software applications and encouraged others to join him in his activities. He initially faced charges for exceeding authorized access under the terms of the CFAA, the same clause to later plague Aaron Swartz. However in 1994, noncommercial copyright violation was not yet a criminal act and LaMacchia had not

profited from any of his downloads. When the case against him was dismissed it was dubbed the LaMacchia Loophole. Federal Judge Richard Stearns, who wrote the legal analysis for LaMacchia's trial, encouraged legislators to close it. In response, lawmakers passed the No Electronic Theft Act making copyright infringement a felony offense even in cases where no profit is derived.

At this juncture it is useful to foreground the Comprehensive Crime Control Act of 1984 in order to understand the trajectory of copyright law on the World Wide Web. Introduced under the Comprehensive Crime Control Act of 1984, the CFAA originated out of Title 18 of United States Code section 1030. The Comprehensive Crime Control Act represents one of the first serious overhauls of criminal law since the early twentieth century and it also established the United States Sentencing Commission (USSC). As previously mentioned, the USSC has ramped up many misdemeanor offenses to felony offenses, and has also conflated some aspects of civil and criminal law. The latter is perhaps most noticeable in the legal theory surrounding copyright. When U.S. code 1030 was amended in 1986, it was dubbed the Computer Fraud and Abuse Act (CFAA). Though the CFAA has been greatly expanded over the years, Aaron's Law represents the first serious attempt to rein it in.

Unfortunately, Aaron's Law failed in 2014 and was subsequently reintroduced in 2015. The sponsor of the second attempt to pass the bill was, again, Representative Zoe Lofgren (D-CA), but this time with Senate cosponsors Ron Wyden (D-OR), Rand Paul (R-KY), and Jim Sensenbrenner (R-WI) (Cohn, 2015, April 29). Much like its earlier incarnation, the bill has languished in the house judiciary committee where it again appears doubtful it will pass (Reader, 2016, Jan. 11).

Many critics of the CFAA have argued that it is too broad, that it is outdated, and that it has resulted in harsh sentencing by turning what would otherwise be misdemeanor offenses into felonies. In a press release issued by Senator Wyden on April 21, 2015, the Senator referred to the discovery that the NSA was spying on legislators when he declared, "Violating a smartphone app's terms of service or sharing academic articles should not be punished more harshly than a government agency hacking into Senate files. The CFAA is so inconsistently and capriciously applied it results in misguided, heavy-handed prosecution. Aaron's Law would curb this abuse while still preserving the tools needed to prosecute malicious attacks" (Senate Website for Wyden, 2015, April 21). In the same press release, Congresswoman Lofgren maintained, "At its very core, CFAA is an anti-hacking law. Unfortunately, over time we have seen prosecutors broadening the intent of the act, handing out inordinately severe criminal penalties for less-than-serious violations**.** It's time we reformed this law to better focus on truly malicious hackers and bad actors, and away from common computer and Internet activities" (Senate Website for Wyden, 2015, April 21).

Oren Kerr, a professor of computer and criminal law, has similarly pointed out that "felony liability under the statute is triggered much too easily." (Kerr, January 27, 2013). Other critics of the CFAA object to the law's vagueness with regard to violations of terms of use rules, employer agreements, or website notices (Lofgren, 2013, June 20). They claim the law is too broad and that it turns trivial offenses like "lying about your age on Facebook or checking personal email on a work computer" into potential criminal felonies (Lofgren & Wyden, 2013, June 20).

Perhaps the vagaries of the CFAA are most clearly illustrated in another high profile hacker case garnering national headlines in 2012: the Steubenville rape case. Derric

Lostutter and Noah McHugh were the Anonymous hackers behind the exposure of what they dubbed "the rape crew" on the Steubenville football team. Several members of the team participated in the sexual assault of an unconscious sixteen-year-old girl at a party and posted it on their social media. When the victim discovered pictures of herself being shared by classmates the next day via Twitter she contacted police. This prompted party-goers to take down their posts. However, Alexandria Goddard, who runs a crime blog, had already downloaded many of the initial tweets about the assault and had re-posted them on her own website at Prinniefied.com. When one of the members of the football team threatened to sue her, she was forced to take the pictures down again. She contacted Lostutter who hacked into a Steubenville football fan website and posted them there. Despite attempts to cover up the case by the local judge, city prosecutor, school administrators, and teammates, two members of the Steubenville football team were eventually charged with rape. Ma'lik Richmond served ten months in a juvenile detention facility while Trent Mays served two years. In the meantime, Lostutter had become the target of an FBI investigation for his role in posting information about the assault on the football fan website. He currently faces a ten to sixteen year prison sentence for violating the CFAA. Lostutter summarized his prosecution under its terms thusly: "You get 16 years for forcibly entering your way into a computer, but you get one year for forcibly entering your way into a woman. I think that's the precedent the government is setting here" (Vandita, 2016, Sept. 11).

One of the purposes of Aaron's Law Act of 2015 is to amend the CFAA in order "to provide for clarification as to the meaning of access without authorization" (Aaron's Law Act of 2015). The amended law will clearly lay out the criteria for what constitutes unauthorized access to a computer by changing the phrase "unauthorized access" to read

instead, “access without authorization means to obtain information on a protected computer that the accesser lacks authorization to obtain by knowingly circumventing one or more technological or physical measures that are designed to exclude or prevent unauthorized individuals from obtaining that information’’ (Aaron’s Law Act of 2015). The idea is to establish “that breaches of terms of service, employment agreements, or contracts are not automatic violations of the CFAA” (Senate Website for Wyden, R., 2015, April 21). As already mentioned, the government’s case against Swartz pivoted on the question of the manner in which he had accessed MIT’s computers while a guest user at the college. According to MIT’s report, the government prosecutor attacked Swartz for his circumvention of the normal procedures for downloading materials over the Internet but failed to address the fact that he was, indeed, a legitimate guest user of MIT’s networks. “Aaron Swartz was authorized to access the network, regardless of whether he used improper means to do so” (Abelson, et al., 2013, p. 137). Indeed, the university appeared to regret its lack of assertion on this point and mused over its role as an institution of higher education confronting the government’s role as an enforcer of copyright laws.

> [T]he CFAA has the effect of transforming minor violations of very broad service terms from a contractual issue (often never intended to preclude research) into a potential federal felony. This creates a chilling effect on important research and puts MIT in the awkward position of determining what is a felony based on its choice of the terms in its TOS [terms of service]....University rules of access are not designed for the purpose of defining the predicates for criminal prosecutions. Forcing them into this role impedes the university’s ability to support open access and innovation

(Abelson, et al., 2013, pp. 94 – 95).

Another purpose of Aaron's Law is the elimination of redundant charges. Limiting the prosecutor's ability to inflate the penalties by "stacking multiple charges" for essentially the same offense will make punishments more proportional to the crime (Lofgren, 2013, June 20). According to MIT's analysis of Swartz's sentence, Heymann was able to increase the original four felony charges to thirteen by simply re-interpreting the same offense in different ways, thereby charging Swartz multiple times for the same offense.

> Essentially, the superseding indictment took the four counts from the initial indictment and broke each of them into multiple counts, by charging Aaron Swartz's alleged conduct (as related to each of the four legal theories of liability) as discrete events in place of being merged into single allegations of liability. Also, the theory of liability for the final count, alleging damage to a protected computer, was expanded.
>
> One effect of these charging decisions was to—theoretically—increase the maximum penalties to which Aaron Swartz might be subject from 35 years to 95 years imprisonment; and from $1 million to $3 million in fines (Abelson, et al., 2013, p. 39).

This meant that though Swartz was originally indicted on July 14, 2011, with one count of wire fraud and three violations of the CFAA for a total of four felonies, Heymann's superseding indictment on September 12, 2012, broke each of these four counts down into further discrete violations to include "two counts of wire fraud and 11 counts of violating the

CFAA" (Abelson, et al., 2013, p. 38). This left Swartz facing up to thirteen separate felonies and ninety-five years in prison, a significant expansion of the punitive force of the original indictment

In its footnotes, MIT has commented:

> It is important to the fair and efficient administration of justice in the Federal system that the government bring as few charges as are necessary to ensure that justice is done. The bringing of unnecessary charges not only complicates and prolongs trials, it constitutes an excessive—and potentially unfair—exercise of power" (p. 38).

Indeed, Representative Darrell Issa has remarked on the ethicality of inflating charges in order to force the defendant into a plea bargain.

> I'll make a risky statement here: Overprosecution is a tool often used to get people to plead guilty rather than risk sentencing… It is a tool of question. If someone is genuinely guilty of something and you bring them up on charges, that's fine. But throw the book at them and find all kinds of charges and cobble them together so that they'll plea to a 'lesser included' is a technique that I think can sometimes be inappropriately used (Reilly, et al., 2013, Jan. 15).

In point of fact, other nations recognize its coercive potential for abuse and prohibit the use of plea-bargaining altogether.

The text of Aaron's Law is evocative of nearly all of the thematic elements to do with the struggle for freedom of information and open access to the Internet. The explanatory opening of the bill – "To amend title 18, United States Code, to provide for clarification as

to the meaning of access without authorization" – points up the dispute over who has access to information, under what conditions, and with what social outcomes (Aaron's Law Act of 2015). The linguistic frames of "access without authorization" or "exceeding authorized access" highlights the significance of the user's manner of connection to the Internet when accepting a website's terms of service. As already noted, clickthrough contracts can incriminate any number of harmless Internet activities. Aaron Swartz addressed this issue in his writings on free culture. In a piece entitled "UTI Interview with Aaron Swartz," he has contended that, "no one reads those licenses and they put all sorts of absurd things in there" (2015, p. 14). He elaborates on the point musing, "When you're forced to follow laws passed by a government of the people, that's one thing, but when you have to follow all sorts of additional restrictions added by some unaccountable corporation, it's quite a different situation. What if they make you promise not to say anything negative about their software, as Google almost tried to do? What if they ask for your firstborn son? No one will actually know they agreed to these provisions, because they didn't read them – they just wanted to use the software they spent their own money to purchase – but they'll be held accountable for violating them" (2015, p. 14).

