Unorthodox Hacking: Addressing Sexism in Hacktivist Communities to Expand Options for Electronic Civil Disobedience

Giulia Curcelli

Honors Thesis
Curriculum in Peace, War, and Defense
University of North Carolina at Chapel Hill

Spring 2017

Approved: ____________________________

Sara Bush Castro
Advisor
Curriculum in Peace, War, and Defense

Kenneth Andrews
Reader
Department of Sociology
Table of Contents

Introduction ..........................................................................................................................3
Literature Review ................................................................................................................14

Case 1: Mr. Robot Season 1 ..................................................................................................24

Case 2: Aaron Swartz and Freedom of Information .........................................................48

Case 3: The Transborder Immigrant Tool ..........................................................................71

Conclusion: A Future Direction for Electronic Civil Disobedience ..................................94

Appendix One: Graph of DDoS Attack ............................................................................99

Appendix Two: The Political Compass .............................................................................100

Appendix Three: Diagram of Research Aims .................................................................101

Bibliography .....................................................................................................................102
Introduction

With the proliferation of the computer over the past few decades, hacktivism—a form of activism through computer hacking—has become widespread on the international political stage, a critical aspect of cybersecurity, and an emerging question of the balance between free expression and national security. Public perception often frames hacktivists as malevolent practical jokers, but discourse is shifting to mirror hacktivists’ perceptions of themselves as fighters for justice and an open internet. Because cyberspace remains fresh and relatively legally unregulated, the constraints for this political participation continue to evolve.

A subset of hacktivism is electronic civil disobedience. Academics have formed various frameworks for the translation of traditional civil disobedience to the cyber realm, viewing civil disobedience as an acceptable and healthy element of democracy. In contrast, the security industry largely derides hacktivism as wholly threatening. Academics have also begun to explore the links between gender and hacktivism, acknowledging the male hacker archetype and the disproportionately low number of women involved in hacking and technology.

Building on existing frameworks for the translation of civil disobedience to the cyber realm, this analysis of electronic civil disobedience centers around three case studies that illustrate different types of and perspectives on ECD. In particular, I examine how the subjects of each case study do and do not talk about and experience gender, and how this influences their understanding of hacking and what should be considered electronic civil disobedience. This research bridges the gap between existing work on when hacktivism is electronic civil disobedience and the influence of gender on
hacktivism. Currently, the views of hacking communities and legal professionals on what constitutes acceptable civil disobedience are fundamentally misaligned. What hackers see as legitimate, law enforcement sees as criminal. What law enforcement sees as acceptable civil disobedience, hackers do not see as hacking. Ultimately, I argue that electronic civil disobedience has more potential than its current use, but to increase its prevalence would require a shift in perspective by both government and practitioners of civil disobedience.

The government does not distinguish between criminal and activist hacking but must begin to do so to treat electronic civil disobedience as true civil disobedience, affording sentences accordingly. On the part of hackers in particular, their perspectives are limited by their gendered view of technology, and dismantling sexism and patriarchy in tech communities will aid in this perspective shift.

To contextualize the case studies, I begin with an overview of civil disobedience in the United States. I then provide an introduction to hacking culture in the United States, including the definitions and origins of relevant jargon. Next I discuss how the culture of the internet makes it a particularly well-suited venue for political participation, and I address the issues that also arise in this domain. Following this background, I survey the existing literature on the translation of civil disobedience to the cyber world, on hacker identity, and on the role of gender in hacktivism. I will also use this literature to define a hacker archetype relevant to my case studies.

For each case, I provide an overview of the individual’s or organization’s history, including particular sections on the movement context of their activism and a technical description of their hack. I then discuss the hack’s perception, both legally and in hacking communities. I discuss how the hack fits into academic descriptions of traditional civil
disobedience. Then, I explore the particular ways in which the individual or group fits into or breaks the established hacker archetype, particularly through their politics and gender experiences. Especially with the latter identity, I focus on its effect on other hackers’ perceptions of the case as fitting into electronic civil disobedience.

I conclude that the individuals and groups more entrenched in patriarchy and maleness take traditional approaches to their hacking, while those with female experiences or progressive views of gender approach hacking more creatively and less destructively. But because femininity is culturally seen as weak and lesser than masculinity, those who conduct hacks perceived as more feminine are less likely to be accepted into predominantly male hacktivist communities. Thus, their hacks, which indicate potential for functional use of electronic civil disobedience, are not seen as proper hacktivism.

I intentionally limit the scope of this thesis in two ways. In this analysis, I categorically exclude whistleblowing from the discussion.¹ Hacktivist organizations such as Wikileaks rely on the distribution of classified information as their form of protest, but this is a fairly simple translation from the physical world to the cyber world. The internet provides a new venue, but the release of information is the same, so I exclude this less interesting discussion. Additionally, because state borders do not directly translate to the internet, the use of civil disobedience transnationally creates new challenges beyond the scope of my case studies. I limit my analysis to an American perspective on electronic disobedience.

¹ Whistleblowing is defined as an employee’s disclosure of information to law enforcement or other government agencies about an employer’s wrongdoing that violates the law or causes injury to people. Legal Information Institute Wex, s.v. “Whistleblower,” https://www.law.cornell.edu/wex/whistleblower.
civil disobedience, though the viability of expanding electronic civil disobedience into international law provides an opportunity for further research.

Ultimately, I hope to create a greater space for the existence of electronic civil disobedience that balances a respect for the American political tradition of dissent with a practical approach to preserving national security. My case studies provide a breadth of possibilities of varying feasibility. What I define as constructive, direct electronic civil disobedience—perceived as more feminine by hackers—holds that potential. I supplement the existing work on electronic civil disobedience by extending a gendered analysis that provides a viable and accessible yet necessarily constrained model of political participation for a digital age, expanding on the possibility of creative, non-destructive hacking for a variety of domestic and global issues.

**History of Civil Disobedience**

The history of civil disobedience in the United States provides context for its continued use in the 21st century. Henry David Thoreau coined the term “civil disobedience” in 1849 when he explained his refusal to pay poll taxes because they would help fund American slavery and the United States’ war against Mexico, both of which he morally opposed. In an article for the *Rutgers Computer and Technology Law Journal*, law professor Jonathan Liljeblad provides an overview of the many diverse criteria that activists and academics have created in the years since Thoreau. His comparison includes the ideas of Russian writer Leo Tolstoy, Indian activist Mahatma Gandhi, and American Civil Rights leader Martin Luther King, Jr. Thoreau explained civil disobedience as an individual act guided by one’s personal conscience, and Tolstoy
added to this by urging nonviolence. Tolstoy saw the state as unnecessary, so his idea of civil disobedience would not require respect of the overarching rule of law. Sharing a revolutionary mentality with Tolstoy, Gandhi also sought to replace the British government in India with an independent one, but he stipulated that protestors should accept punishment for their actions and withstand suffering inflicted by their punishers. King then specified that participating in civil disobedience is a moral responsibility, and he agreed with Gandhi that accepting punishment was an important step in protesting injustice.²

Liljeblad adds further complexity to this history by adding the perspectives of academic scholarship on civil disobedience. Political theorist Hannah Arendt believed that acts of civil disobedience must be a form of public communication and reflective of popular opinion. Historian, activist, and author Howard Zinn sees civil disobedience as the necessary violation of a law when legal channels are insufficient to protect a fundamental human right at risk. Political philosopher John Rawls provides a widely-accepted³ list of requirements for an act of civil disobedience: that it be public, nonviolent, conscientious, political, in conflict with the law, aimed to alter law and policy, and representative of a community’s sense of justice. Rawls also believes that even when violating the law, a protestor must maintain respect for the overarching system of law, thus accepting their assigned punishment. Sociologist and philosopher Jurgen

---

Habermas lists nonviolence, symbolism, illegality, and an appeal to justice as his requirements.4

These varied opinions have many similarities, but Liljeblad also raises a significant split in opinion in academic literature on civil disobedience. Direct civil disobedience violates the specific law that it seeks to change, while indirect civil disobedience violates a different law—often trespassing or resisting arrest—to bring attention to a different, unjust law. Because direct civil disobedience focuses on the specific injustice it seeks to change, it often receives more leniency in sentencing and is seen as more legally justifiable.5

As Liljeblad notes, this understanding of history is important because placing one’s violation of the law in the same tradition of civil disobedience gives it increased legitimacy.6 The broad idea of breaking a law to protest injustice has been a critical and respected element of American democracy from the American Revolution to the suffrage, civil rights, and anti-Vietnam War movements.7 This shift of an action from criminality to altruism will also prove relevant to perceptions of hacking as well.

**Origins of Hacking**

To understand electronic civil disobedience, one must understand the meanings and origins of the words hacking and hacktivism. Merriam-Webster offers two relevant definitions of the word “hacker”: either “an expert at programming and solving problems with a computer” or “a person who illegally gains access to and sometimes tampers with

5 Ibid., 214.
6 Ibid., 198-199.
7 “Civil Disobedience.”
information in a computer system.”\(^8\) To understand these two definitions, an article in the technology magazine *Wired* traces the evolution of the word. In minutes from a 1955 meeting, The Tech Model Railroad Club at the Massachusetts Institute of Technology noted, “Mr. Eccles requests that anyone working or hacking on the electrical system turn the power off to avoid fuse blowing.” Here, hacking referred to students’ creating and modifying model trains that connected to the electrical system. For almost a decade, the word “hack” retained its playful and creative meaning. It frequently referred to particularly great pranks MIT students played, which were often technically complex. In November 1963, a headline in the MIT campus newspaper reported “Telephone Hackers Active.” The article described an unauthorized intrusion where a hacker connected a computer to the MIT phone system. This incident, now referring to computer connections and criminality, shifted the meaning of the word. By the 1980s until the early 2000s, “hack” as used in mainstream culture now referred to criminal activity. Recently, though, burgeoning tech startups like Facebook have adopted the word and placed it back into a positive light. They use the hack to refer to the creation of new software, applications, and websites, or to attempts to break into a company’s own system to find vulnerabilities and make it more secure.\(^9\) This change in meaning is also reflected in the rise of hackathons (hack marathons), gatherings where programmers work intensely for a few days on shared projects in an environment of creativity and collaboration.\(^10\) In this sense, the term hacking is now akin to brainstorming or creating, though it retains its dual


meaning of gaining illegal access to computer systems. Most broadly, hacking means to apply technology in an unconventional way, whether legally or illegally.¹¹

Hacktivism merges the idea of hacking with political activism. The Cult of the Dead Cow, founded in 1984 as one of the first hacktivist organizations, coined the term. The organization’s founder Oxblood Ruffin defined hacktivism as the use of “technology to improve human rights across electronic media.” In the group’s statement “The Hacktivismo Declaration,” he wrote that hacktivism should be used to protect rights including but not limited to those listed in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. One specific freedom that Ruffin notes is “the liberty of fair and reasonable access to information,” particularly important to internet communities. He directly tied hacktivism to existing ideas of social justice and human rights advocacy, but at the time hacking was still perceived in a primarily negative light. The group’s quest to distinguish hacktivism from criminal definitions of hacking was not immediately successful.¹²

The Critical Art Ensemble, a performance art and activist collective, invented the term Electronic Civil Disobedience to refer to a specific type of hacktivist tactic. Founded in 1987, the group focuses on the interaction between art, technology, and activism.¹³ The group hoped to combat increasing authoritarianism throughout the world. Because finance and government were shifting online, CAE realized that the best venue for their protest would also be the internet and that it was a particularly important venue for them

¹¹ Brian Alleyne, “‘We are all hackers now’: critical sociological reflections on the hacking phenomenon,” Goldsmiths Research Online (2011): 2.
to resist the spread of authoritarianism. They used all the technology available to them, including fax machines, phones, and, increasingly, computers. CAE’s proposal of ECD did not merely combine technology and activism but also focused on a particular, well-established, and widely accepted strategy of protest.\(^{14}\)

### Internet Culture and Understanding Hackers

Also important in evaluating electronic civil disobedience is understanding the culture of the internet in which much of ECD takes place. This culture makes the internet a well-suited venue for participation while posing some challenges for electronic civil disobedience. Early hackers in the 1960s and 1970s dedicated themselves to the openness of the internet, a principle that endures in most hacking cultures. They believed in the importance of information sharing and that technology could foster community.\(^{15}\) The value of openness on the internet creates a space for anybody to participate, which aligns with the American political tradition. Everyone can have a voice on the internet, just as in politics. Computers provide a new venue to exercise political participation.

The use of technology for protest also raises new challenges. The internet has the power to elevate the voices of small groups of individuals. While this power is valuable and allows marginalized people to be heard, it can also give undue power to small, unpopular factions.\(^{16}\) As infrastructure and capital have shifted online, the internet has also become highly regulated, in conflict with its founding principles.\(^{17}\) This has driven some politically-oriented hackers to conduct their work anonymously, particularly those

\(^{14}\) Hurst, “Examining Hacktivism,” 6, 37.  
\(^{15}\) Alleyne, “‘We are all hackers now,’” 4, 8.  
\(^{16}\) Ibid., 3.  
\(^{17}\) Hurst, “Examining Hacktivism,” 22.
who believe in libertarianism and the threat of corporate and government surveillance.\textsuperscript{18}

This regulation reflects the privatization of most internet spaces. Because most spaces are private spaces and not government-owned public property, disruptive civil disobedience creates conflict with the rights of private property owners. Free speech and property rights butt heads,\textsuperscript{19} and there is no public street or sidewalk for activists to occupy.

Ricardo Dominguez, founder of the Electronic Disturbance Theater, the focus of my third case study, retorts that the history of civil disobedience “is one of blockage or trespass…that disrupts the everyday flow of power.”\textsuperscript{20} Protests in private spaces on the internet are not significantly different from the disruptive history of traditional civil disobedience. This last concern, he believes, is unnecessary.