Clickthrough contracts come down to a question of contract law. When looked at as a linguistic framing device, a contract can be seen as a speech act that formalizes an agreement between two people. As already noted, speech acts are epistemological frames. The violation of a software license or a website's terms of service are forms of contract disputes that used to fall within the jurisprudence of civil law. In the past, judgments against the defendant were typically resolved by paying restitution to the plaintiff. However, as the trajectory of digital copyright law has revealed in the cases of Kim Dotcom and David

LaMacchia, copyright infringement increasingly falls within the jurisprudence of criminal law. The conflation of what were once two distinct areas of legal theory has proven problematic to some judges particularly with regard to punishment for secondary copyright infringement. Secondary or indirect copyright infringement is the idea that a primary party who provides intermediary access to the Internet to another party is nevertheless legally liable for the second party's act of copyright violation. Internet service providers and software distributors are just two of those who might be on the hook for the copyright violations of their clients under this interpretation of the law. New Zealand judge David Harvey raised the issue when he wrote an initial ruling in favor of Megaupload musing that the DOJ was confusing civil law with criminal law in cases of indirect copyright infringement and that this was being unfairly used to prosecute Kim Dotcom.

The violation of an agreement to connect to the Internet in a specified manner by accepting a provider's terms of service is one that raises an interesting question: How does the Internet modify previous understandings of contract law? How does this new digital medium make harsher legal punishments possible in cases of alleged intellectual property theft? Adequately defining legal contracts is a necessary precursor for the enforcement of copyright law but the metaphorical dimensions of the Internet play a largely unrecognized role in this dispute. Because associated frames and metaphors for thought, communication, and learning are so deeply embedded in our explanations for cognition, we often do not realize that we are applying them to our functional descriptions of the Internet itself. The fact that we are largely unconscious of the embedded metaphors that inform our understandings of the Net means that we are also unaware of the misunderstandings they create.

As already mentioned, the evolution of our metaphors for describing the operations of the Internet is one that has developed from the idea of a "network of connections" to one of "data storage." From there it has further evolved into the idea of data conduits of variable speed and delivery and thence to one of paywalled data secured for profit by its owners. While the metaphor of "network connection" is the one favored by the original Netizens – the hackers and computer geeks who collectively helped build the World Wide Web – the metaphor of "data content" is the one favored by international trade associations and giant media conglomerates. The latter's objectification of data guarantees intellectual property rights on the Internet through the enforcement of contracts even though Netizens are largely unaware of what they are signing when they accept a company's terms of service agreement.

If the devil is in the details, then clickthrough contracts are perhaps the Internet's own version of the Faustian bargain. The irony that Aaron Swartz would be brought down by something so negligible could not have been lost on the Internet's own boy.

VI. The Conduit Metaphor Writ Large

Cognitive linguists argue that language and cognition are virtually synonymous. In *Metaphors We Live By* (1980), Lakoff and Johnson have shown that more than flowery figures of language, metaphor plays a fundamental role in human cognition. Since they "unite reason and imagination" (p. 193), metaphorical concepts engage what Lakoff and Johnson call Imaginative Rationality. Imaginative Rationality helps generate the metaphors that enable reasoning. As important to science as it is poetry, the Imaginative Rationality of conceptual metaphor facilitates the development of theories and hypotheses necessary to understanding our world. It also implicates attitudes, values, and ideologies. Because conceptual metaphors are techniques for symbolizing and organizing concepts that support the interpretation of information and facilitate meaning-making about our world, metaphors are functionally epistemic in nature. In fact, the systematicity of metaphors means they can function as a kind of heuristic device for problem solving. A heuristic is a mode of inquiry – a methodology – for analyzing a given subject. Metaphors and heuristics are shorthand forms of thinking that facilitate comprehension through the creation of representational models that bridge concepts and realities. By and large, metaphors for the Internet are dominated by allegories of cognitive and communicative interactions that take a decidedly socio-epistemic stance on the form, meaning, and function of the Net. The dispute over competing metaphors to describe the Internet brings into sharp relief an emergent theory of knowledge in cyberspace.

Sally Wyatt (2004) has noted in her article, "Danger! Metaphors at Work in Economics, Geophysiology, and the Internet," "[I]t is … important to think about metaphors of the

Internet not only because they reveal what different actors think it is but also because they tell us something about what they want it to become" (pp. 244 - 245). This is especially true of the debate over freedom of information on the Internet. If, as Lakoff and Johnson suggest, metaphors orientate us to a particular reality, then the dispute between hackers/hacktivists and government/corporations might stem from their very different epistemological aspirations on the World Wide Web. Metaphors and their associated linguistic frames reveal a predisposed ideological orientation that when applied to the Internet, predicates a particular social epistemology. A close examination of the goals of the disputants as expressed through their use of metaphor might reveal their intentions with regard to the social construction of knowledge on the Web.

The network depiction of the Internet is based on the freedom to connect while a data orientated depiction is not. A network metaphor places value on a hacker ethic of sharing, collaborating, and learning while a data metaphor places value on a corporate doctrine of bartering, marketing, and hoarding. The open and expansive connection to knowledge and information espoused by hackers, hacktivists, and civil libertarians is at direct odds with the more narrow and restrictive one espoused by governments and corporations. Indeed, the manner of objectifying information favored by big media giants and trade associations in order to maximize profits on the Internet has steadily eroded the digital materials available for fair use in the public domain.

Hackers/hacktivsts value sharing information as though it were "a banquet of knowledge" and emphasize abundance, research, and free expression. On the other hand, government/corporations value restricting information as though it were "intellectual property" and emphasize scarcity, profit, and control. A hacker ethic for the free exchange

of information draws on associated frames of transparency, openness, and freedom. Such an ethic stands in marked contrast to a government/corporate stance for controlling information based on associated frames of secrecy, containment, and restriction.

The metaphors – or heuristic devices – used by government/corporations to frame notions of "data," "intellectual property," and "knowledge economy" support their ideological stances for the proscription of social epistemology in cyberspace. Based as they are on ideologies of profit and control, these metaphors will shape the meaning and purpose of the Internet in a narrow fashion that fosters scarcity and secrecy. On the other hand, the heuristic frames used by hackers/hacktivists to represent ideas of "connection," "intellectual repast," and "knowledge ecology" support their ideological stances in favor of an unhampered social epistemology in cyberspace. Based as they are on ideologies of sharing and collaborating, hacker/hacktivist metaphors shape the meaning and purpose of the Internet in an expansive fashion that fosters abundance and transparency. A hacker ethic that places value on freedom of information, freedom from censorship, and the right to privacy on the World Wide Web is one that recognizes the fundamental importance of digital rights and the free development of social epistemology for Netizens.

There can be little doubt that the Internet as a medium of publication and communication has significantly changed the idea of intellectual property rights in the digital age. While both hackers/hacktivists and government/corporations possess ideologies that reify information, there are nevertheless important differences in how they do so. Because of the systematicity of metaphors favoring certain types of interpretations over others, metaphorical concepts "can hide an aspect of our experience" and make us believe that they are "so much the conventional way of thinking…that it is sometimes hard to imagine that

[they] might not fit reality" (Lakoff & Johnson, 1980, p. 10 - 11). Rather than recognizing them for what they are – representational models for reality – such metaphors become so embedded in our epistemic frameworks that we are not even aware of them anymore. Instead they become established truisms and articles of faith that preclude our ability to entertain alternative ideas about the social construction of knowledge in the Information Age.

As an example of this tendency, government and corporate authorities necessarily deselect metaphors of social relationships in the construction of knowledge in order to objectify *data* on the Internet. The idea that intellectual property contains information irrespective of any larger social context is one that precludes the possibility for recognizing the mutually shared aspects of human meaning-making (1980, p. 11). Not so hackers and hacktivists. They select metaphors for social relationships in the construction of knowledge in order to objectify *connections* on the World Wide Web. While they are nevertheless objectifying an abstraction, hacktivists do so in order to recognize the important social dimension of individual acts of cognition in a process of collective meaning-making.

Whether a data-oriented or a connection-oriented depiction of the Internet, one of them presents a more elegant interpretation of the purpose of the Internet when looked at from the point of view of Occam's Razor. Occam's Razor is a heuristic that holds that a simple and direct approach to solving a problem is better than a complicated one. If metaphors demonstrate the attitudes and values of antagonists over the form and purpose of the Internet, an epistemological stance that favors *sharing* information as though it were intellectual sustenance is one that signifies a humanistic attitude for the social construction of knowledge. On the other hand, an epistemological stance that favors *selling* information

as though it were intellectual property is one that denotes a corporate attitude toward social epistemology. According to the dictates of Occam's Razor, a heuristic with fewer parts is more desirable than a complex one. Of the two approaches to the social construction of knowledge – either sharing it or selling it – the hacker predisposition for sharing information makes for a direct one-to-one connection between individuals on the World Wide Web. This stands in contrast to the government/corporate predilection for selling information on the Internet, which necessitates the insertion of a middleman between individuals. By injecting a third party into the normal communications between individuals in the form of a government or business intermediary, the metaphor of "intellectual property" defies Occam's Razor and inhibits the meeting of minds in cyberspace. In short, the authorized agent required by government/corporations acting to regulate information on the Internet violates the simplicity of Occam's Razor. In proprietizing acts of cognition, a profit-motivated heuristic conceals the cooperative aspects of a social epistemology in cyberspace. This is perhaps the crux of the dispute between hackers/hacktivists and digital rights activists on the one hand, and government/corporations on the other. Hackers/hacktivists and their advocates favor direct people-to-people connections on the Net to facilitate maximum knowledge exchange while government/corporations favor mediated connections that control and commercialize the content of data on the Net. One takes a socio-epistemic approach to the Internet for the benefit of research, collaboration, and free expression for all while the other takes a social control approach to the Net to ensure the securitization and monetization of information for profit by the few.