Even with the varied traditions of hacking, government and corporate institutions associate all hacking with criminality.\textsuperscript{21} The notoriously vague Computer Fraud and Abuse Act, passed in 1986, broadly outlines computer-related offenses. These include computer-related espionage, fraud, and extortion, theft of financial information, distribution of code that damages computer systems, and unauthorized access of a protected computer. A protected computer was originally defined as any computer belonging to the U.S. government or financial institutions, or “used in interstate or foreign commerce or communication” whether located in the United States or abroad. The National Information Infrastructure Protection Act, signed by President Clinton in 1996, expanded the definition to include any computer connected to the internet.\textsuperscript{22}

\textsuperscript{18} Alleyne, “‘We are all hackers now,’” 7.
\textsuperscript{20} Hurst, “Examining Hacktivism,” 68.
\textsuperscript{21} Ibid., 11.
criminal charges for hacking fall under the CFAA, and many lawyers, including the National Association of Criminal Defense Lawyers, believe that sentencing guidelines for those charges are overly harsh.²³

Even with severe criminal repercussions, hackers believe they are unlikely to be caught, thinking that law enforcement has inadequate experience handling cybercrime, that companies are unlikely to report attacks, or that they have the skills to avoid being detected or identified. In a survey of 127 attendees of a computer hacker convention, those who had participated in illegal hacking agreed more with the statement “I can gain from hacking illegally” than with “I can lose from hacking illegally.” Hackers believe the benefits of their work outweigh the risks of being caught and punished.²⁴ A wide array of potential benefits motivates hackers, among which are fame, financial gain, and political change. A politically motivated hacker might be state-sponsored, affiliated with a terrorist group, or driven by activism.²⁵

Rather than lone actors, hackers are members of a virtual community that reinforces their questionable legal decisions.²⁶ This community is rife with hierarchies that delineate individual actors’ motivations and experience. Hackers fall into the categories of Black, White, and Grey Hat hackers. Black Hat hackers reflect the culturally prevalent image of a hacker, someone accessing systems illegally and for malicious reasons. White Hat hackers focus on penetration testing—attempting to break systems to find their weaknesses and then make them more secure. Grey Hat hackers fall

²⁴ Ibid.
²⁶ Ibid.
into the morally grey area between White and Black Hat hackers. They might move between the two and may be driven by curiosity or ego. Further, hackers are commonly divided into elites and script kiddies. Elites are the most skilled developers who understand the systems they create and attack. Script kiddie, in contrast, is a derisive term to refer to amateur hackers who purchase or use predeveloped programs to conduct their hacking. They do not understand the technology they use as elites do, and so they are looked down upon by other hackers.

**Literature Review**

I locate this research within three relevant realms of existing literature, ultimately determining a framework for electronic civil disobedience and a hacker archetype that will guide the following case studies.

*The Validity of Hacktivism as Civil Disobedience*

The first pertinent area is the question of when hacktivism is civil disobedience. A 2002 article from philosophy professor Brian J. Huschle in the *International Journal of Applied Philosophy* provides an early evaluation of how civil disobedience can translate effectively to cyberspace. Huschle outlines a framework to understand this transformation of civil disobedience from the physical to the electronic sphere. First, he lists particular criteria for classifying an action as civil disobedience—these are an amalgamation of the various criteria explored in the previous section on the history of civil disobedience. According to Huschle, one must calculate that an injustice exists and

---


28 Siciliano, “7 Types of Hacker Motivations.”
decide to break a law to protest that injustice (either direct or indirect disobedience). Using a non-violent approach and exhausting other democratic methods of effecting change, one must commit civil disobedience as a public act. Most importantly to Huschle, the disobedient person must maintain respect for the rule of law, understanding that they may likely be punished for their disobedience, and that they can continue to protest the perceived injustice through legal action.  

He then applies these criteria to electronic civil disobedience (ECD), a specific subset of hacktivism that meets the criteria for civil disobedience. Four additional characteristics complicate protest in cyberspace. The first two refer to the effects of globalization and non-citizen protest and are thus beyond the scope of this paper. The third characteristic reconciles that someone can protest with anonymity or physical distance to avoid the consequences of their actions. The fourth acknowledges that a single person can also have a larger effect by protesting in cyberspace than they could protesting traditionally. With the intersection of these four unique characteristics, Huschle addresses potential challenges in meeting the standard criteria. First, he reconciles the ambiguity of the terms violence and non-violence in cyberspace by arguing that protestor’s intentions (seeking justice versus causing harm) fulfill the requirement of non-violence. Next, he notes that anonymity interferes with the condition that subjects accept the legal consequences for their actions. He also believes that making an act public involves seeing the people who conduct the act, though he acknowledges that sometimes a group will claim responsibility for a hack when individuals do not, still giving the work a public face.  

---


30 Ibid., 74.

31 Ibid., 76-78.
believes that true cases of electronic civil disobedience are uncommon, though not impossible. Electronic civil disobedience can exist, but it occupies a small space not to be confused with revolutionary or peaceful protests.\textsuperscript{32}

Huschle’s framework has necessary nuance in answering whether hacktivism can function as a form of civil disobedience, and it has been the jumping off point for many other scholars who share the belief that electronic civil disobedience is a feasible means of political participation. Recent research has more strongly posited that hacktivism is an important and usable protest technique, including a 2015 article in the \textit{New England Law Review} by law student Tiffany Marie Knapp. Rather than propose changes in the methods of hacking, she argues for amendments to the Computer Fraud and Abuse Act. The reforms she proposes include a provision regarding a hacker’s intent and scaling back certain first-time charges to misdemeanors, to more closely reflect equivalent crimes of traditional civil disobedience.\textsuperscript{33} Other lawyers, while exploring hacktivism and not electronic civil disobedience specifically, also advocate for changes to the CFAA to make online protests more feasible. In 2013, Joshua Adams, a masters of law student at the George Washington University, argued for decriminalizing certain forms of hacktivism altogether as a form of free speech protection, while maintaining reasonable limits, such as the non-protection of foreign hacktivists.\textsuperscript{34} Unlike Huschle, though, Adams does not address the complications of anonymity: how will law enforcement know if a hacker is an American citizen or not? A 2015 article in the \textit{Penn State Law Review} by law student

\textsuperscript{32} Ibid., 81.
Andrew T. Illig suggests other possible reforms to the CFAA. He proposes an amendment requiring hacktivists to notify a target of an impending attack and then pay for network repair costs, or requiring them to prove political motivation. Regardless of the feasibility of Illig’s and Adams’ suggested changes, they believe hacktivism is worth protecting.

These and other scholars agree that electronic civil disobedience has a place in American politics, which puts them in strong contrast with most computer security professionals. In a 2011 article for computer magazine *PC World*, information security writer Robert Vamosi claims that not one of the security experts he interviewed condoned hacktivism. Further, he cites an interview of a former hacker from the hacktivist collective Anonymous who disavowed his former work. With this single perspective of a reformed hacker, Vamosi makes the claim that hacktivism, particularly attacks that access secure or classified data, “could endanger lives—a high price to pay for increased security awareness.”

Steve Mansfield-Devine, the editor of technical journal *Network Security*, believes that no analysis of hacktivist motivations “alters the fact that most of the hacktivist actions are illegal. And the motivation is largely irrelevant to the victims.” The only benefit of hacktivism that he perceives is the increased demand for security professionals to defend against attacks. To ground his arguments, Mansfield-Devine cites directors and CTOs of security companies, the people who have an incentive to dissuade hacktivism. If more people see hacktivism as a legitimate form of protest,

---

companies will need to invest more money in protecting their assets or repairing damage. Security companies are biased, while academics do not have the same financial motivation to misrepresent the positive potential of electronic civil disobedience.

*A Sociology of Hackers*

The second relevant realm of research is the sociology of hackers, which provides a necessary understanding of the individuals participating in electronic civil disobedience. An early important document in this area is “A Portrait of J. Random Hacker,” compiled throughout the 1980s and 1990s as a part of the Jargon File, a glossary of computer slang curated by programmers. In 1983, the whole file was first printed in paperback as *The Hacker’s Dictionary*. According to the Jargon File, J. Random Hacker is “a mythical figure like the Unknown Soldier; the archetypal hacker nerd.” To build “A Portrait of J. Random Hacker,” the curators of the Jargon File compiled responses from 100 hackers to better understand what those archetypal hacker qualities were. While written over 20 years ago, this document provides lasting insight into a community that is often difficult to study. Insider knowledge could bias researchers, but here it helped them overcome challenges inherent to studying an underground community. The document explores everything from appearance and interests to food preferences, drug use, and sexual habits. Most relevant for my research are gender and politics. While hacker culture has more female participation than technical professions do, the field is still overwhelmingly male. Politically, different generations of hackers hold different views but are consistently anti-authoritarian.⁴⁸

The various works of Tim Jordan and Paul Taylor are among the most cited and respected research on the sociology of hacking. In a 1998 article in *The Sociological Review*, Jordan and Taylor shift the focus of hacking research from hackers as “pathological individuals” to members of a community. They examine six aspects of hacker culture. First is the ease with which hackers use technology. Second is an “ambivalent relationship” with secrecy, where hacks must be secret because of their illegality, but hackers have a strong tradition of sharing knowledge and seeking recognition within their community. This ties to the third aspect, anonymity, which refers not to the secrecy of the hack but to the secrecy of the hacker’s true identity. The fourth component is membership fluidity, referring to the high turnover rate of membership in the informal network of hackers. The fifth characteristic is male dominance and misogyny, which, combined with a competitive drive for the best hack, intensifies the macho hacker persona. The sixth aspect of hacker culture is the array of motivations for such dedication to their craft—addiction, curiosity, thrill, power, recognition, and service to others.39

As other research expanded on and confirmed these early articles, the hacker archetype solidified. Sociologist Brian Alleyne, who has hacking experience himself, published an article in 2011 in the tradition of Jordan and Taylor. He confirmed that the hacker population is “overwhelmingly male,” though otherwise diverse in background and political views. He also critiqued the trend of security professionals and publications dividing hacking into strictly good and evil for being overly simplified. In outlining different types of hacking, Alleyne brings attention to “tinkering,” or hardware hacking.

---

One example he provides is a dual-SIM card phone available in many developing countries, particularly on the African continent. These modified phones take advantage of cell networks’ differing rates and services in a non-costly way. Alleyne believes hardware hackers are overlooked because in American culture they are outnumbered by software hackers, and in developing countries they are seen as products of necessity that do not conform to Western perceptions of hacking.\(^{40}\)

*Gender in Hacktivism*

Leonie Maria Tanczer, a postdoctoral researcher of cybersecurity, collective action, and gender studies, draws on the research of Jordan and Taylor to further study the “male-only” stereotype of hacktivism. In a 2015 article with a sample of five women and five men, Tanczer conducted a discourse analysis of hacktivist communities, believing that a gendered analysis was particularly necessary for a community focused on creating social and political change. Language reflects and perpetuates cultural stereotypes, so it was an appropriate venue to study the gender biases of hacktivists. Though Tanczer’s sample size is small, she is the first to venture into studying the direct link between gender and hacktivism. In interviews with her subjects, she recognized four patterns of discourse. Most prominently, she identified Male Oblivious Discourse among the men she surveyed, wherein they overlooked gender entirely. Not acknowledging sexism is in itself a form of sexism, and a male identity in the predominantly male hacktivist community affords the privilege of seeing gender as a non-issue. Female hackers push back on this attitude through Female Discourses of Resistance. This is either an Emphasis Discourse, where they actively emphasize their identities as women

\(^{40}\) Alleyne, “‘We are all hackers now,’” 1-33.
and hackers and combat the sexism in the community, or Negation Discourse, where women struggle with feelings of exclusion and with justifying a hacktivist identity. When confronted with their sexism or erasure of women, men retaliate with a Male Justification Discourse, where they try to defend themselves and explain away their Oblivious Discourse.\(^ {41} \)

A specific experience that Tanczer cites as Negation Discourse is particularly interesting in the context of my work. One woman who did not participate in the study explained to Tanczer that she identified as an activist and a hacker but not a hacktivist because her hacking work was not recognized as “real hacking” by other hackers:

> teaching everyone at occupy how to use wordpress, or teaching sewing classes at a makerspace in a poor neighbourhood…Skills that are categorized as ‘feminine’ are not thought of as real work in our society, so because of systemic social prejudices both within the hacker culture and society at large, by definition women are often not hacktivists.\(^ {42} \)

Comparing this with the experiences of the other women in her survey, Tanczer concludes that when faced with the struggle to reconcile their female and hacktivist identities, some will altogether drop the label hacktivist. Men, who dominate hacking communities, set definitions and decide what is considered hacktivism. Because of men’s built-in gender biases, these definitions often exclude work perceived as more feminine.\(^ {43} \)

Jessi Ring, a PhD student in communications studying hacking and feminism, builds on Tanczer’s work to disrupt the idea of hacktivism as a male-only practice. In a 2015 article in *The International Journal of Critical Cultural Studies*, she argues for a broader view of hacktivism. She views hacking as a process and “a way of engaging with

\(^ {41} \) Leonie Maria Tanczer, “Hacktivism and the male-only stereotype,” *New Media & Society* 18, no. 8 (2016): 1599-1615.
\(^ {42} \) Ibid., 1606.
\(^ {43} \) Ibid., 1607.
systems” rather than an act. Because men and masculinity are the cultural default, viewing hacking or hacktivism as genderless just reinforces existing practices and male hegemony in the field. Women, LGBTQ+ people, and people of color engage with these systems in different ways, and feminist hacktivism, as Ring refers to it, encompasses this difference. In her definition of feminist hacktivism, she includes activities like crafting and tinkering. As Alleyne discussed, hardware hacking is often excluded from definitions of hacking. Ring brings these hacks into her definition of feminist hacktivism, building a more inclusive conception of hacktivism that includes individuals of diverse identities. She acknowledges the limitation of her work as only theoretical. She draws on interviews that other researchers conducted and published with feminist hacktivists, but she also sets herself a plan for expanding and bolstering this research. In a burgeoning field, Tanczer’s and Ring’s work provides the launching point for further research.

Relevant Frameworks

To create a consistent structure for each case study, I use two specific frameworks established by the preceding literature. First, I use Huschle’s framework of electronic civil disobedience to analyze each hack as it fits into his criteria. Second, I use the hacker archetype of anti-authoritarian men established by various authors to study the individuals or group conducting the hack.

I tie these two frameworks to the concept of psychological acceptability, traditionally used in computer security. It is one of the fundamental design principles for creating secure systems and networks: interfaces and settings must be intuitive and must work how non-expert users would expect, lest a user accidentally configure a system that

---

is insecure. If the security mechanisms are too complicated, the user might turn them off completely.\(^4^5\) Essentially, good system design will conform to a user’s mental model. I extend this principle to the use of electronic civil disobedience. For the public to perceive a certain hacktivist action as acceptable, it must fit into their mental model of what a protest looks like. Philosopher Tommie Shelby alludes to this with his term “impure dissent”—political speech that deviates from the standard by blending legitimate political arguments with atypical elements such as profanity, violent or pornographic images, or nicknames and colloquialisms.\(^4^6\) These do not nullify the content of the speech, but the way in which someone conveys information deviates from public perception of what political speech looks like. Protests conducted with impure dissent might face more criticism for their tactics than attention to their cause. Thus, psychological acceptability is also relevant in civil disobedience. Protests that do not conform to society’s psychological model are more difficult to understand, though not inherently invalid. I examine each of my case studies through this lens as well, analyzing whether they fit into hackers’ perceptions of hacking and law enforcement’s perceptions of civil disobedience.


Case 1: *Mr. Robot* Season 1

**Overview**

My first case study is the 2015 television series *Mr. Robot*, lauded as one of the most accurate portrayals of hacktivist culture in media. As addressed in the existing literature, researchers of hacking communities encounter the challenge of studying any illicit activity. So much of hacking takes place underground that getting a full understanding of the individuals who choose to use electronic civil disobedience is difficult. Other researchers have chosen to use a content analysis of popular media about hacking because in addition to fleshed-out characters, it provides insight into the culture that created the portrayals.⁴⁷ *Mr. Robot* not only provides deep insight into one archetypal hacktivist but also reflects the way American society perceives hacktivist culture.

The show follows protagonist Elliot Alderson, a cybersecurity engineer by day, as he joins the anti-capitalist hacktivist group fsociety, analogous to the real-world hacker collective Anonymous. Elliot quintessentially fits the hacker archetype of anti-authoritarian male, and he and fsociety utilize widely established tactics of electronic civil disobedience. After a summary of the show’s narrative and authenticity, I explain the goals of fsociety as an anti-capitalist anarchist organization and raise the concern of whether civil disobedience is justified in advancing a revolutionary cause. I also examine the specific hacks fsociety uses, in particular a distributed denial of service attack. After this technical discussion, I discuss how this case fails to fit into Huschle’s framework of electronic civil disobedience, making DDoS attacks an unreasonable approach for civil disobedience. I then study the ways in which Elliot and fsociety as a whole fit the hacker

---

archetypes of male and anti-authoritarian. I argue that their tactic makes their electronic
civil disobedience psychologically unacceptable to law enforcement, but the combination
of their tactic and archetypal identity leads other hackers to see it as a legitimate hack.
Elliot’s sexism limits his understanding of hacking to traditionally male attacks, which
leaves him few options for electronic civil disobedience that fits the perceptions of both
law enforcement and other hackers.

Narrative of Mr. Robot and Technical Background

Elliot Alderson embodies many quirks of a stereotypical hacker: he sports a black
hoodie, lives off of fast food, and is socially reclusive. He is profoundly lonely, and he
narrates Mr. Robot by addressing the audience as an imaginary friend. By expressing his
inner thoughts and many frustrations to the viewer, he tries to placate his isolation. He
suffers from anxiety, depression, an opiate addiction, and, revealed late in the first
season, hallucinations of his dead father.

Elliot works for Allsafe, a cybersecurity contractor whose focus is protecting
large corporations. E Corp, one of Allsafe’s primary clients, is the world’s largest
conglomerate. Elliot refers to the company as Evil Corp, believing the company is home
to the truly immoral people in the world. Elliot’s childhood friend Angela also works at
Allsafe as an account executive on the E Corp account. Both Elliot’s father and Angela’s
mother worked for E Corp, were poisoned in a toxic waste leak at one of the company’s
plants, and died from leukemia. One of the primary motivations for Elliot’s hatred of E
Corp is the company’s cover-up and poor treatment of his and Angela’s parents.

---

48 Mr. Robot, “eps1.0_hellofriend.mov,” episode 1, directed by Niels Arden Oplev, written by Sam Esmail,
USA Network, June 24, 2015.
One day at work, Allsafe CEO Gideon Goddard calls Elliot into his office to show him the evidence of a RUDY attack on E Corp’s servers, which Elliot describes as “awesome.” Gideon notes that the E Corp servers are being attacked nearly every week.\(^{49}\) A RUDY attack, which stands for “R U Dead Yet?”, is a type of distributed denial of service (DDoS) attack.\(^{50}\) Typically, a DDoS attack will overwhelm a server with requests for information so that a user looking to legitimately use a web page is unable to load it. When a user enters a URL into their browser, they send a request to a server that asks, “Are you there?” known as a ping. If too many pings occur at one time, the server cannot respond to any of them. A DDoS attack can come from many people colluding to refresh the same page at once, or malicious code can infect unwitting users and turn their machines into “botnets” so one central computer can manipulate other computers into nonconsensually sending pings.\(^{51}\)

For this action to be considered a DDoS attack, it must have the intent of bringing the server down. If many people try to access the same webpage at once, the server may be unable to manage the load, but the users did not intend to bring the server down. This distinction becomes important when hackers are prosecuted under the Computer Fraud and Abuse Act for DDoS actions, as the law specifies that attackers must cause “intentional damage.”\(^{52}\)

A RUDY attack is a slow-rate distributed denial of service. The connections between the user and server, while fewer in number, are kept open longer, eventually

\(^{49}\) Ibid.
\(^{52}\) Ibid., 12-13.
monopolizing the server’s resources and making it inaccessible to other users. Other DDoS attacks are often detected by the unusual spike of incoming requests to the server, but a RUDY attack subverts this detection by making fewer requests overall.\(^{53}\) (Appendix One shows a sample graph of a DDoS attack.) Visible in the graph is the spike in overall requests to a website, which means more people (or botnets) than normal are trying to access that server. Visualizing the attack helps to recognize a DDoS attack is happening and stop it, but because a RUDY attack will not send as many requests per second, the spike is not as high, and it is more difficult to detect. This characteristic makes RUDY attacks harder to protect against and a more effective technique to bring down targeted servers. Bringing down a server might bring down a website, but it could also have much more severe effects. Conducting a DDoS attack against critical infrastructure could take down financial and medical systems, water purification systems, or the power grid. The RUDY attack on E Corp’s server might have only affected a website, but the attack implies larger possibilities for disruption.

On a night soon after Gideon tells Elliot about the RUDY attack, an even more severe DDoS attack hits E Corp. Angela calls Elliot into the Allsafe office at 3 a.m. to help Lloyd Chung, the cybersecurity engineer on-call, manage what Lloyd calls “the worst DDoS attack I’ve seen.” Upon further examination Elliot expresses that he thinks the attack goes beyond a denial of service and that the attackers placed malicious code that allows the attacker to remotely take over a system, often undetected, known as a rootkit.\(^{54}\) When Elliot and Lloyd try to restart the E Corp servers, the virus replicates

---

\(^{53}\) “R.U.D.Y. (R-U-Dead-Yet?)?”

itself and crashes the servers, and in trying to defend against a typical DDoS attack, they unintentionally spread the virus through the whole system of many servers.  

This attack introduces Elliot to the hacktivist group fsociety. When inspecting the last infected server after isolating it from the rest of the system, he finds a file named fsociety00.dat. DAT files provide additional information about another program, in this case about the rootkit. However, Elliot believes finding the file was too easy, and he finds a note that says “LEAVE ME HERE.” He leaves the file, modifying the permissions so he is the only person who can access it. He is then approached by Mr. Robot, a man who leads the hacktivist organization fsociety, recruiting Elliot to join the group’s mission to “set in motion the largest revolution the world will ever see.” However, viewers later discover that Mr. Robot is a hallucination of Elliot’s father who Elliot does not recognize, implying that Elliot was the leader of the group all along. Through this convolution of Elliot’s brain, Elliot himself may be the one launching the DDoS attacks on behalf of fsociety. Darlene, Elliot’s sister and a member of fsociety, confirms that she and Elliot founded the group and it was his idea to launch these hacks, though Elliot does not remember this.

55 Mr. Robot, “eps1.0_hellofriend.mov.”
57 Mr. Robot, “eps1.0_hellofriend.mov.”
58 Mr. Robot, “eps1.7_wh1ter0se.m4v,” episode 8, directed by Christoph Schrewe, written by Randolph Leon, USA Network, August 12, 2015.
59 Mr. Robot, “eps. 1.8_m1rr0r1ng.qt,” episode 9, directed by Tricia Brock, written by Sam Esmail, USA Network, August 19, 2015.
**Authenticity and Real-World Parallels**

Though Elliot Alderson is a fictional character, he gives us a level of insight into the mentality and motivations of a hacker that are difficult to acquire elsewhere, particularly in the culture of anonymity on the internet. The creators and producers of *Mr. Robot* work hard to create authentic stories, and both Elliot’s character and the technology stand up to the scrutiny of hackers and cybersecurity experts. In the documentary *Mr. Robot_dec0d3d.doc*, Jeff Moss, real-life a hacker known as “Dark Tangent,” describes how fans of the show take screenshots of the code portrayed on the show and check for its authenticity. The show’s writer and technology producer Kor Adana leads a team of security and law enforcement experts in crafting realistic hacks, around which writers create storylines. *Mr. Robot* is a product of creators and writers who are mostly men, and it cannot be separated from the lens through which they view the world. Their views on gender and anti-capitalist movements will inevitably seep into the storylines and characters they craft.

Fsociety very directly parallels Anonymous, a prominent real-life hacktivist network that also uses DDoS attacks as one of its primary tactics. Anonymous first gained notoriety in 2008 when it took on the already controversial Church of Scientology, defacing and launching DDoS against some local chapter websites. The Church of Scientology filed a copyright claim to remove a copy of one of their videos of Tom Cruise from the video sharing site YouTube, but Anonymous fought back against what it viewed as censorship. In their video response, Anonymous warned that it had

---

60 *Mr. Robot*, “Mr. Robot_dec0d3d.doc,” special episode, USA Network, June 20, 2016.
decided that your organization should be destroyed, for the good of your followers, for the good of mankind, and for our own enjoyment. We shall proceed to expel you from the Internet and systematically dismantle the Church of Scientology in its present form.62

Adana cites this attack by Anonymous as the inspiration for fsociety’s assault on E Corp, where it also sought to fully destroy its target for an ambiguous greater good. Fsociety members wear masks to cover their faces, reminiscent of hackers for Anonymous who adopted the Guy Fawkes mask from the film *V for Vendetta*.63

**Movement Context**

Fsociety, while vague about its specific goals, seeks some sort of socialist or anarchist revolution.64 In their first encounter, Mr. Robot explains to Elliot that fsociety wants to destroy “the virtual reality of money” by bringing down one conglomerate and launching a financial meltdown, erasing the records of debt stored in data centers and ultimately bringing about wealth redistribution.65 Once they have encrypted and in essence destroyed all of E Corp’s information, fsociety publishes a masked video announcement, similar in style to Anonymous. They address the public:

Any money you owe these pigs has been forgiven by us, your friends at fsociety. The market's opening bell this morning will be the final death knell of Evil Corp. We hope as a new society rises from the ashes that you will forge a better world. A world that values the free people, a world where greed is not encouraged, a world that belongs to us again, a world changed forever.66

Fsociety crafts their vision for a new society with particular word choice. Referring to E Corp as “pigs,” they decry capitalism for its greediness and inhumanity. Then, the phrase

---

63 *Mr. Robot*, “Mr. Robot_dec0d3d.doc.”
65 *Mr. Robot*, “eps1.0_hellofriend.mov.”
66 *Mr. Robot*, “eps1.9_zer0-day.avi,” episode 10, directed by Sam Esmail, written by Sam Esmail, USA Network, September 2, 2015.
“rise from the ashes” conjures the image of a new society rising from smoking, post-revolutionary rubble. The image they create is a post-uprising reconstruction, but other than the redistribution of wealth and abolishment of debt, they are not specific about what this new society should look like.

The vagueness of fsociety’s vision may be attributable to inter-group disagreement about the details of this post-revolution world. Before the group releases the hack encrypting all of E Corp’s data, Trenton, a Muslim-American woman, shares a conversation with Darlene, Elliot’s sister. Trenton accuses Darlene of only seeking momentary anarchy and not legitimately caring about economic revolution because Darlene was eager to release the encryption hack before all of the backups had been destroyed, even if it did not work permanently. Trenton, conversely, tells of how her parents immigrated to the United States from Iran for freedom and a better life, but her parents have thousands of dollars of loans and work unfulfilling jobs; “They won’t shut up about how great America is, but they’re going to die in debt doing things they never wanted to do.”

Trenton and Darlene share a revolutionary urge, but they have different visions of what that post-revolution world should look like. For both of them, hacking is connected to changing the world and creating anarchism of different incarnations.

Authors Jeff Shantz and Jordon Tomblin believe that hacking is a particularly well-suited tool to advancing anarchism, as they explain in their book *Cyber Disobedience: Re://Presenting Online Anarchy*. They believe that cyber activists can draw from the principles of anarchism, particularly due to the many parallels between anarchism and hacktivism. They ground this opinion in early tech activists’ perception of

---

67 *Mr. Robot*, “eps1.6_v1ew-s0urce.flv,” episode 7, directed by Sam Esmail, written by Kate Erickson, USA Network, August 5, 2015.
the internet as a shared resource, a part of the communication commons, fighting against states and corporations who work to privatize it. The authors focus particularly on Anonymous and explain that the hacktivist collective’s structure looks similar to how anarchists organize. Just as anarchists are leaderless, Anonymous is a network of loosely-affiliated and non-hierarchical hackers who share common goals of justice, freedom, and accessible information; their only condition of participation is that hackers do not take credit for their work beyond the name Anonymous. Shantz and Tomblin compare certain actions by Anonymous and other hacktivists to real-world equivalents for civil disobedience—for example, they view a denial-of-service attack much like a virtual sit-in. Because police and government surveillance organizations have worked to stifle the development of offline radicalism, they have in turn encouraged more radicalization online.68 The internet provides a new venue for revolutionaries and anarchists to both organize and execute new types of attacks, uniquely well-suited to these social movements.

Other theorists of civil disobedience caution against the use of civil disobedience for revolutionary purposes because it does not adhere to a respect for the overarching legal system. Huschle, for example, does not believe that revolutionary acts are a valid form of civil disobedience, whether online or not, because they do not maintain respect for the overall rule of law. He would disagree with fsociety’s use of hacking because they sought to reform the entire system of capitalism, not a particular law that was unjust. The only condition he allows is that an act to protest an unjust state might be punished by an unjust legal system. For a minor crime, an activist could receive a major punishment.

68 Shantz and Tomblin, *Cyber Disobedience*, 1-2, 4, 7-8, 61, 105.
Only in a “severely unjust nation,” Huschle says, would revolutionary-oriented disobedience be justified. In his view, this would exclude the actions of fsociety from being legitimate, but particularly for Trenton and Elliot, they believe deeply that capitalism is severely unjust. Darlene might only be seeking momentary chaos, but they see capitalism as a grand injustice that can only be solved with revolutionary change. In their view, their work would fit into Huschle’s exception. Shantz himself is an anarchist which naturally colors his analysis and biases him toward seeing revolutionary civil disobedience as legitimate. This, though, is important in itself. Like Trenton and Elliot, his experience biases him to believe using civil disobedience to advance anarchism is legitimate. The benchmark of “severely unjust” is subjective and is not adequate to discount anarchist civil disobedience.

**Technical Tactics: Distributed Denial of Service**

Fsociety’s primary strategy of hacking is through denial of service attacks. This method is one of the most common forms of online protest, likely because the attacks do not require excessive technical knowledge to execute.\(^{69}\) A script kiddie could easily acquire and run the software. Sauter, a PhD student studying activism and technology, has written extensively on DDoS attacks as a technique of electronic civil disobedience. According to Sauter, denial of service attacks provide an attractive opportunity for people looking for low-cost tactics of engagement. Though not everyone who participates in a DDoS action will stay engaged with the cause, the strategy provides an easier step into activist work.\(^{70}\) Originally, experienced offline activists used DDoS attacks to utilize the

---

\(^{69}\) Sauter, *The Coming Swarm*, 15.

\(^{70}\) Ibid., 6.
internet as a new platform for their work. Nowadays, though, this hack is primarily used by members of the internet subculture focusing on internet-based issues.  