Hence, the struggle over the purpose of the Internet is at heart a struggle for the metaphor to frame it. Various studies that look at the linguistic framing of the Internet have

testified to the power of metaphor in constructing our interpretation, experience, and understanding of it. Lakoff and Johnson's (1980) treatise on the power of metaphor in everyday life demonstrates its important cognitive function as a representational model of reality that helps us interpret and understand the world around us. They have shown that because metaphors are a part of our cognitive processes, they actively shape and determine our reality.

> Metaphors may create realities for us, especially social realities. A metaphor may thus be a guide for future action. Such actions will, of course, fit the metaphor. This will, in turn, reinforce the power of the metaphor to make experience coherent. In this sense metaphors can become self-fulfilling prophecies (p. 156).

In a documentary film entitled *Das Netz* (2003), publishing entrepreneur John Brockman has this to say on the self-fulfilling nature of metaphors.

> Reality isn't this thing in front of us on a presidium stage; it's a moveable feast. We are creating technologies then we ARE the technologies. It's not your heart is *like* a pump. Your heart IS a pump. It's not your brain is *like* a computer. Your brain IS a computer until the next thing comes along. Now you're a neural net or now you're an information system (as cited in Dammbeck, 2003).

Brockman appreciation for the power of metaphors to frame our perceptions of technology is pleasantly utopianist, but he unwittingly touches on the dangers of the Net's

ability to create hyperreality. Jean Baudrillard and Michael Reddy address this subject further on when they look at the consequences of merging metaphor and reality for its affects on inducing the kind of amnesia of consciousness that precludes healthy skepticism.

In *Alternative and Activist New Media* (2011), Leah A. Lievrouw has also discussed the significance of competing metaphors for the Internet:

> From the days of the pre-browser internet of the 1970s and 1980s to today's Web 2.0, a tension has grown up between what I have called the competing *pipeline* and *frontier* visions of the internet and other new media systems (Lievrouw, 2006a, 2008). On one hand, the pipeline or center view sees traditional and new media alike as just so many "factories" for the manufacture and distribution of cultural products intended for consumption on an industrial scale. On the other hand, the frontier or edge view regards media more as venues for participation, speech, interaction, and creativity, and considers the vast and growing archive of media products and content as a trove of resources to be re-fashioned and re-presented by users "rummaging in the universal media archive…[where] all the data in the world…make up one lovely big amusement park" (Lovink, 1997, pg. 59). The pipeline view tends to see media technologies and content in terms of property and gatekeeping, production, and consumption; the frontier view is more likely to value reputation, credibility, creativity, reciprocity, voice, and trust as well as ownership, and to see media and information technologies as opportunities to create and communicate as well as consume. These contrasting views have helped to shape the popular understanding of the proper cultural and economic role of new media over the last three decades, as

> well as the technical design of the systems themselves. Disputes about what new media are for, who gets to use them, and who decides have set the stage for the current rise of alternative and activist new media projects (2011, p. 2).

Lievrouw's notion of the Internet as a space, terrain, or thing is a longstanding one. Some of our most common metaphors for the Internet represent it as a topography or object, including the aforementioned metaphors of frontier and pipeline. The Internet has long been characterized as a meeting place as depicted by the proliferation of virtual communities, villages, cafes, hotels, and parks on the World Wide Web. Other metaphors have presented it as a page, a net, a web, libraries, pneumatic tubes, digital commons, data clouds, an information superhighway, and a global brain.

Science fiction author William Gibson first coined the term "cyberspace" in his iconic novel *Neuromancer* (1984). He described it thusly:

> Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts … A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding (p. 67).

This is also where a topographical sense of the Internet perhaps first emerged so that it began to be described as a kind of "Wild West," a place where anything goes. Other metaphors have focused more on its cognitive sense by likening it to a virtual reality, a

global brain, a distributed information system, and a repository for all human knowledge. As Gibson has noted, the largely fictional environs of cyberspace are dependent on the kind of Imaginative Rationality that requires "the willing suspension of disbelief" for the Net's very existence as a social construct (Coleridge, 1802). In *Crime and Puzzlement* (1990), John Perry Barlow has described the symbolic nature of an early Internet prototype he dubbed the Well:

> In this silent world, all conversation is typed. To enter it, one forsakes both body and place and becomes a thing of words alone. You can see what your neighbors are saying (or recently said), but not what either they or their physical surroundings look like. Town meetings are continuous and discussions rage on everything from sexual kinks to depreciation schedules (Barlow, 1990, June 1).

As a large-scale metaphor for thinking and expression, The Internet is a conduit for thoughts, feelings, and ideas conveyed through electronic communications to a wired-in world Netizenry. In essence it is a giant conduit metaphor.

The conduit metaphor is an overarching heuristic of communication that while typically used to describe meta-language, is also applicable to the Internet itself. In some sense, it is the metaphysical antecedent to the Internet since it entails the idea that meaning is physically contained in symbols. The objectification of meaning and ideas inherent in the conduit metaphor are implicated in the very architecture of the Internet since computers at beginning and end points decode texts transmitted from senders to receivers. Reddy has stressed that, "the assumption that human communication achieves the physical transfer of

thoughts and feelings" creates a frame conflict where people assume that language holds meaning independent of any effort by communicators to avoid misunderstandings (1979, p. 287). His cautionary tale of the pitfalls of the conduit metaphor is nowhere more true than with the Internet.

Perhaps more importantly, the conduit metaphor is a useful reminder that the alchemy of Internet and reality occurs predominately in the minds of those who buy into it. The Internet is less an actual "place" called cyberspace than it is the Imaginary writ large, a kind of chemical wedding of mind and technology. While seductive, it is nevertheless necessary to occasionally step back and remind ourselves that much like the conduit metaphor, it is wholly symbolic and, in the words of Lakoff and Johnson, ultimately an engagement in Imaginative Rationality. At its best, the Internet serves as a tool for enabling the free expression and unrestricted knowledge expansion of utopian-minded hackers and hacktivists in a democratic world forum. At its worst, it becomes a tool of social control that compartmentalizes knowledge in the service of a dystopian world order of privileged elites. Science fiction author William Gibson has based most of his novels on the latter theme. The potentially mind-altering utopian/dystopian nature of this new media form is the largely unspoken subtext in any discussion about the next phase of its development: Artificial Intelligence (AI).

As an early thought experiment on computer intelligence developed by Alan Turing, the Turing Test sought to discover if there were any distinguishable differences between human intelligence and computer intelligence. In the Turing Test, an experimenter asks a tester to sit in a room apart from a second person and a computer. All three parties are ensconced in separate rooms so that none are able to see the other. The purpose of the experiment is for

the tester to guess the respective identities of the other two by asking them a series of questions. Questions and answers are conducted between the rooms via a tele-printer to ensure that the tester has no other means to verify the identities of the respondents except by their written communications. With nothing more than texts as clues, the tester is tasked with ascertaining whether or not they are talking to a computer or another human being. In this manner, Turing sought to reformulate the question, "Can machines think?" to one of "Can machines *imitate* thinking" well enough to deceive a human judge? (Turing, 2003, p. 50).

Computers that write have long been the ambition of linguists, educators, computer scientists, and AI theoreticians interested in studying the links between human and machine cognition. In hopes of teaching computers basic literacy skills, scientists and linguists have embarked on a quest to program computers to produce novels, sonnets, and poems. So far the results have been mixed. In an article appearing in *The Guardian* on Nov. 11, 2014, journalist Tom Meltzer interviewed a few of the computer scientists involved in programming computers to write stories for National Novel Writing Month. Two of the projects, Scheherazade and the Metaphor Magnet, have as their objective the teaching of literacy to computers by having them analyze vast troves of literature and then having them try to produce similar texts. Journalist Nicholas Lezard reviews one of these robot narratives below:

> *Scheherazade*
>
> *John got into his car with his disguise, gun and note in his knapsack and headed towards the Old Second in the next town over, repeating his rehearsed demands silently over and over in his head.*

John watched while a little old lady left the bank and walked to her car and then slipped on his gloves, slipped his gun into his coat pocket, grabbed his mask and strode determinedly to the lobby door and pulled it open.

John looked at his reflection in the glass of the door, gave himself a little smirk and covered his face. John took another deep breath as he wondered if this was really a good idea, and entered the bank.

John looked around the bank, making sure his timing was right.

John spotted a young blond teller, Sally, behind the counter.

John stood behind the lady and toddler and politely waited his turn, noticing the nameplate on the counter ... "*Sally*".

When it was his turn, John, wearing his Obama mask, approached the counter. Sally saw Obama standing in front of her and she felt her whole body tense up as her worst nightmare seemed to be coming true.

Once Sally began to run, John pulled out the gun and directed it at the bank guard. John wore a stern stare as he pointed the gun at Sally.

Sally screamed hysterically which alerted other people in the bank.

[Lezard's review]: My first thought was: "Oh look, it's an extract from Dan Brown's new novel." Then I realised it was even clumsier than the master of turning rubbish into money. But not that much clumsier. I suspect that Scheherazade may even have been programmed using algorithms determined by genre fiction in general and

> Brown in particular, so relentless is the parade of clichés, redundant modifiers, and dimwit expositions. “Sally screamed hysterically which alerted other people in the bank” is a killer of a closing sentence, isn’t it?
>
> The disturbing thing is that a little tweaking of the program, such as getting the machine to learn that you don’t begin six consecutive sentences with the same word, especially if it’s “John”, could have turned this into something that might have been written by a very stupid human being with a tin ear; and there is plenty enough of that around. But even if one day the computer will pass muster at the level of the sentence, there is, on this evidence, no foreseeable way as yet that it will be able to construct a narrative that is both plausible and gripping. You may breathe easy. Unless you are Dan Brown (Meltzer, 2014, Nov. 11).