The examples of denial of service attacks in Mr. Robot are not as simple as most. Elliot and Lloyd’s reactions to both the first RUDY attack and the second DDoS/rootkit attack indicate that they are impressed by their strength and technical capability. Elliot’s reaction of labeling the RUDY attack as “awesome” frustrates Gideon. Rather than being upset by the attack, Elliot marvels at the complexity of the attack. For a hacker himself to be fascinated by a fairly standard approach speaks to the hack’s sophistication. Lloyd’s superlative calling the second attack the worst DDoS he has seen speaks to the same impression as the first. These hacks were beyond a standard denial of service in their complexity, gaining greater respect from hackers and cybersecurity professionals. 

Activists often compare DDoS attacks to strikes, blockades, and sit-ins, among other traditional tactics of civil disobedience; frequently, they refer to DDoS as “virtual sit-ins.” Like a sit-in, DDoS attacks are indirect disobedience, themselves an illegal action used to protest a larger injustice. They violate the Computer Fraud and Abuse Act, which criminalizes a person who “knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer.” Argyro Karanasiou, a law professor specializing in IT and media law, evaluates the comparison of DDoS attacks with offline protests and determines that none of the analogies fit well enough to protect

71 Ibid., 7.
72 Ibid.
DDoS as a form of free speech. Sauter acknowledges that while the common analogy to sit-ins is imperfect, hacktivist continue to claim that DDoS is their act of civil disobedience conducted online.

**Distributed Denial of Service as an Act of Electronic Civil Disobedience**

Despite hacktivists insistence that DDoS attacks are a tool of electronic civil disobedience, this tactic fails in many ways to meet Huschle’s framework of civil disobedience. As Huschle specifies, civil disobedience should be a public act. Academics disagree on whether DDoS attacks fulfill this requirement. Karanasiou does not believe DDoS attacks are a public act because a public act assuming a risk—being willing to sacrifice for the cause—which anonymous hacktivists do not do. Sauter, in contrast, places DDoS in a category of conduct-based activism, where acts rather than speech convey the message. These hacks are an imagined “visual spectacle of the mass,” similar to seeing a mass of protesters marching on the streets. The act itself speaks to the public. Nevertheless, for protests to gain media support, they must fit into the mental image of what the media expects a protest to look like. While hacktivists may see their DDoS attacks as civil disobedience, the media often does not distinguish between criminal and activist DDoS, or the media omits the political issues for coverage of the hack itself. Mr. Robot offers very little insight into media coverage of fsociety’s DDoS attack, but fsociety publishes their own video messages of a masked man speaking to the

---

75 Ibid., 101.
77 Ibid., 89.
78 Ibid., 60-61, 159.
public. They do not specifically reference their DDoS action, so how the public perceived the message is unknown. While many DDoS cases might be public acts, fsociety’s hack does not meet this requirement.

Civil disobedience must also be non-violent, which does not mean non-disruptive. Critics of DDoS attacks often compare them to past social movements without acknowledging that past movements have also practiced disruption. For example, casual consumers of history often cite Dr. Martin Luther King, Jr.’s propensity for nonviolence, forgetting that King also encouraged creating “tension” through direct action to force opposing parties into negotiation. Of course, Sauter acknowledges that it is easy to see past social movements as just with the benefit of hindsight, but disruption to one’s own status quo is less comfortable.79 Saunter believes drawing excessive parallels between old and current social movements is unproductive and simplistic, lacks the context of history, and often is used only to fault current activists. Upon properly examining past movements, one can see that disruption draws attention to a cause and does not in itself delegitimize a type of protest.80 DDoS actions disrupt the regular flow of internet traffic, but the question remains as to whether they qualify as non-violence. U.S. law defines the crime of violence as the use or attempted or threatened “use of physical force against the person or property of another.”81 Michael Turner, a University of Cambridge student of intelligence and international security, suggests that the target of a DDoS attack determines whether the act is nonviolent. If the targeted website being taken offline leads

---

80 Ibid., 51.
to destruction of property or loss of life, the attack should be considered violent.\textsuperscript{82}

Through this understanding, because the RUDY and second DDoS attack on E Corp did not hurt anyone or permanently damage property, the hack was nonviolent.

A third qualification of civil disobedience is that those who practice it submit to legal consequences for their protest. Activists who participate in sit-ins are typically charged with trespassing, which carries a $100 fine and/or 30 days imprisonment, or with resisting arrest, a $500 fine and/or two and a half years imprisonment.\textsuperscript{83} In contrast, a DDoS action can be very legally dangerous as the judicial system does not differentiate between criminal and political motivations.\textsuperscript{84} Hackers who engage in denials of service are charged with fraud, facing hundreds of thousands of dollars in fines and long prison sentences. With the threat of such harsh sentencing, the few defendants who are caught and arrested for participating in DDoS attacks often take plea deals, resulting in a lack of legal precedent in the United States to view DDoS as civil disobedience.\textsuperscript{85} A notable exception to criminal sentencing took place in Germany in 2001, when Andreas-Thomas Vogel organized a protest against Lufthansa Airlines’ website for the company’s participation in the deportation of immigrants. A German court viewed his actions as intended to “influence public opinion,” rather than as a “show of force.”\textsuperscript{86} They understood Vogel’s actions to fit within a model of civil disobedience in a way that American courts have not yet viewed DDoS attacks.

\textsuperscript{82} Michael Turner, “Is There Such a Thing as a Violent Act in Cyberspace?” (research paper, University of Cambridge, 2013): 5.
\textsuperscript{83} Sauter, \textit{The Coming Swarm}, 143.
\textsuperscript{84} Ibid., 103.
\textsuperscript{85} Ibid., 145.
\textsuperscript{86} Ibid., 140.
The lack of acceptance of legal action in *Mr. Robot* reflects anonymity, one of the issues Huschle raises in translating civil disobedience to cyberspace. Some organizations like the Electronic Disturbance Theater and *the electrohippies* shared their identities when conducting DDoS actions, while groups like Anonymous and fsociety have not. Sauter raises the valid criticism that the current approach to civil disobedience allows states, those in possession of power, to dictate the terms of protest for activists, often members of marginalized groups with little leverage. The state retains the power to decide the legitimacy of its own critics, leaving little opportunity for oppressed voices to air their complaints unless they are willing to risk everything. Activists are unlikely to discard their anonymity while at risk for such severe legal prosecution, but the legal system will not change until it views DDoS acts as civil disobedience. Because DDoS actions operate within existing spheres of the internet rather than by creating new spaces, in conflict with the aforementioned rights of private property owners, they might be seen as acts of trespassing. Were the state to pursue sentences similar to trespassing for participants in DDoS attacks, both parties could shift their understanding of DDoS attacks to more closely match traditional civil disobedience. The current users of DDoS, though, cling to anonymity.

Another challenge in the translation of civil disobedience to the internet is the previously raised issue of non-volunteer botnets in DDoS attacks. In the 1999 Seattle protests against the WTO, the British-based hacktivist group *the electrohippies* used “client-side distributed actions,” meaning that many individual users (i.e. clients) must

---

87 Ibid., 99.  
88 Ibid., 90.  
89 Ibid., 3-4.
actively participate in the denial of service attack. They believed that this created “democratic accountability,” as a significant mass of people must participate for the DDoS attack to have any impact.\textsuperscript{90} Since the late 1990s, though, technology for defending systems against DDoS attacks has improved, and volunteer-based attacks rarely result in downtime for the sites of major corporations.\textsuperscript{91} Now, people can volunteer their machines to act as botnets, so organizers can execute the DDoS at their chosen time while their volunteers are not on their computers. While this type of attack requires less involvement from them, volunteers are still willing participants in this democratic form of DDoS.\textsuperscript{92}

Conversely, organizers can turn computers into non-volunteer botnets by infecting computers with viruses that allow the organizers to remotely control the machines and use them as participants in a DDoS attack. When done without the consent of the computer’s owner, this raises huge ethical questions about the action’s political validity. Still, there are other methods of multiplying the amount of traffic to a website without the use of botnets.\textsuperscript{93} In \textit{Mr. Robot}, both the initial R.U.D.Y attack and the second DDoS attack could theoretically be executed in any of these ways, but given the small size of fsociety, it seems likely that the group used botnets in their attacks, potentially nonconsensual botnets, potentially to the risk of their legitimacy. Later, after fsociety has launched its encryption attack to destroy debt, Darlene tells Elliot that their group has grown wildly popular. People want to join fsociety and are protesting across the city in

\textsuperscript{90} Ibid., 43.  
\textsuperscript{91} Ibid., 71.  
\textsuperscript{92} Ibid., 129.  
\textsuperscript{93} Ibid., 10-11.
their support. If fsociety were to launch another DDoS with the support of those masses, they could use volunteer botnets, and that attack would be more justified in a framework of civil disobedience. Still, Sauter warns against judging the legitimacy of a protest by the group’s pool of resources. They differentiate between technological effects and actual effects: the same attack, when launched against a large corporation, could draw lots of attention but do little to hurt the company but could decimate a small website with little notice. They urge that “we not privilege technological facts over the motivations and stated goals of the participants and the actual effects of the action. To do so […] ultimately devalues human agency in our dealings with technology.” The potential use of botnets, though, is but one of many criticisms of fsociety’s approach. Within Huschle’s framework, these DDoS attacks cannot be classified as civil disobedience.

**Elliot as Hacker Archetype**

In discussing Elliot as the individual leading fsociety’s hacks, his gender and political views are relevant to understanding this imperfect use of electronic civil disobedience. Both of Elliot’s identities fit into the dominant categories of male and anti-authoritarian established in the review of existing literature. With his use of conventional hacking tactics, inhabiting these dominant identities makes him the quintessential hacktivist.

---

94 *Mr. Robot, “eps1.9_zer0-day.avi.”*

**Gender**

In a pop culture critique, technology writer Joanne McNeil brings light to the reflection of these hacktivist gender issues in *Mr. Robot*. The show’s female characters pale in the shadow of Elliot’s complexity. An article from technology magazine *Wired* calls fsociety a “paint-by-numbers ensemble cast” and argues that none of its members besides Elliot demonstrate any sign of skills capable of executing their grand hacks. An African-American man and Muslim woman are thrown into the group for token diversity, but neither are given much complexity or character. Darlene, Elliot’s sister and a member of fsociety, is arguably the most prominent woman on the show, and even her characterization is shallow. McNeil bemoans how instead of being “smart and strong willed, [Darlene] is shallowly crass and aggressively one of the bros.”

Tanczer explains that the creation of technology is often conflated in language with masculinity and power, while receiving and using technology is feminine. A portrayal of Darlene as “one of the bros” plays into the consistent depiction of hacking as masculine, though in this case not male. Darlene herself participates in something akin to Tanczer’s Male Oblivious Discourse. As a masculine woman, she conforms to the dominant masculine identity, overlooking gender in hacktivist spaces. Because she fits the masculine archetype, she does not diversify the group’s perspective on hacking.

Elliot’s response to his friend Angela’s struggles further demonstrates how he follows the tropes of his gender. *Mr. Robot* asks Elliot to change the IP address in the

---

97 Zetter, “*Mr. Robot* Is the Best Hacking Show Yet—But It’s Not Perfect.”
98 McNeil, “The First and Second Rules of Mr. Robot.”
99 Tanczer, “Hacktivism and the male-only stereotype,” 1601.
fsociety00.dat file he found to make it appear that the DDoS attack came from the computer of Terry Colby, CTO of E Corp. When Angela, as the account executive, and Elliot meet with Colby to discuss the hack, Colby praises Elliot’s work, but he patronizes Angela and refuses to listen to her. Elliot defends how Angela responded to the attack, but Colby kicks her off the case, saying, “She’s not going to work out for us, not on this level. We need to stick to the more tech savvy here.” Colby believes that Angela is unqualified to discuss the hack. Upset by this disrespect for Angela, Elliot is persuaded to frame Colby and passes the investigators a folder listing an IP address that will lead back to Colby’s computer. After the meeting though, Angela refuses to talk to Elliot. Weeks later, she reveals she was embarrassed by Elliot’s response. She tells him, “You didn’t have to stick up for me in there. I know that you were just trying to help, just don’t do it again. Even if I’m losing, let me lose, okay?” Elliot believed he was defending Angela from Colby’s overt sexism, but his comments perpetuated the trope of Angela as the helpless woman in need of saving, of the boy rescuing the girl. Elliot himself may have felt he was acting out of friendship and not in a male savior role, but Angela’s response clearly indicates discomfort in her gendered role at the company. She does not want to be seen as needing defense and wants to hold her own. Using Tanczer’s analysis of gendered discourse in hacktivist communities to understand this interaction, Elliot participates in Male Oblivious Discourse, where he never acknowledges gender and therefore subtly perpetuates sexism. Though he may not explicitly express misogynistic ideas, his male identity affords him the privilege of not having to see gender, which itself is sexist. The male dominance in hacking communities also brings sexism to those communities, and as

100 *Mr. Robot*, “eps1.0_hellofriend.mov.”
a product of male writers and a culture steeped in patriarchy, Elliot reflects that sexism. His male gender, as well as the biases that brings, fulfill the hacker archetype.

**Politics**

Elliot also holds anti-authoritarian political views reflective of the hacker archetype, which interact with a “greater good” mentality to form his motivation for his hacktivism. Lance James, chief scientist at Flashpoint, the leading company in providing business risk intelligence, has over a decade and a half of experience in information security. Interviewed in *Mr. Robot_dec0d3d.doc*, James said that compared to other media depictions of hackers, Elliot is strikingly accurate for his psychological profile as well as his skills. His disillusionment with society and participation in counterculture reflect experiences James has seen in many real-life hackers. Ryan Kazanciyan, chief security architect at security company Tanium and a technical consultant for *Mr. Robot*, concurs that hacktivism often reflects an anti-establishment perspective. Particularly in crafting Elliot’s character, Egyptian-American show creator Sam Esmail took inspiration from the Arab Spring, where young people used technology to productively “channel the anger against the status quo” for change.

For Elliot, his anti-establishment view is rooted in cynicism toward capitalism. Elliot admits, “Sometimes I dream of saving the world. Saving everyone from the invisible hand, one that brands us with an employee badge. The one that forces us to work for them. The one that controls us every day without us knowing it.”

---

102 *Mr. Robot*, “Mr. Robot_dec0d3d.doc.”
103 Zetter, “*Mr. Robot* Is the Best Hacking Show Yet—But It’s Not Perfect.”
104 *Mr. Robot*, “eps1.0_hellofriend.mov.”
alludes to philosopher Adam Smith’s theory of the invisible hand, which suggests that in a free market economy, self-interest will drive individuals and the economy will guide itself to a point of equilibrium of supply and demand.\textsuperscript{105} Elliot turns this symbol of capitalism on itself to highlight the negative sides of the system, particularly a blind obedience and hyper-focus on money. Elliot further believes that there is “a powerful group of people out there that are secretly running the world, […] the top one percent of the top one percent, the guys that play God without permission.”\textsuperscript{106} He is at his core driven by this anti-authoritarian, populist belief that this group of elites guides political and corporate decisions unbeknownst to the public, and financial and political power should be returned to the people.

The \textit{Wired} article frames Elliot as a classic jaded young person, which lends itself to anti-authoritarianism and a disdain for the status quo. Simply, “Elliot is Ponyboy for the digital age, a kid forced into early adulthood through tragedy.”\textsuperscript{107} With a reference to the young narrator of S.E. Hinton’s 1967 coming-of-age novel \textit{The Outsiders}, this perspective views Elliot with typical youth disillusionment. Elliot is the replica of a timeless character for a digital age. \textit{Mr. Robot\_dec0d3d.doc} also suggests that one of the reasons for the show’s huge success is that it “speaks to the current generation’s corporate culture and to their frustration with the status quo.”\textsuperscript{108} Multiple times, Elliot thinks to himself or utters the phrase, “Fuck society,” which becomes the moniker of his

\textsuperscript{106} \textit{Mr. Robot}, “eps1.0_hellofriend.mov.”
\textsuperscript{107} Zetter, “\textit{Mr. Robot} Is the Best Hacking Show Yet—But It’s Not Perfect.”
\textsuperscript{108} \textit{Mr. Robot}, “Mr. Robot\_dec0d3d.doc.”
organization, fsociety. This mentality speaks to alienated Millennials and makes Elliot a compelling character motivated by a revolutionary ideology.

When Mr. Robot first asks Elliot to frame Terry Colby for the DDoS attack, Elliot is hesitant. But as he rides the subway home, he sees an advertisement asking, “How Will I Repay My Student Loan Debt?” From his apartment, he hacks Angela’s bank account and finds that her student loan debt is nearly $200,000. He reads news articles on “Debt Slavery, the New American Dream” and the increasing global gap between the rich and the poor. Elliot’s research further persuades him that E Corp holds much of the world’s excessive debt, building resentment that encourages him to participate in fsociety’s takedown of the company. Seeing Angela’s bank account, though, makes a global issue personal, and Elliot is compelled to help her. Ultimately, his gender and political views interact to push him into action when he decides to frame Colby at the aforementioned meeting.

Elliot’s activist mentality assures that his work is at its core always human. His drive to serve the greater good works in conjunction with his anti-establishment views to create his identity as a hacktivist seeking revolution. Initially, his altruism surfaces as legal impulses. When he first learns about fsociety at the arcade, he thinks to himself that the fsociety00.dat file contains the arcade’s IP address, which would be enough evidence to take to law enforcement. Elliot feels driven to do the “right” thing, which here manifests in his consideration for turning the group in. He then reconciles this urge with the understanding that the right decision is not always the legal one. Because of this analysis, Kor Adana classifies Elliot and fsociety as Grey Hat hackers, led by good

---

109 Mr. Robot, “eps1.0_hellofriend.mov.”
110 Ibid.
intentions despite some of their highly illegal practices. Ultimately, Elliot wants his work to serve humanity at large, and he is not bound by legality. He distinguishes between what is legally right and, in his view, morally right, and he follows the latter, as practitioners of civil disobedience do. Mr. Robot presents a strong hacker archetype with Elliot’s character. He fits the cultural understanding of who a hacker is.

**Psychological Acceptability**

This case represents the perpetual challenge of hacktivists: while other hackers see their work as electronic civil disobedience, the law does not. There is no question that a distributed denial of service attack is an accepted type of hacking, but it functions less effectively as a type of activism. Because of the common use of DDoS tactics for criminal purposes, law enforcement does not see the hack as civil disobedience. Therefore they make no distinction based on intentions of an attack as criminal or activism. Within this current perception, DDoS attacks are not a feasible technique of civil disobedience, but fsociety defaults to the use of DDoS for their activism. This limit in perspective comes from their archetypal identity. In addition to the linguistic patterns that Tanczer’s research identified, she found that women largely opposed “destructive and illegal” hacktivism, including DDoS attacks. Linking Elliot’s gender and his technical approach, the choice of a DDoS attack is a masculine decision. His ingrained sexism sets limits on his perspective of the definition of hacking. To break into computer systems is a masculine understanding of hacking. Because of the limits on his definition, he also limits his options for civil disobedience.

---

111 *Mr. Robot,* “Mr. Robot_dec0d3d.doc.”
112 Tanczer, “Hacktivism and the male-only stereotype,” 1605-1606.
The internet slang used by many hackers bleeds into their activist work, creating an instance of philosopher Tommie Shelby’s impure dissent. The most notable example in *Mr. Robot* is the label fsociety, an abbreviation of the explicit phrase “Fuck society” that Elliot repeats. With their language, fsociety diverges from a common understanding of polished and respectable activism. This does not detract from their cause, but it makes it more difficult for outsiders to perceive them as activists. In *Mr. Robot*’s world, society does not have the same challenges accepting the activism of fsociety, but no real-world hack has gained such traction and mass support. While Elliot may be able to use a DDoS attack in his activism, that approach is not widely feasible for real-life hacktivists. The association of the act is too criminal, and courts do not offer leniency in sentencing for civil disobedience conducted through DDoS attacks. Removing the mental limits imposed by sexism introduces new options for civil disobedience that law enforcement recognizes. With a traditional tactic and dominant identity, Elliot represents the problem with much of current hacktivism—he limits his options to ones that law enforcement will not accept.
Case 2: Aaron Swartz and Freedom of Information

Overview

My second case study is the work of Aaron Swartz, a prodigious programmer, entrepreneur, and activist. Swartz was arrested in 2011 for downloading hundreds of thousands of academic journal articles from the JSTOR database in violation of their legally binding Terms of Service preventing automated downloading. Under the CFAA, Swartz was charged with 13 felony counts including wire fraud, computer fraud, unlawfully obtaining information from a protected computer, recklessly damaging a protected computer, aiding and abetting, and criminal forfeiture. After two years of legal bargaining, Swartz committed suicide in 2013. Though Swartz never stated publicly if his downloading was an act of civil disobedience, activists perceived it as such and have since held him up as a fighter for open access and freedom of information. With posts from Swartz’ personal blog and published interviews with him, his family, and his peers, contextualized with scholarly articles from academics and librarians, I use Swartz’ case as an example of relatively low-tech electronic civil disobedience related directly to the policies and culture of the internet.

While Swartz fits into the dominant identity categories of the hacker archetype, he navigates his identity with more nuance than Elliot in Mr. Robot. Simultaneously, his work fits a different, broader definition of hacking than Elliot’s, while still conforming to society’s perception of what electronic civil disobedience looks like. Through a feminist lens, Swartz viewed hacktivist culture less rigidly than someone with Elliot’s perspective and thus saw more available avenues of protest. The execution of his protest raises the issue of attempted anonymity, but Swartz maintained respect for the prevailing legal
system in an effective use of civil disobedience. Yet this implementation of electronic civil disobedience remains widely inaccessible so long as courts continue to see no distinction between criminal and activist hacking. Swartz’s use of technology, though less conventional than Elliot’s, was still too similar to the court’s understanding of criminal hacking. Though Swartz held less rigid views of gender and thus less constrained views on the definitions of hacking, his approach still ventured too close to criminal hacking.

Swartz’ Narrative

From his childhood, Aaron Swartz surrounded himself with computers. According to a profile of him published in *The New Yorker*, by his early teens, he was working alongside top innovators to develop new internet technologies. In his twenties, he extended his interests into politics, where he often fought to maintain freedom of information on the internet. Swartz’s early life was wildly successful, but at age 26, he killed himself, in the midst of a legal battle for violating the Computer Fraud and Abuse Act. Prosecutors drew heavily on the Guerilla Open Access Manifesto, a document co-authored by Swartz that encouraged the use of civil disobedience to protest the privatization of information. Since his death, advocates for an open internet have held Swartz up as a martyr for their cause, interpreting his illegal downloading as an act of civil disobedience.¹¹³

Swartz grew up immersed in technology and encouraged to innovate. In a documentary film about Aaron Swartz, Aaron’s brother Ben describes Aaron’s discovery

---

of the computer at a young age: “There was always something to do, always something that programming could solve. The way Aaron always saw it is that programming is magic. You can accomplish these things that normal humans can’t.”\textsuperscript{114} Though Swartz voraciously consumed new knowledge—teaching himself to read at three years old—he disliked an education system that favored memorization and busy work over critical thinking.\textsuperscript{115} He then began to question the society that created it.\textsuperscript{116}

At age 12, Swartz built the Info Network, a website where people could contribute information to articles about things they knew about, similar to the not-yet-created Wikipedia. This was his first foray into the world of crowdsourcing content and open access, a world to which he would often return.\textsuperscript{117}

At age 13, Swartz joined the online programming community designing the RSS tool, an abbreviation for Rich Site Summary or Really Simple Syndication. Instead of individually checking many different websites or blogs for updates on each of them, an RSS feed summarizes the contents of these sites into one place. Masked by the anonymity of the internet, the community members building RSS were unaware that the sharp, technologically literate contributor with the screen name Aaron Swartz was so young. His parents allowed him to connect with these communities offline where he could further engage intellectually.\textsuperscript{118}

Poised between the old age of copyright laws and the new age of freedom on the internet, Swartz took an interest in copyright. With Harvard law professor Lawrence

\textsuperscript{114} The Internet’s Own Boy: The Story of Aaron Swartz, directed and produced by Brian Knappenberger (2014; Los Angeles: Luminant Media.) Online.


\textsuperscript{116} The Internet’s Own Boy.

\textsuperscript{117} Ibid.

\textsuperscript{118} Ibid.
Lessig, Swartz helped to develop Creative Commons, a new model for copyright on the internet. Lessig describes Creative Commons as “some rights reserved” in contrast to traditional copyright’s “all rights reserved.” Creative Commons specifies different degrees of permissible usage, such as whether users can create adaptations of a licensed work, can use the work commercially, or must include an attribution. Now 15 years old, Swartz was in charge of the technical implementation of Creative Commons.\footnote{Ibid.}

In 2004, Swartz began studying at Stanford University, expecting stimulating scholarship but instead finding “a babysitting program for overachieving high schoolers,” as his friend, author Cory Doctorow described Swartz’s experience. After one year, Swartz left college to join the startup incubator Y Combinator. There, Aaron created Infogami, a tool to build websites, which then merged with another Y Combinator project, Reddit. Reddit provides a discussion forum for user-generated news, and in 2005 usage was growing rapidly. Media conglomerate Condé Nast took interest and bought Reddit for tens of thousands of dollars.

After the purchase, Swartz moved to San Francisco to work in the offices of Wired, another Condé Nast company, but he found his work and the monotony of office life unsatisfying. Swartz blogged often about politics, but tech culture was not conducive to his political engagement. Gabriella Coleman, an anthropologist studying hacking and online activism who knew Swartz, noted that “Silicon Valley just doesn’t really quite have that culture that orients technical activity for the purpose of political goals.”\footnote{Ibid.}

Working at Wired, Swartz was surrounded by people who did not share his engagement...
in politics, which he found maddening.\footnote{Aaron Swartz, "Office Space," Raw Thought (blog), November 15, 2006, http://www.aaronsw.com/weblog/officespace.} Here, Swartz’ life begins to diverge from the startup work of his teens into more politically-motivated efforts in his twenties.

Swartz first clashed with the law in 2008. Brewster Kahle, founder and digital librarian of the Internet Archive, attributes Swartz’s legal trouble to Swartz’s goal to “bring public access to the public domain.”\footnote{Ibid.} Federal court records are stored in the Public Access to Court Electronic Records (PACER) database behind a paywall, requiring users to provide a credit card number to access the information. Swartz worked with activists and programmers Steve Shultze and Carl Malamud on multiple approaches to download documents for free, procuring 2.7 million files before the courts blocked their access “pending an evaluation.” When courts saw such massive downloading, they froze the downloading and brought in law enforcement to evaluate whether there had been a security breach.\footnote{Timothy B. Lee, “The inside story of Aaron Swartz’s campaign to liberate court filings,” Ars Technica, February 8, 2013, https://arstechnica.com/tech-policy/2013/02/the-inside-story-of-aaron-swartzs-campaign-to-liberate-court-filings/.} Malamud created a website to make the acquired documents openly available. Swartz and Malamud spoke to the New York Times about their work, and the FBI began to investigate Swartz’ actions. Because neither the library nor PACER explicitly forbids remote downloading, the FBI closed their investigation without bringing charges against him.\footnote{The Internet’s Own Boy.} Swartz’s work was suspect but ultimately not criminal.

Swartz then branched out into political causes not directly related to the internet. He cofounded the Progressive Change Campaign Committee, a platform for people to organize for different progressive causes over the internet. One of the group’s notable
achievements was initiating the grassroots campaign to elect Elizabeth Warren to the Senate.\textsuperscript{125} In 2012, the group reported having over 850,000 members across the United States. As a registered political action committee, it is funded by individual donations under $5000. It criticized President Obama for taking inadequately liberal stances. Most of the organization’s money is spent in advertising for progressive candidates.\textsuperscript{126}

After founding PCCC, Swartz delved into the work that would earn him his notoriety. Because of his love of learning and libraries, he took interest in the distribution of academic journal articles. Many scholarly journals are supported through taxpayer money or government grants, but then users, or often universities, must pay again to access the articles. These fees lock out non-American students and researchers, in particular. Swartz chose to focus on the JSTOR database.\textsuperscript{127} To publish an article on JSTOR is a lengthy process. Academics spend years on their academic research, funded by government grants and university money. They submit their paper to an academic journal, run and subsidized by a university. The work is subjected to the scrutiny of an editor and peer review board. After the author makes changes, the journal editor sends a group of articles packaged together to a for-profit publisher. Publishers then sell the rights to the article to academic search engines such as JSTOR. Publishers profit, and JSTOR has to earn back the money it spent to acquire the article. It charges for subscriptions to its service and restricts the availability of articles to only those with a subscription. This cycle limits availability of research for the very academics doing the research. Though funded by public money, the research is not publicly available.

\textsuperscript{125} Ibid.
\textsuperscript{127} Ibid.
Activists decry this privatization of knowledge as staunching innovation. Swartz took interest in the injustice of this process.