Google’s initial foray into computer generated poetry fared little better even with the added stipulation that its computer read 2,865 romance novels beforehand. In an article appearing in *Android Authority* on May 12, 2016, journalist John Dye has reported:

> The team gave the AI a starting sentence and an ending sentence. Then they asked artificial intelligence to bridge the two concepts using up to thirteen additional sentences. In a sense, they gave it a beginning and an end and asked it to tell a story. What came out was… a little strange. Take a look:
>
> **No.**
>
> he said.

“no,” he said.

“no,” i said.

“i know,” she said.

“thank you,” she said.

“come with me,” she said.

“talk to me,” she said.

“don’t worry about it,” she said (Dye, 2016, May 12).

If the first phase of AI literacy development has proven of dubious merit, Google’s next project is even more problematic: the filtering of fake news. Accusations of fake news have been reverberating around the Net since an army of independent media activists began to take advantage of the new digital publishing tools afforded by Web 2.0. In 2013, Senator Diane Feinstein attempted to restrict the definition of “journalist” to those individuals working for mainstream news outlets. She was met with criticisms from the Electronic Frontier Foundation (EFF) and other free speech advocates on the Web since her legislation would have stripped thousands of bloggers, citizen journalists, and indymedia activists of the protection of their sources, a safeguard afforded “legitimate” journalists. The most recent controversy over fake news began after WikiLeaks exposed corruption in the

Democratic National Committee (DNC) in 2016. It picked up steam after Donald Trump defeated Hillary Clinton for the office of U.S. President. As outrage echoed around the nation over Trump's election, pundits and commentators began seeking explanations for how an apparent easy victory for Clinton led instead to the election of Donald Trump. Still sensitive over accusations of voting irregularities among super delegates that led to the defeat of popular presidential candidate Bernie Sanders, Democratic apparatchiks appeared eager to find a justification for Clinton's loss that did not further implicate their own party leadership. One of the initial explanations they seized on was social media.

A little background is in order here. At around the time of the election, stories began to circulate about the problem of fake news on social media due to rumors about Clinton's reputed ill health. In the troubled weeks after Trump's election, the *Washington Post* and other mainstream media outlets ran a story about a mysterious website claiming to have exposed a number of Russian propaganda fronts masquerading as popular alternative news sites. The website in question, PropOrNot, derided disinformation produced by non-mainstream media sources for their pernicious influence on the outcome of the election. PropOrNot pointed the finger at such widely known left-wing news and analysis sites as *Consortiumnews, Truthout, CounterPunch, Naked Capitalism, Truthdig,* and *Black Agenda Report*. Also accused of being purveyors of Russian propaganda were a variety of far right, libertarian, and international news sites – the latter including *WikiLeaks*. In his piece for *The Intercept,* investigative journalist Glen Greenwald has observed, "Basically, everyone who isn't comfortably within the centrist Hillary Clinton/Jeb Bush spectrum is guilty" (Greenwald, 2016, Nov. 26). When contacted by *The Intercept* seeking evidence for their allegations, PropOrNot declined to comment.

Google and Facebook similarly came under attack. According to an article written by Julia Love and Kristina Cooke for Reuters on Nov. 16, 2016, the new media titans were criticized by the Democratic establishment for their role in facilitating the spread of manufactured news about Clinton's health – not to mention the Pizzagate scandal surrounding her campaign manager, John Podesta. To address those criticisms, the search engine and social media company issued statements of intent to modify their policies in order to prevent further fake news from appearing on their sites. "The shifts come as Google, Facebook and Twitter Inc. (TWTR.N) face a backlash over the role they played in the U.S. presidential election by allowing the spread of false and often malicious information that might have swayed voters toward Republican candidate Donald Trump" (Love & Cooke, 2016, Nov. 8). Curiously un-ironic in their depiction of what had been ostensibly portrayed as a genuine election process (if this is a democracy in a legitimate two-party system, it is the will of the people to pick the candidate of their choice whether or not the news agency agrees), Reuters and other mainstream media outlets continued to revile just about everyone in the country for Trump's victory. That is everyone except the Democratic party itself which the mainstream media depicted as a lugubrious victim of the election outcome.

Though Facebook CEO Mark Zuckenberger initially denied any influence on the election, he eventually joined Google CEO Eric Schmidt in promising to rein in the dissemination of fake news on their sites. Toward that end, Google and Facebook have stated they will implement algorithms designed to detect and prevent the spread of future fake news. Given the political ramifications of identifying "fake news," the idea of censoring its content seems highly problematic especially by a non-human agent with less

than exemplary literacy skills in the employ of two of the Internet's largest media companies.

However, fake news is nothing new. Noam Chomsky and Edward S. Herman's definitive book, *Manufacturing Consent* (2002) lays bare the manipulation of the fourth estate by government and corporate interests engaged in "perception management" in order to control U.S. domestic and foreign policy at home and abroad. For example, in the lead-up to the U.S. invasion of Iraq in 1990 (a.k.a. Operation Desert Storm), stories disseminated through astroturf organizations backed by multinational PR firms claimed that invading Iraqi soldiers had murdered Kuwaiti babies in the maternity ward of a Kuwait public hospital. In addition to President Bush and White House officials, this story was uncritically repeated by the U.S. mainstream media and the public at large. Only after hundreds of thousands had died in the U.S. invasion of Iraq was it finally revealed that the story was fabricated by a public relations firm with the support of U.S. backers in collaboration with members of the Kuwait royal family (2002, p. 78). The second invasion of Iraq in 2003 (dubbed Operation Shock and Awe) was similarly precipitated by a propaganda campaign, this time with top-level U.S. politicos alleging that Iraq had "weapons of mass destruction" (WMD). After the country was invaded and hundreds of thousands more killed, the Bush administration remained notably silent about the fact that no WMD's were to be found.

Military psyops is as old as empire. When HBGary was hacked by LuzSec, Cory Doctorow wrote an analysis for *Boing Boing* detailing some of the highlights of the disclosure of the company's emails. One of them addressed the aforementioned plan to engage in "persona management" through the creation of online sockpuppets. A sockpuppet is a false persona that interacts with Netizens on the World Wide Web in order to spread

political propaganda favorable to U.S. geo-political interests. The purpose is to build popular support for international U.S. policies through coordinated disinformation campaigns carried out by disguised online personas controlled by U.S. military agents. When the U.S. Airforce was revealed to have made the initial request to HBGary for the creation of the sockpuppet software, hacktivists around the Net were outraged. Doctorow reported:

> The enormous corpus of email leaked from federal security contractor HB Gary following Anonymous' hacking of the company's servers continues to deliver compromising payloads.
>
> This time, it's [sic] internal emails detailing the creation of "persona management" software to simplify the process of pretending to be several people at once online, in order to simulate widespread support for a point of view – astroturfing automation software. The software appears to have been developed in response to a federal government solicitation seeking automated tools for astroturfing message boards in foreign countries (Doctorow, 2011, Feb. 18).

A follow-up article appearing in *The Guardian* a month later led with the headline, "Revealed: US spy operation that manipulates social media." The authors of the article, Nick Fielding and Ian Cobain (2011), detailed the U.S. military's plans to "secretly manipulate social media sites" in order to "spread pro-American propaganda" on the Net. It revealed that a similar campaign in Iraq during the coalition occupation of the country went by the name "Operation Earnest Voice" (OEV) and tried to de-radicalize jihadists through ensnarement in online conversations designed to sway their political opinions. General James "Mad Dog" Mattis stated, "OEV 'supports all activities associated with degrading

the enemy narrative, including web engagement and web-based product distribution capabilities'" (Fielding & Cobain, 2011, Mar. 17). However, U.S. Central Command (Centcom) was at pains to deny any plans to target popular American social media platforms like Twitter and Facebook.

Closer to home, activists in the Black Panther party were targeted with a poison pen campaign to destabilize their leadership and neutralize the movement during the government's COINTELPRO program of the 1960s. The government's Counter Intelligence Program (or COINTELPRO) was one of several covert government operations that sought to derail the civil rights and anti-war movements of the 60s and 70s. In the case of the Black Panthers, FBI agents initiated a drive to infiltrate, harass, discredit, intimidate, and arrest members of the party, as well as to exert pressure on their private differences to create enmity and discord. One of the FBI's subterfuges included sending letters falsely attributed to different members of the party's leadership in order to make it appear as though one member were threatening another. In coordination with on-the-ground infiltrators in the Panthers, such disinformation efforts succeeded in igniting hatred and suspicion between members that eventually led to the death of at least one leader. All told, the FBI's poison pen campaign fomented the kind of discord and distrust that kept the Black Panthers destabilized, off-balance, and struggling to maintain internal cohesion. Students for a Democratic Society, as well as just about every other social justice group of the 60s and 70s, were similarly targeted.

Epistemic warfare is the term philosopher Peter Ludlow has given to various disinformation drives on the Information superhighway. Not long after Snowden's revelation of massive domestic spying by the National Security Agency (NSA) in 2013,

Ludlow wrote an op-ed piece appearing in the *New York Times* addressing the problem of the surveilling and deceiving of the American public. He points out the role of independent contractors and private security firms (HBGary, Stratfor, Booze Hamilton, et al.) in the employ of U.S. military intelligence charged with disseminating propaganda conducive to the government's political objectives. Drawing on the allegory of Plato's cave, Ludlow has mused on the potential use of cybernetic technologies to fabricate socio-political realities.

> In one of the most referenced allegories in the Western intellectual tradition, Plato describes a group of individuals shackled inside a cave with a fire behind them. They are able to see only shadows cast upon a wall by the people walking behind them. They mistake shadows for reality. To see things as they truly are, they need to be unshackled and make their way outside the cave. Reporting on the world as it truly is outside the cave is one of the foundational duties of philosophers.
>
> In a more contemporary sense, we should also think of the efforts to operate in total secrecy and engage in the creation of false impressions and realities as a problem area in epistemology — the branch of philosophy concerned with the nature of knowledge. And philosophers interested in optimizing our knowledge should consider such surveillance and deception not just fodder for the next "Matrix" movie, but as a real sort of epistemic warfare (Ludlow, 2013, June 14).