In 2010, Swartz was working with Lawrence Lessig as a fellow at Harvard’s Berkman Center for Internet and Society, often visiting MIT’s campus as well. At MIT, Swartz connected with others who shared the school’s spirit of hacking. The campus also had an open network, so were he physically on campus he would have access to the school’s subscription to JSTOR and notoriously fast internet. On September 24th, he registered a newly purchased laptop on MIT’s network, using the name Gary Host; the network would see this user as “GHost.” Swartz wrote a script, a program to run automatically, that would download articles continuously from JSTOR. The code itself, written in the Python language, was fairly simple. The articles in the database had a basic numbering system, so the program could grab them sequentially. This continuous downloading was explicitly prohibited in JSTOR’s terms of service, which specify that users cannot “undertake any activity such as computer programs that automatically download or export Content.” To do so could encompass a number of violations of the CFAA, including unauthorized access to a protected computer or computer fraud. When JSTOR detected unusual access to their databases and blocked Swartz’ computer, he spoofed his IP address, tricking the network into thinking it was a different computer trying to access the database. Eventually, to speed the process even more, Swartz plugged directly into the network from an unlocked supply closet instead of connecting through

---

129 Nanos, “Bob Swartz: Losing Aaron.”
130 *The Internet’s Own Boy*.
WiFi. The police traced the downloading to his laptop in the closet and installed a surveillance camera, finally catching him.132

In early 2011, Swartz was arrested by MIT campus police and a U.S. Secret Service agent, who was collaborating with the Cambridge police on the New England Electronic Crimes Task Force, a creation of the PATRIOT Act to investigate the “use of schemes involving new technology.”133 Those around Swartz at the time described him as upset, stressed, depressed.134 The year was high time for activism online and offline as the Arab Spring spread, Anonymous launched numerous online campaigns, and the government dealt with the fallout of Wikileaks’ publication of leaked documents from Army soldier Chelsea Manning. In July, Swartz was indicted on four felony counts—wire fraud, computer fraud, unlawfully obtaining information from a protected computer, and recklessly damaging a protected computer135—on the same day that two LulzSec hackers in England were arrested. Swartz’s brother Ben and father Robert speculated that Aaron’s actions looked similar enough to other hackers’ that prosecutors wanted to use his case for deterrence.136 Even once JSTOR dropped their civil case against Swartz, the government continued to prosecute a criminal one.137

In the interim, Swartz continued his activism. In October 2011, the internet took up arms against the Stop Online Piracy Act (SOPA), a bill that would require internet service providers (ISP) to block an entire website for one copyright violation. For example, if one user uploaded pirated work onto video sharing website YouTube, the

---

132 MacFarquhar, “Requiem for a Dream.”
133 The Internet’s Own Boy.
134 Ibid.
136 The Internet’s Own Boy.
137 Liljeblad, “Understanding the Complexities of Civil Disobedience,” 197.
entire site would be in violation. Believing this would irreparably damage the core structure of the internet, Swartz began to organize against the bill. Through Demand Progress, an online activism organization that he cofounded, Swartz helped with widespread mobilization. Many websites including Wikipedia and Reddit engaged in an internet “blackout” day where their pages were unavailable and instead displayed anti-SOPA messages that reminded users of the importance of free information. The White House declared their opposition to the bill, and members of Congress began flipping their positions against the bill as well, eventually recalling the bill altogether.\textsuperscript{138}

In September 2012, courts added additional felony counts against Swartz, making a total of 13 charges. Eleven of those involved the Computer Fraud and Abuse Act (CFAA). According to his father, Swartz was terrified of the idea of imprisonment.\textsuperscript{139} He and his lawyer declined a plea deal in favor of a trial. His family and friends were worried for his mental health as he isolated himself from them. Displaying a façade of composure on his blog, Swartz did not mention the impact of his troubles on his mental health, but he felt the effects deeply. On January 11, 2013, he hanged himself in his apartment.\textsuperscript{140}

His family and friends decried the prosecutorial overreach that they believe contributed to Swartz’s death. Quinn Norton, Swartz’s ex-girlfriend and a journalist covering hacktivism and internet politics, lamented that Swartz was “the internet’s own boy, and the old world killed him.” Responding to Swartz’s death, Representative Zoe Loftgren and Senator Ron Wyden introduced an act into Congress to reform the CFAA,

\textsuperscript{138} The Internet’s Own Boy.
\textsuperscript{139} Nanos, “Bob Swartz: Losing Aaron.”
\textsuperscript{140} Ibid.
named “Aaron’s Law.” Posthumously, Swartz became a symbol and a voice for the freedom of information on the internet, values he lived his life pursuing.\footnote{Ibid.}

\textit{Movement Context}

Swartz’s previous experience in open access activism lent context to his downloading. In Swartz’s case, prosecutors discovered the Guerilla Open Access Manifesto, a document published and signed by Swartz in 2008. Speaking to prosecutors, Swartz’s ex-girlfriend Quinn Norton mentioned the document, which had been written by Swartz and three others, edited by Norton, and signed solely by Swartz.\footnote{Ibid.} The radical document encourages civil disobedience to protest the privatization of information and is fitting with Swartz’s history of politically engaging with the open access movement.

Denise Troll Covey, a librarian at Carnegie Mellon University, defines open access as the movement toward free online availability of journal articles with the permission of the author. She defines two worlds of knowledge, one where researchers should be ethically driven to share their knowledge freely, and knowledge itself cannot be owned; and the second where researchers must express that knowledge through a fixed artifact that can be owned and copyrighted. Researchers typically sign over their copyrights to the journals that publish their articles, and the price of journal subscriptions escalates, so the researchers often infringe on the copyright of their own articles by making them available on their personal websites—sometimes intentionally violating copyright, sometimes unknowingly. Publishers, motivated by profits, worry about

\footnote{Ibid.}
researchers distributing their own work, but no publisher has yet charged a researcher with copyright infringement.¹⁴³

Librarians, argues Covey, have a duty in their positions to participate in civil disobedience to advocate for open access. Librarianship is dedicated to service, to “organize, preserve and provide equitable access to resources.” As Harvard law professor Lawrence Lessig concurs, “the motive to give deserves as much respect as the motive to get.” Researchers, particularly those who knowingly violate the copyright to their own work, wish their work to have the widest distribution possible.¹⁴⁴ The nature of research is to build on previous knowledge, but privatizing knowledge prevents that growth. Swartz shared these beliefs that the open access movement serves the public by making knowledge more widely available and encourages the development of further knowledge.

In the Guerilla Open Access Manifesto, Swartz encouraged everyone to fight back against the privatization of information, against powerholders who controlled the distribution of information and were reluctant to relinquish that power. He explicitly advocates for civil disobedience to break the status quo of unjust copyright law:

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, filing download requests for friends.¹⁴⁵

Swartz listed these two examples of common internet practices, though often not thought of as civil disobedience. With a concerted and widespread effort, he believed that

¹⁴⁴ Ibid.
everyday users of the internet could reclaim a space founded to foster the free exchange of ideas. These acts of civil disobedience would change unjust copyright law to make knowledge available to everyone, not just those privileged enough to pay or have access to a database subscription.

Even with Swartz’s history of activism for open access, exactly what he planned to do with the JSTOR articles is unclear. He often enjoyed sorting through large sets of data, and his father Bob thinks it most likely that Aaron was planning to analyze the funding sources of the articles for signs of corrupt science, similar to a project he had previously done on a legal database with Lessig. Nevertheless, prosecutors cited the Guerilla Open Access Manifesto to spin Swartz’s hacking as an act of civil disobedience, and open access advocates have also claimed his actions as acting in their favor.

Swartz was not the only person to use this technically elementary hack to advance the open access movement. His arrest inspired others to add downloaded articles to filesharing sites. The same year of his arrest, scientists created the hashtag #ICanHazPDF to facilitate sharing articles. With this hashtag, one researcher can post a tagged request on Twitter for a specific article, and a stranger with database access can send the researcher the requested article. In 2012, Alexandra Elbakyan, a graduate student in Kazakhstan, set up Sci-Hub, a database of pirated journal articles. As of 2016, her database contained approximately 50 million articles, and she openly claims responsibility for her site’s creation. She also speaks about her fight for open access, influenced by her childhood in a former Soviet state where access to the internet and

---

146 Nanos, “Bob Swartz: Losing Aaron.”
other sources of information was limited.\textsuperscript{148} Since Swartz’s arrest and death, many have continued the fight for open access, often in the same tradition of releasing journal articles as civil disobedience.

\textbf{Tactics}

Scholars debate over whether to consider Swartz’s approach a form of hacking, likely because their definitions of hacking vary. Librarian Benjamin Hockenberry makes a point to refer to Swartz’s work as a “bulk download” rather than hacking. Hockenberry cites security professional Alex Stamos, a witness for the defense, who argues that Swartz did not hack JSTOR “for all reasonable definitions of ‘hack,’” since Swartz’s automated program did essentially the equivalent of loading a page, right clicking, and saving the article to one’s own computer.\textsuperscript{149} For the sake of Swartz’s case, understanding that computer hacking cases typically receive long sentences, Stamos seems to underrepresent Swartz’s work. If one adopts a broad definition of hacking, such as “manipulating technology for unorthodox means,”\textsuperscript{150} Swartz’s actions fit well within the parameters of a hack.

Lawyer Austin Murnane views Swartz’s case much more harshly than many academics, believing firmly that Swartz was in the wrong, prosecutors did not overstep, and there is no issue with the CFAA. Murnane frames Swartz’s work in a way that fits more conventional definitions of hacking. He cites Swartz’s obfuscation of network security protocols and secretively entering a basement closet without authorization as

\textsuperscript{148} Michael S. Rosenwald, “Meet the woman who put 50 million stolen articles online so you can read them for free,” \textit{The Independent}, April 1, 2016, http://www.independent.co.uk/news/world/americas/meet-the-woman-who-put-50-million-stolen-articles-online-so-you-can-read-them-for-free-a6964176.html.

\textsuperscript{149} Hockenberry, “The Guerilla Open Access Manifesto.”

\textsuperscript{150} Tanezer, “Hacktivism and the male-only stereotype,” 1600.
proof that Swartz had no “innocent reason” for his work.\footnote{Austin C. Murnane, “Faith and Martyrdom: The Tragedy of Aaron Swartz,” \textit{Fordham Intellectual Property, Media \\& Entertainment Law Journal} 24, no. 4 (June 22, 2014): 1101-1130.} This fits more directly into a narrow definition of a hack, describing unauthorized access to systems. Framed differently, Swartz’s downloading still falls into hacktivism, using a hack to advance political aims.

\textbf{Translation of Civil Disobedience to the Cyber Realm}

Various interpretations of Swartz’s actions affect the degree to which the case fulfills Huschle’s framework. Swartz’s work was indirect disobedience in protest of copyright law, but had his actions played out differently it could have been a direct protest. Similar to how Elliot in \textit{Mr. Robot} uses illegal DDoS actions to protest the perceived injustice of capitalism, indirect protest takes place when the law broken is different from the target of the protest. Swartz’s charges for violating JSTOR’s Terms of Service and improperly using MIT’s network included wire fraud, computer fraud, unlawfully obtaining information from a protected computer, and recklessly damaging a protected computer, none of which pertain to the copyright laws that open access advocates seek to reform.\footnote{United States of America v. Aaron Swartz, 11-CR-10260 (D. Mass September 12, 2012), https://www.wired.com/images_blogs/threatlevel/2012/09/swartzsuperseding.pdf.} When framed as civil disobedience, this was an indirect protest. Had Swartz not been caught and then later released the documents, he would have violated the copyright laws he sought to change. Law professor Kent Greenaway believes that direct disobedience is more justifiable, and thus more effective, because it
targets the specific issue of interest.\textsuperscript{153} Swartz did not protest in this way—perhaps because he did not intend to, or perhaps because he did not have the opportunity.

The view of Swartz’s downloads as civil disobedience raises questions about why Swartz took precautions to hide his identity when accessing the MIT network, as acts of civil disobedience should be a public demonstration. Even while maintaining a secret identity, Swartz was stopped before he could use the articles for anything. Had he planned a public act such as distributing the articles online, it is conceivable that he simply did not have enough time to complete his act of protest before his arrest.\textsuperscript{154} As it was conducted, Swartz’s act needed the additional context of his Guerilla Open Access Manifesto for the public to view it as civil disobedience.\textsuperscript{155} Many scholars would dispute the categorization of Swartz’s work as civil disobedience because it was conducted secretly. For example, 20\textsuperscript{th} century political theorist Hannah Ardent saw secret acts as indicative of self-interest and therefore crime, and she would not have classified Swartz’s work as civil disobedience because of his efforts of secrecy.\textsuperscript{156} Nevertheless, other scholars concur that Swartz may not have intended for his downloading alone to act as civil disobedience, and were it made public—as it was—he could not complete a direct protest of copyright law.

Even with lawbreaking and attempted anonymity, Swartz maintained respect for the legal and governing systems in which he operated, a tenet that Huschle maintains is important for civil disobedience. Overwhelmed by his arrest and prosecution, he may have expected more leniency for his actions, particularly on a campus like MIT. In the

\textsuperscript{153} Liljeblad, “Understanding the Complexities of Civil Disobedience,” 214.
\textsuperscript{154} Ibid., 205-206.
\textsuperscript{155} Ibid., 213.
\textsuperscript{156} Ibid., 204, 206.
Swartz family’s statement after Swartz’s death, they bemoaned how “MIT refused to stand up for Aaron and its own community’s most cherished principles.” MIT encouraged a culture of creativity, dissent, and unorthodoxy. Quinn Norton, who described Swartz as a “data pack rat” who loved sorting through millions of documents, posited that “he somewhat reasonably thought that if MIT didn’t like [what he was doing] they’d just tell him to stop.”157 Though Swartz disagreed with the privatization of knowledge, he did not seek to revolutionize the democratic system that created it. He sought reform for a specific area of the law but still respected the overarching system, and his extensive political engagement throughout his life is a testament to this respect. He deeply respected this criteria of Huschle’s framework.

**Swartz as a Hacker Archetype**

While Swartz fit many of the dominant identity categories of the hacker archetype, including his male gender and anti-authoritarianism, he navigated these identities with more nuance than the previous example of Elliot from *Mr. Robot.* Particularly regarding his gender, Swartz realized his privilege within the hacking community. He did not participate in the Male Oblivious Discourse common in hacktivist communities and instead acknowledged the community’s gender biases and worked against them. In this way, Swartz perceives gender through a feminist lens, giving him a different perspective than Elliot. This perspective will influence how Swartz defines the scope of hacking, helping to explain his choice in tactic for electronic civil disobedience.

**Gender**

---

157 Nanos, “Bob Swartz: Losing Aaron.”
Swartz’s most outright comment in support of women in hacktivist communities occurred in an interview that blogger Philipp Lenssen conducted with Swartz over instant messenger in 2007. Lenssen himself engaged in Male Oblivious Discourse, which Swartz then countered. After Swartz commented that he was not hassled or delegitimized at technology conferences because of his young age, Lensenn remarked, “It’s typical for the hacker spirit, right. Who cares about age and looks, as long as you’re smart!” Swartz retorted that he would disagree based on the poor treatment of women and racial minorities in tech and hacker spaces.\textsuperscript{158} While Lensenn overlooked the barriers that gender minorities face in technical fields, Swartz pushed back and refused to engage in the same ignorance so prevalent for many of his peers.

Asked to give specific instances of misogyny in the tech community, Swartz spoke of both outright offensive comments and the culture of passing the blame. He noticed one conversation in particular at a hacker gathering when tech executives referred to holding their business meetings at strip clubs. That same conference hosted a seminar on discrimination that claimed that self-segregation into groups with similar identities resulted in fewer women and people of color in tech spaces, while neither racism nor sexism was a real problem. About these experiences, Swartz commented: “The denial about this in the tech community is so great that sometimes I despair of it ever getting fixed. And I should be clear, it’s not that there are just some bad people out there who are being prejudiced and offensive. Many of these people that I’m thinking of are some of my best friends in the community. It’s an institutional problem, not a personal one.”\textsuperscript{159}

\textsuperscript{159} Ibid.
Swartz acknowledges his own complicity in the community’s sexism, but that gives him a more progressive view on gender than those who do not acknowledge the issue whatsoever.