Ludlow warns of the possibility of military psyops waged against homegrown U.S. activists in a strategy of low-intensity conflict for purposes of full-spectrum military dominance. Such was the revelation of hacktivist Jeremy Hammond when he exposed the

surveillance operations of government intelligence contractor, Stratfor, who spied on a variety of human and animal rights groups in the United States. These included activists from the Occupy Wall Street movement, environmental activists, animal rights activists, and even politically minded comedians like the Yes Men. The latter "had humiliated Dow Chemical with a fake news conference announcing reparations for the victims [of Union Carbide in Bhopal, India]. Stratfor regularly copied several Dow officers on the minutia of activities by the two members of the Yes Men" (Ludlow, 2013). Perhaps most disturbingly, Hammond's email hack also revealed Stratfor's attempt to collaborate with NPR's *Morning Edition* to coordinate a regular public affairs program on national radio airwaves. This has not been the first time that U.S. intelligence agencies have sought to control mainstream media messages. An earlier program called Operation Mockingbird targeted the U.S. media for a wide-ranging propaganda drive designed to inculcate passive acceptance of U.S. government policies in the general public. Ludlow closes his op-ed with a discussion of the effects of secrecy and duplicity in the development of social epistemology.

> The Greek word deployed by Plato in "The Cave" – aletheia – is typically translated as truth, but is more aptly translated as "disclosure" or "uncovering" – literally, "the state of not being hidden." Martin Heidegger, in an essay on the allegory of the cave, suggested that the process of uncovering was actually a precondition for having truth. It would then follow that the goal of the truth-seeker is to help people in this disclosure – it is to defeat the illusory representations that prevent us from seeing the world the way it is. There is no propositional truth to be had until this first task is complete.

> This is the key to understanding why hackers like Jeremy Hammond are held in such high regard by their supporters. They aren't just fellow activists or fellow hackers – they are defending us from epistemic attack. Their actions help lift the hood that is periodically pulled over our eyes to blind us from the truth (Ludlow, 2013, June 14).

While Plato's allegory of the cave suggests the possibility for enlightenment, perhaps a more applicable allegory for the Information Age is to be found in Michael Reddy's conduit metaphor and the parable of the evil magician. In it, Reddy posits the idea of a disinformation operative in the form of an evil magician who deceives the inhabitants of the toolmakers paradigm into believing that their communications are of the conduit variety rather than the toolmakers variety (See Chapter Three, section D for a refresher on Reddy's ideas). This change in perspective towards their efforts to communicate signifies that the radical subjectivity originally enjoyed by the inhabitants of the toolmakers paradigm is replaced instead by the radical *objectivity* of the conduit metaphor. The latter's objectification of language results in the loss of the inhabitants' original belief in the need to work hard to interpret and comprehend their shared ideas with one another. The denizens of the toolmakers paradigm no longer believe they have to engage in diligent social work in order to understand each other's messages because the evil magician has deceived them into thinking that communication is a "'success without effort' system" rather than an "'energy must be expended' system" (Reddy, 1979, p. 308). Under the spell of the evil magician, the inhabitants of the toolmakers paradigm are tricked into thinking that the avoidance of miscommunication is superfluous since words hold meaning representational of actual

reality. Reddy has told the story thusly:

> It came to pass, one year, that an evil magician, who was an expert at hypnosis, flew over the toolmakers' compound. Looking down, he saw that, despite the formidable handicaps, Alex, Bob, Curt, and Don were doing quite well with their system of instruction sending. They were very aware that communicating was hard work. And their successes were extremely rewarding to them, because they retained a distinct sense of awe and wonder that they could make the system work at all. It was a daily miracle, which had improved their respective standards of living immensely. The evil magician was very upset about this, and decided to do the worst thing he could think of to Alex, Bob, Curt, and Don. What he did was this. He hypnotized them in a special way, so that, after they received a set of instructions and struggled to build something on the basis of them, they would immediately forget about this. Instead, he planted in them the false memory that the object had been sent to them directly from the other person, via a marvelous mechanism in the hub. Of course, this was not true. They still had to build the objects themselves, out of their own materials—but the magician blinded them to this.
>
> As it turned out, the evil magician's shrewdness was profound. For even though, objectively, the communications system of the compound had not changed one bit, it nevertheless fell very quickly into disuse and decay. And as it crumbled, so did the spirit of harmony and communal progress that had always characterized the relations of Alex, Bob, Curt, and Don. For now, since they would always forget that they had assembled an object themselves and thus bore a large share of responsibility for its

shape, it was easy to ridicule the sender for any defects. They also began to spend less and less time working to assemble things, because, once the mental block descended, there was no feeling of reward for a job well done. As soon as they finished an assembly, the hypnosis would take effect, and suddenly—well, even though they were worn out, still, it was the other fellow who had done all the hard, creative work of putting it together. Any fool could take a finished product out of the chamber in the hub. So they came to resent, and therefore abandon, any assembly jobs that required real work.

But this was not the worst effect foreseen by the evil magician when he cast his peculiar spell. For, indeed, it was not long before each of them came to entertain, privately, the idea that all the others had gone insane. One would send instructions to the others for some device of which he was particularly proud, just as he had always done. Only now, of course, he believed that he sent, not instructions, but the thing itself. Then, when the others would send him instructions in return, to confirm their receipt of his, he would assemble the object, forget, think that they had returned him the thing itself, and then stare in horror at what he saw. Here he had sent them a wonderful tool, and they returned to him grotesque parodies. Really, what could explain this? All they had to do was to successfully remove his object from the chamber in the hub. How could they change it so shockingly in performing an operation of such moronic simplicity? Were they imbeciles? Or was there perhaps some malice in their behavior? In the end, Alex, Bob, Curt, and Don all came privately to the conclusion that the others had either become hostile or else gone

> berserk. Either way, it did not matter much. None of them took the communications system seriously any more (Reddy, 1989, pp. 307 – 308).

If Reddy's conduit metaphor offers a dystopian vision of socio-epistemic development in the Information Age, then Baudrillard's vision is positively apocalyptic. An even more pessimistic interpretation of the Net is Baudrillard's (1994) critique of the postmodern world, in which he argues that the ceaseless duplication and replication at the heart of digital media has begun to overlay the human life-world itself. Perhaps the unforeseen consequences of this can be seen most clearly in the case of Aaron Swartz. His story illustrates Baudrillard's critique of the Internet since its ability to overwrite traditional forms of contracts and records was partly responsible for destroying the Internet prodigy.

Swartz has not been the only one. Millions of foreclosure victims have lost their homes as a result of the virtual elimination of public housing records through the newly created data banks of the Mortgage Electronic Registration System (MERS). Millions more have been disenfranchised through black box voting. As society grapples with the impact of ephemeral digital records, it perhaps goes without saying that the social consequences of the Internet's ability to effectively overwrite public documents and contracts have not been seriously criticized enough.

Lakoff and Johnson remind us that metaphors frame our linguistic and cognitive processes that in turn give rise to our reality. "Metaphors … are conceptual in nature. They are among our principal vehicles for understanding, and they play a central role in the construction of social and political reality" (1980, p. 159). Yet if this tendency toward reality's metaphorical resonance goes unchecked, it can create an echo chamber that renders metaphors as "self-fulfilling prophecies" (p. 156). As more and more of the human life-

world gets absorbed into the Internet, metaphors for the Net will determine not only the future of cyberspace but also our future global world order as well.

In looking at the relationship between the representational and the real, the symbolic and reality, Baudrillard's discussion on the possibility for mapping the knowledge commons evokes another powerful metaphor of the Internet: the map and the territory. In this extended metaphor, he cautions that, "the map is not the territory." Baudrillard reminds us that the map is a *model* of the territory, an abstraction not to be confused with reality. When the map and the territory are conflated, we are in danger of getting lost in terra incognita. For this reason, Baudrillard warns of the potential for "the precession of simulacra" to contribute to the creation of a hyperreal where reality and abstraction are no longer discernable opposites.

> The imaginary of representation, which simultaneously culminates in and is engulfed by the cartographer's mad project of the ideal coextensivity of map and territory, disappears in the simulation whose operation is nuclear and genetic, no longer at all specular or discursive. It is all of metaphysics that is lost. No more mirror of being and appearances, of the real and its concept. No more imaginary coextensivity: it is genetic miniaturization that is the dimension of simulation. The real is produced from miniaturized cells, matrices, and memory banks, models of control – and it can be reproduced an indefinite number of times from these. It no longer needs to be rational, because it no longer measures itself against either an ideal or negative instance. It is no longer anything but operational. In fact, it is no longer really the real, because no imaginary envelops it anymore. It is a hyperreal, produced from a

> radiating synthesis of combinatory models in a hyperspace without atmosphere (Baudrillard, 1994, p. 2).

If the affect of the Internet on our human life-world is one that melds the real and the unreal, then the unfortunate result is the transmogrification of the map into the territory. In fact, according to Baudrillard, there are no more distinguishable differences between abstractions and reality within the digital realms of the hyperreal. As the Internet and advanced communication technologies increasingly disconnect us from the real world and reconnect us to the hyperreal world of cyberspace, its socio-epistemic significance points to the possibility for another useful Internet metaphor: The brain in the vat. The brain in the vat is a thought experiment (or tortured metaphor if you will) that posits the idea of a mad scientist who surgically removes a brain from its body and puts it in a vat. Inside the vat, the brain is comfortably suspended in liquid nutrients and physically wired for sensory stimulation to replicate its original body. In this way, the brain in the vat has no way to know its true state of existence since it continues to receive all the real-world sensory stimuli that it would in normal form.

This has disturbing similarities to another utopian vision of the Internet: the global brain. The global brain is a theory of computer-powered human knowledge enhancement in which diverse information and communication technologies (ICT) around the planet are linked together to make up a world-wide distributed information system. Facilitated by social media, the global brain will be a digitally enabled neural net of epic computational ability. Like a Matrioshka brain, this emergent collective consciousness is seen as the next stage in human cognitive development and a globalized social epistemology.