Swartz also refers to himself explicitly as a feminist, notable for someone of any gender. Swartz’s chronic illness sometimes hospitalized him, and in one blog post in September 2006 he recounts his experience in a post titled, “A Feminist Goes to the Hospital.” Simply the title and the act of self-identifying as a feminist is important to understanding Swartz. In an article published in 2005, sociologist Janice McCabe studied the relationship between feminist self-identification attitudes toward gender using data from a 1996 survey. Some shy away from the term “feminist,” seeing it as too radical or unnecessary, and McCabe acknowledges the survey’s limitations in creating a closed, yes-or-no question where respondents could not elaborate on their definition of feminism. McCabe determined that 29 percent of women self-identified as feminists, compared to only 12 percent of men, though liberal ideology, higher levels of education, and urban location increased the probability of identification. For men more than for women, feminist self-identification is more strongly correlated to a belief in gender equality. For Swartz, this significant linguistic choice confirms his views. While he conforms to the male hacker archetype, he views the world through a feminist lens and acknowledges the disturbing prevalence of misogyny in tech and hacker spaces. This understanding of gender will help to explain Swartz’s choice in tactic of electronic civil disobedience and others’ perceptions of his work.

---

Politics

While feeling at odds with the world around him, Swartz used his alienation to drive him to make the world better. His political beliefs fit well with the hacker archetype of left-leaning and anti-authoritarian. He described himself as politically “lower-left (-5.50, -7.69 as of 2003-08-23),” referring to his placement on the Political Compass, a test that maps ideology onto a two-dimensional graph, more complex than a traditional left-right dichotomy. (See Appendix Two for a visual representation.)\(^{162}\) The X axis maps economic beliefs from left to right, and the Y axis maps social beliefs from authoritarian (top) to libertarian (bottom), where (0,0) would be perfectly centrist. The most extreme economic positions range from communism (-10) to neo-liberalism (10), and social positions range from anarchism (-10) to fascism (10).\(^{163}\) Swartz’s numbers place him squarely in the Libertarian Left quadrant, indicating both economic and social liberalism.

Swartz experienced a disconnect between himself and the society surrounding him. Gabriella Coleman described Swartz as having “a strong personality that definitely ruffled feathers at times. It wasn’t necessarily the case that he was always comfortable in the world, and the world wasn’t always comfortable with him.”\(^ {164}\) His early critiques of the education system reflect his burgeoning anti-authoritarian nature, driving him to question the mainstream. His writings on his blog reflect that this tendency to criticize and not conform to widely accepted cultural norms continued through his life. Writing about “Life in Suburbia: Land of Cliché,” he described suburbia as “the fake coat of paint


\(^{164}\) The Internet’s Own Boy.
that lets you pretend your unhappy life is just as nice as everyone else’s, even if it flakes off.”

Swartz critiqued the world around him from an outsider perspective, but he did not find it necessary to try to fit in. When he began working at the Wired offices in San Francisco, he was similarly harsh: “Wired has tried to make the offices look exciting by painting the walls bright pink but the gray office monotony sneaks through all the same. Gray walls, gray desks, gray noise.”

Swartz’s brother Ben remarks that Aaron despised working for a corporation and intentionally got himself fired by not showing up for work. Swartz’s disregard for his employment reflects his anti-authoritarianism. Even if it were financially beneficial, he could not be beholden to a corporation that interfered with his productivity and authenticity.

While Swartz was heavily critical of mainstream culture, he wanted to work inside the dominant system to change it. He was both disillusioned and idealistic. At age 16, Swartz wrote on his blog, “I’m not going to waste my time on things that won’t have an impact. […] I want to make the world a better place.” In much of Swartz’s work, altruism was his primary motivation, demonstrating an activist mentality. With similar drive to revolutionize the predominant culture, Swartz’s approach presents a contrast with Elliot’s mentality in Mr. Robot. Where Elliot wants to overthrow the whole system, Swartz worked within its limits to make it better. Both Elliot’s and Swartz’s politics reflect a blend of activism and the anti-authoritarian hacker archetype, manifested in different ways.

---

166 Swartz, “Office Space.”
167 The Internet’s Own Boy.
168 Swartz, “Aaron Swartz: The Website.”
Psychological Acceptability and Shifting Perspectives

Regardless of ambiguous intent, compared to his peers, Swartz was poised particularly well to effectively commit an act of civil disobedience. The identity categories that Swartz inhabited shaped the way his work was perceived. His hack was not as technically complex as Elliot’s, nor as destructive. But because Swartz holds a privileged male identity, activists give him the benefit of the doubt and see his work as legitimate. Scholars’ disagreement on whether Swartz’s approach consisted of hacking reflects the thin line he walks. Without his maleness, his tactic would likely not be seen as real hacking. Particularly because the political issues with which he was concerned were related to the internet, other hackers and activists view his work as electronic civil disobedience. Still, a feminist identity allowed Swartz to see a variety of valid protest forms. He did not see hacking as only destructive, exclusively masculine.

Swartz’s work also fit into other activists’ perceptions of what an act of electronic civil disobedience would look like. Open access activists claimed Swartz’s downloading as an act in support of their work, though Swartz never openly made that claim. But because they perceived it as a public display of breaking an unjust law, it became that. The culture surrounding Swartz was able to perceive his downloading as protest, which lends legitimacy to the protest as a public act of civil disobedience. Swartz’s approach, though different that Elliot’s in Mr. Robot, was not so far out of the realm of hacking that society could not understand it as civil disobedience. While perhaps less traditional, it was not overly unconventional. Some people like Murnane view Swartz’s work within the narrow definition of hack, to gain unauthorized access to systems. Others, like Hockenberry and Stamos, argue that it was not a hack, but were they to expand their
definition of hacking to the unconventional use of technology, they would have to classify Swartz’s work as hacking.

Both his individual identity and the psychological acceptability of his tactic for other hackers support Swartz’s use of civil disobedience, but such harsh legal prosecution disincentivizes other activists from pursuing this option. Because courts see civil disobedience as a valuable contribution to a democratic system, they can often offer leniency in sentencing civil disobedients. But so long as they make no distinction between hacking for crime and for activism, activists will seek anonymity to avoid unreasonable punishment. Courts have not applied the same nuance to computer crimes, making many of the most common types of electronic civil disobedience imperfect. If an activist cannot publicly claim their work, they will not perfectly fit a definition of civil disobedience, but so long as courts do not adapt their sentencing, cyber activists will not be inclined to publicly take responsibility for their work. Swartz’s work appeared too similar to the courts’ understanding of criminal hacking for them to perceive it as civil disobedience. Thus, while his hack was psychologically acceptable to hacktivists, it was not to lawyers. They could see no distinction between Swartz’s work and a crime. Unless legal bureaucracy shifts, courts will continue to judge electronic civil disobedience harshly in a way that is impractical for protesting.

The next chapter discusses the Electronic Disturbance Theater’s Transborder Immigrant Tool, an example of an alternative and viable form of electronic civil disobedience. The Transborder Immigrant Tool moves further away from masculine, traditional forms of hacking into a creative, feminine space. Though hackers see its

approach not as hacking, the tool’s use of nontraditional tactics creates a psychological rift between the use of technology and the use of civil disobedience, giving it more potential for effective use. In contrast to the first two cases, where hackers perceived the work as hacking but law enforcement perceived it as criminal, law enforcement is lenient on EDT for their civil disobedience, while hackers see the approach as not technically advanced or truly hacking.
Case 3: The Transborder Immigrant Tool

Overview

My final case study, which provides significant contrast to the two previous examples, is the Transborder Immigrant Tool (TBT) developed by the Electronic Disturbance Theater (EDT), a performance and activist collective. The Transborder Immigrant Tool, which for nearly a decade has remained only a prototype, guides undocumented immigrants crossing the Mexican border into the United States, helping them find caches of water and providing poems of encouragement. Drawing on published interviews with members of the collective and analyses of their work from various disciplines, I argue that the TBT fits well within the parameters of electronic civil disobedience but does not fit within hackers’ psychological model of what hacktivism looks like. After establishing the overview, movement context, and technical tactics of the TBT, I discuss how the tool translates to the established model of civil disobedience. I then acknowledge how the Electronic Disturbance Theater fits the hacker archetype with its strong anti-authoritarian leftism. More significantly, I explore the ways in which EDT breaks the hacker archetype. The group identifies as artists first and activists second, bringing a different experience and perspective to hacking. Their members also have a breadth of gender experiences, giving them unique perspectives in the male-dominated tech community. Guided by their progressive views of gender, the group frames their work as “queer technology,” linking their hacking themselves directly to their understanding of gender. Their approach to hacktivism builds new spaces of protest on the internet rather than using existing venues, with creative rather than destructive tactics of hacking. With this divergence from the hacker archetype, though, other hackers
struggled to accept the TBT as legitimate hacking. This perspective, I argue, is rooted in their sexism, and a necessary shift in perspective will open up more avenues for valid protest.

**Background on the Electronic Disturbance Theatre and the Transborder Immigrant Tool**

Throughout his childhood and adolescence, Ricardo Dominguez participated avidly in theater and performance art. This interest continued into his mid-twenties, and when he joined the newly-formed performance collective Critical Art Ensemble (CAE) in 1987, he found a group that merged his artistic and political interests. The Critical Art Ensemble brought together like-minded individuals who believed that economic and symbolic interruption made civil disobedience most effective, and with infrastructure shifting online, so must protests. The group coined the term electronic civil disobedience to represent that shift of resistance into the technologically advancing world as they began to incorporate fax machines and telephones into protests.

Though he left CAE in the early 1990s, Dominguez’s interest in electronic civil disobedience resurfaced in December 1997 after the Acteal Massacre, where the Mexican government killed 45 civilians, including women and children. The government targeted Las Abejas, a group of indigenous Christian pacifists, for their support of the Zapatista Army of National Liberation (EZLN), a rebel group opposing the Mexican government for signing the North American Free Trade Agreement (NAFTA). On April 10, 1998,
Dominguez and his newly formed artist-activist group Electronic Disturbance Theater (EDT) launched a protest against the website of Mexican president Ernesto Zedillo in support of the EZLN. Bret Stalbaum and Carmin Karasic managed the technology and administration, while Dominguez and Stefan Wray handled publicity and communication. The group launched a “virtual sit-in” using a tool they created called FloodNet. Instead of accessing real pages of the website, the tool would request fake pages with names like “justice” and “human rights.” When the website replied with a 404 error, a standard website response for pages that do not exist, the response would read, “justice not found on this site,” or “human rights not found on this site.” These requests also strained the server hosting the website, similar to a distributed denial of service, so that other requests to the site were slowed down significantly. Some hackers criticized this use of technology as “wimpy” because it slowed down the servers instead of taking them offline altogether, which the EDT did not want to do. The group preferred to demonstrate the masses assisting them in their protest, rather than simply taking down the website.

The EDT continued using FloodNet throughout 1998 in their Stop the War in Mexico (SWARM) Project, and in September they launched another protest as a performance at the Ars Electronica Festival on art, technology, and society. Festival attendees and others could participate in the FloodNet action, which targeted the websites of the Mexican president, Frankfurt Stock Exchange, and U.S. Department of Defense.

---

173 Hurst, “Examining Hacktivism,” 42, 49.
174 Leonie Tanczer, “Hacking the Label: Hacktivism, Race, and Gender,” Ada: A Journal of Gender, New Media, and Technology, no. 6 (February 2, 2015).
175 Hurst, “Examining Hacktivism,” 49.
176 Tanczer, “Hacking the Label.”
The protest ended after 8 hours, rather than the planned 24 hours, when the DoD launched a counterattack to disable the FloodNet tool.\textsuperscript{177}

Through these first protests, the EDT developed its guiding principles. Wray described electronic civil disobedience as a supplement to traditional, physical civil disobedience to create a more powerful hybrid civil disobedience.\textsuperscript{178} Above all, though, the group’s work would be artistic and symbolic, less concerned with technological or even political effectiveness.\textsuperscript{179} Dominguez sought to focus on semantic resistance, questioning and destabilizing the norms of a system and culture as a whole instead of disrupting only the function of a machine through modifications to software or hardware.\textsuperscript{180} Thus, the imagery of the group’s work would take precedence. Finally, Dominguez asserted that they would tie their names to their work to provide contrast with the anonymity of most online activity.\textsuperscript{181}

The DoD response suggests that the EDT’s work was perceived as more than just symbolic. Masters student Shannon Hurst, who researched the EDT through the lens of theater studies, critiques the action—and the response it provoked—for bringing activism to a standstill and further silencing the voice of indigenous Mexicans or even inviting retaliation upon them. She also believes that such a protest tactic homogenized participants and “extinguishe[d] their empowerment as individual actors,” by putting them all behind the name and rules of the EDT, instead of allowing them to retain their autonomous identities.\textsuperscript{182} Even after such controversy, in 1999 the EDT released the

\textsuperscript{177} Hurst, “Examining Hacktivism,” 49-51.  
\textsuperscript{178} Ibid., 15-16.  
\textsuperscript{179} Ibid., 48.  
\textsuperscript{180} Ibid., 15.  
\textsuperscript{181} Ibid., 47.  
\textsuperscript{182} Ibid., 52-55.
“Disturbance Developer Kit,” a version of the FloodNet software for other activists to use in their own protests.183

In 2005, Dominguez was hired by the University of California at San Diego in the visual arts department and was tenured in 2009.184 Through the university, he created the Electronic Disturbance Theater 2.0, which alongside the newly formed b.a.n.g. (bits, atoms, neurons, and genes) lab at the California Institute for Telecommunications and Information Technology (Calit2), would explore “the disturbance of borders: national, gender, disciplinary, fiction/non, through the exploitation and re/performance of technology, poetry and the imaginaries of each.”185 Dominguez and Stalbaum returned for the second incarnation of the Electronic Disturbance Theater, joined by artist and theorist Micha Cardenas, poet and border studies scholar Amy Sara Carroll, and artist Elle Mehrmand.186

In 2007, EDT 2.0 and b.a.n.g. lab began developing the Transborder Immigrant Tool, an application loaded onto inexpensive cell phones to guide those crossing the Mexican-United States border to water caches while providing welcoming poetry.187 The program, coded by Stalbaum and UCSD undergraduate student Jason Navarro,188 uses global positioning system (GPS) data without requiring phone service or transmitting

183 Goldstein, “Digitally Incorrect.”
185 Hurst, “Examining Hacktivism,” 57.
data from the phone that could alert authorities to the users’ locations.\textsuperscript{189} The group hoped for their project to function in conjunction with and as augmentation for other organizations’ existing work in the immigrant rights movement. In particular, the app would locate water caches placed by humanitarian organizations to help migrants endure long stretches of desert.\textsuperscript{190} EDT 2.0 saw this project as representative of the growing potential of technology to directly intervene to improve people’s lives.\textsuperscript{191}