On a more prudent note, it is worth remembering that as more and more of our daily social interactions get overwritten by ICT systems, the consequence of allowing ourselves to be disconnected from our physical lives in geographical space and time to be reconnected to a non-corporeal virtual reality in cyberspace means that we are unwittingly charting new territory. It needs little reminding that ICT systems have a tremendous potential to either significantly expand our consciousness or greatly control it. Due to the potential of the Internet and cybernetic systems in general to function as a socio-epistemic reality writ large, we should be mindful of the dangers of allowing the Net to become a giant conduit metaphor. Not to torture a metaphor more than necessary, but if we are not careful, we are in jeopardy of becoming "brains in a vat" where our sensory comprehension of social reality is increasingly mediated by advanced cybernetic systems. Lakoff and Johnson's caveat regarding the conduit metaphor's potential for misrepresenting social realities seems nearly prescient in the age of the surveillance state. "When a society lives by the CONDUIT metaphor on a large scale, misunderstandings, persecution, and much worse are the likely products" (1980, p. 232). Such was the tragic end of Aaron Swartz.

References

Aaron's Law Act of 2015, S. 1030, 114 Cong. (2015). Retrieved Dec. 25, 2015, from https://www.wyden.senate.gov/download/?id=dc65223a-35ce-40ad-9aca-dc89183dc678&download=1

Abel, D. (2013, July 30). In Aaron Swartz case, MIT remained neutral, internal report finds. *Boston.* Retrieved Sept. 18, 2015, from http://www.boston.com/metrodesk/2013/07/30/aaron-swartz-was-not-targeted-mit-according-independent-review/Xq0O8auOdygzPYwixR6VDP/story.html

Abelson, H., Diamond, P.A., Grosso, A., & Pfeiffer, D.W. (Review Panel). (2013, July 26). Report to the President: MIT and the Prosecution of Aaron Swartz. Retrieved Sept 18, 2015, from http://swartz-report.mit.edu/docs/report-to-the-president.pdf

Anonymous. (2013, Jan. 13). Anonymous to target DOJ after Aaron Swartz death and protect funeral home from hate group. *Pastebin.* Retrieved Sept. 17, 2015, from http://pastebin.com/PKm921c9

Anonymous. (2013, Jan. 17). Operation angel: Phase two. *Pastebin.* Retrieved Dec. 10, 2016, from http://pastebin.com/r8ushvbW

Assange, J. (2006, Nov. 25). The curious origins of political hacktivism. *Counterpunch.* Retrieved April 5, 2017, from http://www.counterpunch.org/2006/11/25/the-curious-origins-of-political-hacktivism/

Assange, J. (2006, Dec. 3). Conspiracy as governance. *IQ.org.* Retrieved Oct. 24, 2016, from https://web.archive.org/web/20070129125831/http:/iq.org/conspiracies.pdf

Bamford, J. (1982). *The puzzle palace.* New York: Penguin Books.

Barlow, J.P. (1990, June 1). Crime and puzzlement. *Electronic Freedom Frontiers (EFF).*

Retrieved April 18, 2017 from https://w2.eff.org/Misc/Publications/John_Perry_Barlow/HTML/crime_and_puzzlement_1.html

Barlow, J.P. (1996). A declaration of the independence of cyberspace. In P. Ludlow (Ed.), *crypto anarchy, cyberstates, and pirate utopias* (pp. 27 – 30). Cambridge, Massachusetts: The MIT Press.

Basso, J. (1997). How public relations professionals are managing the potential for sabotage, rumors and misinformation disseminated via the Internet by computer hackers. *IEEE Transactions on Professional Communication,* 40.1.

Baudrillard, J. (1994). Simulacra and simulation. Ann Arbor: The University of Michigan Press.

Bennett, A. (2012, Oct. 2). Key: LA visit about jobs. *NZ Herald.* Retrieved Jan. 27, 2017, from http://www.nzherald.co.nz/news/article.cfm?c_id=1&objectid=10837799

Bennett, W.L. & Segerberg, A. (2012). *The logic of connective action: digital media and the personalization of contentious politics.* Cambridge, Massachusetts: Cambridge University Press.

Blue, V. (2013, Feb. 19). Anonymous oplastresort hacks investment firm, cites stratfor ties. *Zdnet.* Retrieved Dec. 10, 2016, from http://www.zdnet.com/article/anonymous-oplastresort-hacks-investment-firm-cites-stratfor-ties/

Burke, Kenneth. (1950). *A rhetoric of motives.* Berkeley: University of California Press.

Burke, Kenneth. (1969). *A grammar of motives.* Berkeley: University of California Press.

Carter, J. & Wilson, A. R. (2004). *Sex and rockets: The occult world of Jack Parsons.* Port Townsend, Washington: Feral House.

Castells, M. (2010). *The rise of the network society.* (2nd ed.). West Sussex, UK: Wiley-Blackwell.

Castells, M. (2011). *Communication power.* New York: Oxford University Press.

Castells, M. (2012). *Networks of outrage & hope: Social movements in the Internet age.* Cambridge, Massachusetts: Polity Press.

cDc loves you too. Who we be. (n.d.). *Cult of the Dead Cow.* Retrieved Aug. 29, 2016, from http://w3.cultdeadcow.com/cms/about.html

Chaos Computer Club. In *Wikipedia*. Retrieved April 3, 2016, from https://en.wikipedia.org/wiki/Chaos_Computer_Club

Chomsky, N. & Herman, E. S. (2002). *Manufacturing Consent.* (2nd ed.). New York: Pantheon Books.

Cohn, C. (2015, April 29). Aaron's Law reintroduced: CFAA didn't fix itself. *Electronic Frontier Foundation (EFF).* Retrieved Sept. 17, 2015, from https://www.eff.org/deeplinks/2015/04/aarons-law-reintroduced-cfaa-didnt-fix-itself

Coleman, G. (2011). Hacker politics and publics. [Electronic version]. *Public Culture,* 23(3). Duke University Press. pp. 511 – 516.

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

Coleman, G. (2013, Feb. 4). Geeks are the new guardians of our civil liberties. *MIT Technology Review.* Retrieved Feb. 14, 2013, from http://www.technologyreview.com/news/510641/geeks-are-the-new-guardians-of-our-civil-liberties/

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

New York: Verso.

Coleridge, S. T. (1802). *Lyrical ballads, with a few other poems.* [Electronic version]. Retrieved July 23, 2017 from http://www.english.upenn.edu/~mgamer/Etexts/lbprose.html

Corey, D. (2016, June 30). ACLU files a lawsuit to repeal the Computer Fraud and Abuse Act used to prosecute Aaron Swartz. *Boing Boing.* Retrieved Aug. 2016, from http://boingboing.net/2016/06/30/aclu-files-a-lawsuit-to-repeat.html

Croft, W. & Cruse, D.A. (2004). *Cognitive linguistics*. Cambridge: Cambridge University Press.

Cullen, K. (2013, Jan. 15). On humanity, a big failure in Aaron Swartz case. *The Boston Globe.* Retrieved 2015 from https://www.bostonglobe.com/metro/2013/01/15/humanity-deficit/bj8oThPDwzgxBSHQt3tyKI/story.html

Dabrowska E. & Divjak D. (Eds.). (2015). *Handbook of cognitive linguistics.* Northumbria University: Mouton De Gruyter.

Dammbeck, L. (Director). (2003). *Das Netz: The Unabomber, LSD, and the Internet.* [Documentary]. Germany: B. Film Verleih.

Day, E. (2013, June 1). Aaron Swartz: Hacker, genius…martyr? *The Guardian*. Retrieved Dec. 26, 2016, from https://www.theguardian.com/technology/2013/jun/02/aaron-swartz-hacker-genius-martyr-girlfriend-interview

Demand Progress. (2011, July 19). Federal government indicts former Demand Progress executive director for downloading too many journal articles. *Common Dreams.* Retrieved Oct. 19, 2016, from http://www.commondreams.org/newswire/2011/07/19/federal-government-indicts-

former-demand-progress-executive-director-downloading

Department of Justice, U.S. Attorney's Office, District of Massachusetts. (2013, Jan. 16). Statement Of United States Attorney Carmen M. Ortiz regarding the death of Aaron Swartz [Press Release]. Retrieved Sept. 18, 2015, from http://www.justice.gov/usao-ma/pr/statement-united-states-attorney-carmen-m-ortiz-regarding-death-aaron-swartz

Doctorow, C. (2011, Feb. 18). HBGary's high-volume astroturfing technology and the Feds who requested it. *Boing Boing*. Retrieved Feb. 8, 2016, from http://boingboing.net/2011/02/18/hbgarys-high-volume.html

Doctorow, C. (2016, June 30). ACLU files a lawsuit to repeal the Computer Fraud and Abuse Act used to prosecute Aaron Swartz. *Boing Boing.* Retrieved Aug. 2016, from http://boingboing.net/2016/06/30/aclu-files-a-lawsuit-to-repeat.html

Draper, J. (2015). Who is John Draper aka captain crunch? *Webcrunchers.* Retrieved Aug. 29, 2016, from http://www.webcrunchers.com/who-is-john-draper-aka-captain-crunch/

Dye, J. (2016, May 12). After reading thousands of romance books, Google's AI is writing eerie post-modern poetry. *Android Authority*. Retrieved May 14, 2016 from http://www.androidauthority.com/google-ai-poetry-692231/

Earl, J. & Kimport, K. (2011). *Digitally enabled social change: Activism in the Internet age.* Cambridge, Massachusetts: MIT

Emmons, A. (2017, April 27). Brown taken back into custody before PBS interview. *The Intercept.* Retrieved May 2, 2017, from https://theintercept.com/2017/04/27/formerly-imprisoned-journalist-barrett-brown-taken-back-into-custody-before-pbs-interview/

Eubanks, P. (2004). Poetics and narrativity: How texts tell stories. In C. Bazerman and P. Prior (Eds.), *What writing does and how it does it* (pp. 33 – 56). New York: Lawrence

Erlbaum Associates.

Evans, V. & Melanie G. (2006). *Cognitive linguistics: An introduction*. Edinburgh: Edinburgh University Press.

Fairclough, N. (2001). *Language and power.* (2nd ed.). London: Longman.

Febvre. L. & Martin, H.J. (1997). *The coming of the book: The impact of printing, 1450-1800*. London: Verso.

Ferenstein, G. (2013, Jan. 13). Anonymous appears to have hacked MIT website, leaves Swartz tribute. *TechCrunch.* Retrieved Sept. 4, 2015, from http://techcrunch.com/2013/01/13/anonymous-appears-to-have-hacked-mit-website-leaves-swartz-tribute/

Fielding N., & Cobain, I. (2011, Mar. 17). Revealed: U.S. spy operation that manipulates social media. *The Guardian.* Retrieved from April 6, 2017, http://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks

Fillmore, C. J. (1982). Frame semantics. In The Linguistic Society of Korea (Eds.), *Linguistics in the morning calm* (pp. 111-137). Seoul: Hanshin Publishing Co.

Geeraerts, D. (Ed.). (2006). *Cognitive linguistics: Basic readings.* Berlin: Mouton de Gruyter

Gibson, W. (1984). *Neuromancer.* New York: Ace Science Fiction.

Greenberg, A. (2012). *This machine kills secrets: Julian Assange, the cypherpunks, and their fight to empower whistleblowers*. New York: Plume.

Greenberg, A. (2016, Dec. 16). Anonymous' Barrett Brown is free - and ready to pick new fights. *Wired.* Retrieved Dec. 18, 2016, from https://www.wired.com/2016/12/anonymous-barrett-brown-free-ready-pick-new-fights

Greenwald, G. (2016, Nov. 26). Washington Post disgracefully promotes a McCarthyite blacklist from a new, hidden, and very shady group. *The Intercept.* Retrieved Dec. 6, 2016, from https://theintercept.com/2016/11/26/washington-post-disgracefully-promotes-a-mccarthyite-blacklist-from-a-new-hidden-and-very-shady-group/

Guy, S. (2013, Jan. 15). Aaron Swartz was 'killed by government,' father says at funeral. *Chicago Sun-Times.* Retrieved Feb. 15, 2014, from suntim.es/V2s8zu

Hart, C. & Lukes, D. (Eds.). (2007). *Cognitive linguistics in critical discourse analysis.* New Castle: Cambridge Scholars Publishing.

Higgins, P. (2013, Mar. 7). Senate demands answers about Aaron Swartz. *Electronic Frontier Foundation (EFF).* Retrieved Oct. 18, 2016, from https://www.eff.org/deeplinks/2013/03/senate-demands-answers-about-aaron-swartz-more-must-be-done

Horton, S. (2013, Jan. 18). Carmen Ortiz strikes out. *Harper's Magazine.* Retrieved Oct. 18, 2016, from http://harpers.org/blog/2013/01/carmen-ortiz-strikes-out/

In memoriam, Aaron Swartz, November 8, 1986 – January 11, 2013, requiescat in pace. (2013, Jan. 14). *Anon Insiders.* Retrieved Sept 4, 2015, from https://anoninsiders.net/in-memoriam-aaron-swartz-659/

Jonsson, P. (2012, Jan. 21). If feds can bust Megaupload, why bother with anti-piracy bills? *The Christian Science Monitor.* Retrieved Jan. 28, 2017, from http://www.csmonitor.com/USA/2012/0121/If-feds-can-bust-Megaupload-why-bother-with-anti-piracy-bills/(page)/Photo-Galleries/In-Pictures/Today-at-the-Olympics

Kerr, O. (2013, 27 January). Aaron's Law, drafting the best limits of the CFAA, and a reader poll on a few examples. *Volokh Conspiracy.* Retrieved April 23, 2013 from

http://volokh.com/2013/01/27/aarons-law-drafting-the-best-limits-of-the-cfaa-and-a-reader-poll-on-a-few-examples-part-i/

Kessler, R. (2013, Jan. 26). Anonymous hacks department of justice website, threatens to launch multiple warheads. *Gawker.* Retrieved Sept. 4, 2015, from http://gawker.com/5979203/anonymous-hacks-department-of-justice-website-threatens-to-launch-multiple-warheads

KevinTx. (2013, Sept. 23). #OpLastResort – Anonymous – operation last resort. *YouTube.* Retrieved May 16, 2017, from https://www.youtube.com/watch?v=ebGAYntjJGo

Lakoff, G. & Johnson, M. (1980). *Metaphors We Live By.* Chicago: University of Chicago Press.

Lakoff, G. (1992). The contemporary theory of metaphor. In A. Ortony (Ed.), *Metaphor and Thought*. (2nd Ed.). (pp. 203 – 204) Cambridge, Massachusetts: Cambridge University Press.

Lakoff, G. (2004). *Don't think of an elephant: Know your values and frames the debate.* White River Junction, Vermont: Chelsea Green Publishing.

Lakoff, G. (2004, Jan. 14). Election 2004: Inside the frame. *AlterNet.* Retrieved Aug. 8, 2014, from http://www.alternet.org/story/17574/inside_the_frame

Lakoff, G. (2008). Speech to the commonwealth club of California. *FORAtv.* Retrieved 2014 from http://fora.tv/2008/06/20/George_Lakoff_on_The_Political_Mind

Lakoff G. (2011, Oct. 19). How to frame yourself: A framing memo for Occupy Wall Street. *The Blog.* Retrieved Aug. 8, 2014, from http://www.huffingtonpost.com/george-lakoff/occupy-wall-

street_b_1019448.html

Lennard, N. (2013, Jan. 28). Anonymous hacks U.S. Sentencing Commission website for Aaron Swartz. *Salon.* Retrieved Sept. 4, 2015, from http://www.salon.com/2013/01/28/anonymous_hacks_doj_website_for_aaron_swartz/

Lessig, L. (n.d.). Prosecutor as bully. *LESSIG Blog, v2.* Retrieved Oct. 21, 2016, from http://lessig.tumblr.com/post/40347463044/prosecutor-as-bully

Lessig, L. (2005). *Free culture: The nature and future of creativity.* New York: Penguin Books.

Licklider, J.C.R. (2003). Man-computer symbiosis. In Montfort, N. & Wardrip-Fruin, N. (Eds.). *The new media reader.* Cambridge, Massachusetts: The MIT Press.

Lievrouw, L. A. (2011). *Alternative and activist mew media.* Malden, MA: Polity Press.

Limer, E. (2013, Jan, 26). Anonymous attacks department of justice website and threatens worse over Aaron Swartz's suicide. *Gizmodo.* Retrieved Sept. 4, 2015, from http://gizmodo.com/5979249/anonymous-attacks-department-of-justice-website-over-aaron-swartzs-suicide

Lofgren, Z. & Wyden, R. (2013, June 20). Introducing Aaron's Law, a desperately needed reform of the computer fraud and abuse act. *Wired.* Retrieved Dec. 25, 2015, from http://www.wired.com/2013/06/aarons-law-is-finally-here/

Lofgren, Z. (2013, June 20). Rep Zoe Lofgren introduces bipartisan Aaron's Law. *Wikisource.* Retrieved Oct. 30, 2015 from https://en.wikisource.org/wiki/Rep_Zoe_Lofgren_Introduces_Bipartisan_Aaron%27s_Law

Love, J. & Cooke, K. (2016, Nov. 8). Google, Facebook, move to restrict ads on fake news

sites. *Reuters.* Retrieved April 21, 2017, from http://www.reuters.com/article/us-alphabet-advertising-idUSKBN1392MM

Ludlow, P. (2001). New foundations: On the emergence of sovereign cyberstates and their governance structures. In P. Ludlow (Ed.)*, Crypto anarchy, cyberstates, and pirate utopias.* Cambridge, Massachusetts: The MIT Press.

Ludlow, P. (2013, June 14). The real war on reality. *The New York Times.* Retrieved Feb. 17, 2016, from http://opinionator.blogs.nytimes.com/2013/06/14/the-real-war-on-reality/?_r=1&

Lute, J.H. (2013, Mar. 3). DHS cybersecurity: roles and responsibilities to protect the nation's critical infrastructure. *Department of Homeland Security.* Retrieved Oct. 13, 2014, from http://www.dhs.gov/news/2013/03/13/written-testimony-dhs-deputy-secretary-jane-holl-lute-house-committee-homeland

Macfarquhar, L. (2013, Mar. 11). Requiem for a dream. *The New Yorker.* Retrieved Sept. 4, 2015, from http://www.newyorker.com/magazine/2013/03/11/requiem-for-a-dream

Malamud, C. (2013, Jan. 24). Aaron's army. *Public.resource.org.* Retrieved Oct. 19, 2016, from https://public.resource.org/aaron/army/index.html

Masnick, M. (2013, March 7). Holder: DOJ used discretion in bullying Swartz, press lacked discretion in quoting facts. *Techdirt.* Retrieved Nov. 15, 2016, from https://www.techdirt.com/articles/20130306/13444122220/holder-doj-used-discretion-bullying-swartz-press-lacked-discretion-quoting-facts.shtml

McAfee Labs. (2013, Jan. 27). Anonymous releases 'warhead' via #OpLastResort. *McAfee.* Retrieved Dec. 10, 2016, from https://securingtomorrow.mcafee.com/executive-perspectives/anonymous-releases-warhead-via-oplastresort/

McConville, C. & Cassidy, C. (2013, Jan.). Ortiz says suicide will not change handling of cases. *PressReader.* Retrieved Nov. 15, 2016, from www.pressreader.com/usa/boston-herald/20130121/281603827830887

McVeigh. K. (2013, Jan. 14). Anonymous attacks MIT websites after death of Internet activist Aaron Swartz. *The Guardian.* Retrieved Sept. 4, 2015, from http://www.guardian.co.uk/technology/2013/jan/14/anonymous-attack-mit-aaron-swartz

McVeigh, K. (2013, Jan. 24). Hacktivist anger over US government's 'ludicrous' cyber crackdown. *The Guardian.* Retrieved Dec. 26, 2016, from http://www.guardian.co.uk/technology/2013/jan/24/hacking-us-government-cyber-crackdown

McVeigh, K. (2013, Jan. 29). Aaron Swartz case prompts letter to US attorney general from congressmen. *The Guardian.* Retrieved Oct. 18, 2016, from https://www.theguardian.com/technology/2013/jan/29/aaron-swartz-investigation-darrell-issa-cummings-holder

Meltzer, T. (2014, Nov. 11). Once upon a bot: can we teach computers to write fiction? *The Guardian.* Retrieved April 20, 2017 from https://www.theguardian.com/books/2014/nov/11/can-computers-write-fiction-artificial-intelligence

Montfort, N. & Wardrip-Fruin, N. (Eds.) (2003). *The new media reader.* Cambridge, Massachusetts: The MIT Press.

Nissenbaum, H. (2004). Hackers and the contested ontology of cyberspace. *New Media and Society,* 6, 195 - 217. Norton, Q. (2013, Mar. 3). Life inside the Aaron Swartz investigation. *The Atlantic.* Retrieved Oct. 28, 2016, from

http://www.theatlantic.com/technology/archive/2013/03/life-inside-the-aaron-swartz-investigation/273654/)

Office of Legal Education Executive Office. (n.d.). Prosecuting computer crimes. Retrieved Dec. 28, 2016, from http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf

Ortiz, C. (2013, Jan. 16). Statement of United States attorney Carmen M. Ortiz regarding the death of Aaron Swartz. Retrieved Sept. 18, 2015, from https://www.documentcloud.org/documents/557005-statement-of-us-attorney-ortiz-jan-16-2013-pdf.html

Parker, H. (2013, March 7). Senate demands answers about Aaron Swartz, but more must be done. *Electronic Frontier Foundation (EFF).* Retrieved March 10, 2014, from https://www.eff.org/deeplinks/2013/03/senate-demands-answers-about-aaron-swartz-more-must-be-done

Perelman, C. (1982). *The realm of rhetoric.* Notre Dame: University of Notre Dame Press.

Peters, E. (January 28, 2013). Re: United States v. Aaron Swartz. Letter to Robin Ashton, Counsel, US Dept. of Justice. *Keker & Van Nest LLP.* Retrieved Oct. 21, 2016, from http://big.assets.huffingtonpost.com/HeymannOPRletter.pdf

Peters, J. (2016). *The idealist: Aaron Swartz and the rise of free culture on the Internet.* New York: Scribner.

"Petition to remove prosecutor in Aaron Swartz case up for White House response." (2013, Feb. 13). *RT.* Retrieved Jan. 12, 2014, from http://www.rt.com/usa/swartz-prosecutor-petition-response-163/

Pierce, C. P. (2013, Jan. 17). Still more about the death Of Aaron Swartz. *Esquire*. Retrieved January 18, 2016, from http://www.esquire.com/blogs/politics/aaron-swartz-case-

011713

Prosecutor pursuing Aaron Swartz linked to suicide of another hacker. (2013, Jan. 15). *RT.* Retrieved Oct. 19, 2016, from https://www.rt.com/usa/swartz-prosecutor-suicide-hacker-050/

Quinn, N. (2013, March 3). Life inside the Aaron Swartz investigation. *The Atlantic.* Retrieved Oct. 28, 2016, from http://www.theatlantic.com/technology/archive/2013/03/life-inside-the-aaron-swartz-investigation/273654/

Reader, R. (2016, Jan. 11). 3 years after Aaron Swartz's death, here's what's happened to Aaron's law. *MIC.* Retrieved Jan. 13, 2017, from https://mic.com/articles/132299/3-years-after-aaron-swartz-s-death-here-s-what-s-happened-to-aaron-s-law#.6tuoTpdtK

Reddy, M. J. (1979). The conduit metaphor: A case of frame conflict in our language about language. In A. Ortony (Ed.), *Metaphor and Thought* (pp. 284–310). Cambridge, Massachusetts: Cambridge University Press.

Reilly, R.J., Smith, G., & Carter, Z. (2013, Jan. 14). Aaron Swartz's lawyer: Prosecutor Stephen Heymann wanted 'juicy' case for publicity. *The Huffington Post.* Retrieved Nov. 15, 2016, from http://www.huffingtonpost.com/2013/01/14/aaron-swartz-stephen-heymann_n_2473278.html

Reilly, R. J., Grim, R., & Carter, Z. (2013, Jan. 15). Darrell Issa probing prosecution of Aaron Swartz, Internet pioneer who killed himself. *HuffPost*. Retrieved Oct. 18, 2016, from http://www.huffingtonpost.com/2013/01/15/darrell-issa-aaron-swartz-_n_2481450.html

Sandra, G. (2013, Jan. 15). Aaron Swartz was 'killed by government,' father says at funeral.

Chicago Sun-Times. Retrieved Oct. 13, 2016, from http://chicago.suntimes.com/business/17594002-420/aaron-swartz-memorialized-at-service.html

Schneier, B. (2006, Sept. 7). Microsoft and FairUse4WM. *Schneier on security technology*. Retrieved March 20, 2012, from http://www.schneier.com/blog/archives/2006/09/microsoft_and_f.html

Senate Website for Wyden, R. (2015, April 21). Wyden, Lofgren, Paul introduce bipartisan, bicameral Aaron's Law to reform abused computer fraud and abuse act [Press release]. Retrieved Dec. 25, 2015, from https://www.wyden.senate.gov/news/press-releases/wyden-lofgren-paul-introduce-bipartisan-bicameral-aarons-law-to-reform-abused-computer-fraud-and-abuse-act-

Sieczkowski, C. (2013, Jan. 16). Westboro Baptist Church drops Aaron Swartz funeral protest after Anonymous vows action. *Huffington Post*. Retrieved Dec. 10, 2016, from http://www.huffingtonpost.com/2013/01/15/westboro-baptist-church-aaron-swartz-anonymous_n_2479019.html

Sledge, M. (2014, Jan. 25). Eric Holder criticized on anniversary of Aaron Swartz death. *The Huffington Post.* Retrieved Jan. 2017, from http://www.huffingtonpost.com/2014/01/10/eric-holder-aaron swartz_n_4576570.html

Sterling, B. (2002). *The hacker crackdown.* Boston: IndyPublish.

Stout, D. (2000, Sept. 23). Youth sentenced in government hacking case. *The New York Times.* Retrieved Nov. 15, 2016, from http://www.nytimes.com/2000/09/23/us/youth-sentenced-in-government-hacking-case.html

Stryker, C. (2011). *Epic win for anonymous: How 4Chans army conquered the web.* New

York: The Overlook Press.

Swartz, A. (2015). *The boy who could change the world: The writings of Aaron Swartz.* New York: The New Press.

Turing, A. (2003). Computing machinery and intelligence. In N. Wardrip-Fruin & N. Montfort, (Eds.), *The New Media Reader* (pp. 50 - 64). Cambridge, Massachusetts: The MIT Press.

U.S. Department of Justice. (2009). *The Black Vault.* Retrieved Sept. 24, 2015, from documents.theblackvault.com/documents/fbifiles/swartzfbifile.pdf

Van Dijk, T. A. (1977). Context and cognition: Knowledge frames and speech act comprehension. [Electronic version]. Elsevier. *Journal of Pragmatics,* pp. 211 – 231.

Van Dijk, T. A. (2009). *Society and discourse: How social contexts influence text and talk.* Cambridge: Cambridge University Press.

Vandita. (2016, Sept. 11). Anonymous vigilante faces 16 years in prison for exposing Steubenville rapists who walk free. *AnonHQ.* Retrieved Sept. 13, 2016, from http://anonhq.com/anonymous-vigilante-faces-16-years-in-prison-for-exposing-steubenville-rapists-who-walk-free/

Vanity Fair. (2011, April 4). Retrieved Oct. 15, 2014, from http://www.vanityfair.com/business/features/2011/04/4chan-201104

Wachtler, M. (Nov. 8, 2015). Happy birthday Aaron Swartz – RIP. *Whiteout Press.* Retrieved Nov. 9, 2015, from http://www.whiteoutpress.com/articles/2015/q4/happy-birthday-aaron-swartz-rip/

Wikipedia. (n.d.). Kim Dotcom. Retrieved Jan. 27, 2017, from

https://en.wikipedia.org/wiki/Kim_Dotcom

Wikipedia. (n.d.). Representative Zoe Lofgren introduces bipartisan Aaron's Law. Retrieved Dec. 16, 2015, from https://en.wikisource.org/wiki/Rep_Zoe_Lofgren_Introduces_Bipartisan_Aaron%27s_Law

Wikipedia, (n.d.). "Information wants to be free." Accessed Oct. 3, 2014, from http://en.wikipedia.org/wiki/Information_wants_to_be_free

Wright, D. (2013, Aug.). Prosecutor Stephen Heymann compared Aaron Swartz to rapist. *Shadow Proof.* Retrieved from https://shadowproof.com/2013/08/01/prosecutor-stephen-heymann-compared-aaron-swartz-to-rapist/

Wrigley, W. (2013, February 7). Darrell Issa praises Aaron Swartz, internet freedom at memorial. *Huffington Post*. Retrieved February 21, 2013, from http://www.huffingtonpost.com/2013/02/07/darrell-issa-internet-freedom_n_2633197.html

Wyatt, S. (2004). Danger! Metaphors at work in economics, geophysiology, and the Internet. [Electronic version]. *Science, Technology, & Human Values,* Vol. 29 No. 2, Spring 2004, pp. 244-245. Retrieved April 15, 2017, from http://virtualknowledgestudio.nl/documents/danger-metaphors.pdf

Yates, Frances A. (1966). *The art of memory.* Chicago: The University of Chicago Press.