In 2010, the FBI Office of Cybercrime and UCSD began investigations into the Transborder Immigrant Tool, catalyzed by the complaints of three Republican congressmen, and the university threatened to de-tenure Dominguez. Once UCSD Audit and Management Advisory Services determined that the project had used its funds appropriately and as outlined in the grant proposal, they ceased the investigation. The university still asked Dominguez not to speak about the project and refrain from future artist-activist performances, but he refused. He successfully argued that he was hired for his history of activism and to conduct this type of research. His team resumed work on the Transborder Immigrant Tool in 2011, though they have yet to issue a final, functional product.\textsuperscript{192} Nearly 10 years after the project’s inception, EDT 2.0 continues to work on it, and their code is freely available online—with the locations of water caches removed—for others to use for GPS and border navigation purposes.\textsuperscript{193}

\textsuperscript{190} Ibid., 3.
\textsuperscript{191} Ibid., 2.
\textsuperscript{192} Hurst, “Examining Hacktivism,” 61-62.
\textsuperscript{193} Dominguez, “Border Research,” 2.
Movement Context

The Electronic Disturbance Theater 2.0 repeatedly acknowledges their place in a larger context of immigrant rights activism. They acknowledge their limitations in being unable to fully understand the plight of travelers crossing borders, and they use their position to elevate the existing work already done by other organizations.\(^{194}\) As founding member Stefan Wray observed about the SWARM Project, the most effective electronic civil disobedience builds on traditional civil disobedience. EDT’s unconventional use of technology is more effective working within the existing movement than either tactic would be alone.\(^{195}\)

With this mentality, EDT 2.0 sought to bring light to the escalating number of border crossing deaths and the work of other organizations to provide water to migrants in the desert. Though fewer people overall are attempting to cross into the United States, the number of people who die each year trying to do so increases. U.S. Border Patrol estimated 1,934 deaths between 2007 and 2011, but humanitarian organizations working in the area believe those statistics significantly underestimate the true number of deaths.\(^{196}\) One organization, the Border Angels, estimate that a total of 10,000 people have died trying to cross the U.S.-Mexico border. They attribute the discrepancy in numbers to the Border Patrol only reporting bodies found on their usual patrol routes, while the Border Angels find more bodies off those paths while they fill water caches.\(^{197}\)

\(^{195}\) Hurst, “Examining Hacktivism,” 15-16.
\(^{197}\) Cardenas et al., “The Transborder Immigrant Tool,” 2.
Activists attribute the rising death rates to the increasing militarization of the border, making crossing a more treacherous undertaking.\textsuperscript{198} 

Migrants who attempt to cross the border face numerous risks beyond border surveillance and the physical crossing of a fence. If caught, they can face violence inflicted by immigration authorities.\textsuperscript{199} Nights in the desert put their bodies at risk for hypothermia.\textsuperscript{200} Even if they do make it into the United States, many die of exhaustion and dehydration in the desert.\textsuperscript{201} Multiple humanitarian organizations including the Border Angels address this last single but significant challenge. No Mas Muertes/No More Deaths, a faith-based organization operating out of Arizona, also helps to replenish aid caches of water and beans on the U.S. side of the border for migrants to use during their journeys. They write encouraging messages on the jugs of water, such as, “May destinations be reached safely,” similar to the encouraging poetry of the TBT. Near the border, they also maintain an aid station where they provide migrants with meals and medical treatment.\textsuperscript{202} 

No Mas Muertes has faced resistance to their work. Sometimes when they return to refill caches, they will find the water jugs slashed open and drained, they suspect by Border Patrol units or private militias. The organization’s slogan is “Humanitarian Aid Is Never A Crime.” Providing medical treatment to people crossing through the desert is legally allowed, though the organization’s volunteers have faced multiple legal charges, 

\textsuperscript{198} Reed, “Queer Provisionality.”
\textsuperscript{199} Ibid.
\textsuperscript{201} Reed, “Queer Provisionality.”
\textsuperscript{202} Sinsky, “Border diary.”
none of which have stuck. The group’s work continues to assist those crossing through the desert.

In contributing to the larger movement for immigrant rights, EDT 2.0 also raises questions about the concept of borders altogether. Activists critique the language of “illegality” used against undocumented immigrants, common since the U.S first criminalized undocumented immigration into the country in 1929. This language particularly targets non-white people and creates associations with “disease, criminality, and terrorism.” Dominguez created the concept of “transborder” to radically suggest a stateless future where everyone shares the identity of movement, and to represent a group of people with common experience in need of certain protections:

If you count all the folks who are crossing borders across the arcs of the world, it’s a pretty large population—larger than some countries. So the concept of the “transborder” as undocumented bodies moving between states is a way of imagining them as a flowing nation state that perhaps should have their own transborder rights, transborder rights to health, education, labor rights—in the not too distant future we may all be stateless undocumented bodies whose only rights will be transborder rights.

Dominguez joins a group of activists who view migration as a human right and not something that should be restrained or regulated. In offering material support to undocumented immigrants crossing into the U.S., organizations like EDT 2.0 suggest that everyone deserves life regardless of their national origin.

---

203 Ibid.
204 Reed, “Queer Provisionality.”
206 Reed, “Queer Provisionality.”
Technical Description of the TBT

Similar to EDT’s previous work, theater took precedence over technical functionality for the Transborder Immigrant Tool. The app only worked for a one-mile radius around the border between San Diego, California, and Tijuana, Mexico, and it never left the prototype stages. On a Motorola i455 flip phone, which sells for as little as four dollars, the group installed compass-like software that could point the user in the direction of water caches and main roads. Despite the limited geographical area in which it was useful, EDT 2.0 insisted the project was successful, if only for the attention it drew to the larger issue of immigration. They hoped first to absorb some of the negative attention typically paid to border crossers onto their device. They also hoped to challenge the “aesthetic of hate and fear” common to discussions of immigration by showcasing migrants’ humanity and personalizing their struggles.

An addition to further help humanize immigrants was the inclusion of poetry, written by Carrol. At intervals throughout the user’s journey to find water, the Transborder Immigrant Tool provides recordings of poetry in English, Spanish, or various indigenous languages. Through the poetry, EDT 2.0 hoped to ease the length of migrants’ journeys with energizing “poetic sustenance” in addition to the physical sustenance of water. Each poem focuses on an aspect of desert survival, combining art and utility. For example, one poem suggests the best time of day to search for water:

207 Goldstein, “Digitally Incorrect.”
211 Goldstein, “Digitally Incorrect.”
212 Reed, “Queer Provisionality.”
Restrict your water reconnaissance to early or late in the day when your liquid net-gain will outweigh the perspiration you expend. A thirst is seldom quenched; it morphs to reappear on the horizon. Meanwhile, the desert reflects the sun back like a mirror. You are caught in that pair’s uneven, inconsummate exchange.214

According to Carroll, including poetry not only offers hospitality but also makes “a point to resist the dehumanization of human beings and to suggest the aesthetic also sustains.”215 Following the tradition of black lesbian feminist Audre Lorde, who proclaimed that “poetry is not a luxury,”216 Carroll recognized that even with pressing concerns for their survival, migrants could appreciate and benefit from consuming culture.217

Though EDT 2.0 repeatedly defines themselves as artists first and activists second, they should not have felt limited by the immense challenges of implementing the TBT on a functional level, and they should not have underestimated the potential of the technology. In 2009, early in the project’s creation, the team identified certain challenges, such as battery life and encrypting map data so malevolent users could not find the location of caches.218 Shannon Hurst also considers the ethics of including users in the tool as part of a performance, potentially subjecting border crossers to more risk than their already challenging situation. She also asks how the program could hurt users if it malfunctioned or provided incorrect or outdated information, or if its users could be tracked and captured by using the tool.219 While these challenges should not be

215 Hurst, “Examining Hacktivism,” 60.
217 Reed, “Queer Provisionality.”
219 Hurst, “Examining Hacktivism,” 43, 63.
minimized, hacking is inherently about thinking creatively and having a problem-solving mentality. Particularly with EDT 2.0’s approach of creating new spaces in which to protest, should the group want the tool to be fully functional, its implementation need not be a limiting factor.

**The TBT as an Act of Electronic Civil Disobedience**

Despite challenges in its practical implementation, the creation of the Transborder Immigrant Tool was an act of civil disobedience against the Immigration and Nationality Act. The three Republican congressmen who encouraged the investigation of EDT 2.0 claimed that through the tool, tax dollars were being used to “actively help people subvert federal law.” The Immigration and Nationality Act, originally created in 1952, includes Section 274 on “Bringing In and Harboring Certain Aliens.” The section makes it a violation of federal law for a person to bring a non-citizen into the United States somewhere other than a designated point of entry, to provide transportation to a non-citizen in further violation of the law, to shelter or conceal a non-citizen from detection, and to encourage a non-citizen to enter or reside in the U.S. The TBT, according to the congressmen, would encourage immigrants to enter the U.S. illegally. In the group’s tradition of civil disobedience, EDT 2.0 understood that deliberately breaking a law would bring attention to a pressing issue. This approach is a direct protest of the Immigration and Nationality Act, different from the two previous cases of indirect disobedience. As noted previously, law professor Jonathan Liljeblad states that cases of

---

220 Goldstein, “Digitally Incorrect.”
222 Goldstein, “Digitally Incorrect.”
direct civil disobedience often receive lesser sentences than those of indirect civil disobedience because they are seen as more legally justifiable.

The TBT fulfills Huschle’s translation to electronic civil disobedience more completely than the previous case studies. First, Dominguez calculated that an injustice existed, guided by his “belief that there is a higher law that needs to be brought to the foreground: a universal common law of the rights of safe passage.” The way he frames his motivation follows in the tradition of Thoreau. In Thoreau’s interpretation, a just law will align with natural law, and the responsibility falls on each citizen to consider whether they feel a law is just. This sense of an internal moral guide that takes precedence mirrors Dominguez’s language describing a higher law that dictates the right to safe passage. Dominguez’s act of civil disobedience, then, protests injustice in pursuit of that higher law.

In its focus on theater, EDT 2.0 also uses the TBT as a public act of protest, a second of Huschle’s tenets of translation. With the poetic aspect of the tool, they distinguish themselves from strict activists’ focus only on functionality. They seek not only legal but also cultural reform. This approach uses their act of civil disobedience as a public statement to instigate conversation. The group defines themselves as artists first, arguing that successful implementation is secondary to the theatrics. Dominguez differentiates between “disturbing” the law and “breaking” the law, where disturbing the law forces people into a different conversation of “poetry, ethics and justice” instead of

---

225 Reed, “Queer Provisionality.”
discussing only illegality.\textsuperscript{226} This reflects EDT’s focus on creating new spaces to protest, rather than abiding by the traditional limits of what already exists. These new possibilities for resistance are still intended to be seen and to spark further conversation about change, making the TBT a public act.

The group’s lack of anonymity contrasts its work with most other uses of electronic civil disobedience and follows a more traditional model of civil disobedience. Stalbaum, who worked on both the first and second iterations of EDT, distances himself from hackers. He postulates that EDT has never been successfully prosecuted because of the group’s “radical transparency.” Particularly with FloodNet, since the program only slowed websites and did not take them offline as with many DDoS attacks, Stalbaum believes that “no one wants to take on the free-speech aspect” by silencing the group. In his opinion, law enforcement wanted to avoid a First Amendment conflict, particularly because FloodNet was not violating others’ freedom of expression. With this history of taking public ownership of their protests, EDT are more like practitioners of traditional civil disobedience than anonymous hacktivists.

Though electronic civil disobedience should be an available form of protest for everyone, both FloodNet and the TBT faced criticisms of being inaccessible. Hurst remarks that while participating in FloodNet was technically simple, even an internet connection was a “luxury” in 1998. This made it even more risky for EDT to work on behalf of indigenous people already being silenced when those people could not make their voices heard by participating in the protest.\textsuperscript{227} The tool threatened to speak over the

\textsuperscript{227} Hurst, “Examining Hacktivism,” 54.
voices of the people most affected by the Mexican government’s actions. With the Transborder Immigrant Tool, a major challenge that EDT 2.0 recognized was finding a cell phone cheap enough to make it widely available.\textsuperscript{228} It is difficult to claim these protest methods are democratic if they are not broadly accessible to the public. This does not invalidate the work of EDT, but for their tactics to better reflect the sentiment of civil disobedience they must address their practical usability.

**Consistency with the Hacker Archetype: Anti-Authoritarianism**

The Electronic Disturbance Theater 2.0 reflects radical anti-establishment views and is highly critical of mainstream politics in the United States, similar to archetypal hackers. If placed on a strict American liberal-conservative scale, Dominguez’s work falls on the left, or perhaps more specifically, anti-right. The Critical Art Ensemble, where Dominguez got his start, formed from individuals’ dissatisfaction with Reagan-era social and economic policies, particularly since other artists were not addressing urgent and controversial issues such as the AIDS epidemic. Dominguez’s first electronic protest was jamming a fax machine at the National Institutes of Health, a biomedical research agency in the Department of Health and Human Services. He sent repeated messages about the efficacy of AZT, an antiretroviral drug used to treat AIDS.\textsuperscript{229} Over two decades later, when working on the TBT, Dominguez found his work targeted by the extreme right-wing media. Conservative political commentator Glenn Beck claimed that the project would “dissolve the nation.” Increasing coverage of the tool by Fox News brought

\textsuperscript{228} Reed, “Queer Provisionality.”

\textsuperscript{229} Goldstein, “Digitally Incorrect.”
EDT 2.0 an influx of threatening emails from viewers who shared sentiments similar to Beck’s.\textsuperscript{230}

Dominguez and EDT 2.0, though, have also shared criticism of liberal politics in America, and thus a left-right dichotomy is not enough to explain their political views. Using the Political Compass, as referenced in the previous chapter, to orient EDT 2.0’s beliefs, the organization would fall strongly into the category of left libertarian. They are strongly against neoliberal economic policies, evidenced by their support of the anti-NAFTA Zapatistas and by Dominguez’s criticisms of capitalism for affording more rights to a can of soda than to the individuals who produce the can.\textsuperscript{231} This position places them on the far left end of the economic scale (with neoliberalism being on the far right of the X axis). On the Y axis, EDT 2.0 falls on the far bottom in libertarianism, contrasting with authoritarianism at the top. Alison Reed, a professor of English studying performance, identity, power, and social movements, lauds the bilingual poetry of the TBT for producing a “utopian image of global fellowship.” She also believes that the tool urges not only legal reform but, through an “abolitionist ethics of challenging oppressive institutions themselves,” also questions the idea of national borders themselves.\textsuperscript{232} Reed’s mention of abolitionist ethics refers to the movement to dismantle certain state institutions such as police and prisons that have historically imposed violence against minority groups.\textsuperscript{233} Micha Cardenas, a member of EDT 2.0, also refers to herself as a member of this movement, and her other work has focused on similar activist-art to

\textsuperscript{230} Nadir, “Poetry, Immigration and the FBI.”
\textsuperscript{231} Reed, “Queer Provisionality.”
\textsuperscript{232} Ibid.
utilize community-based alternatives to policing. The ideas of abolitionism and “global fellowship” describe an anarchistic alternative world that the EDT 2.0 seeks. With their far left economics, this places the group in the left libertarian quadrant of the Political Compass.

For the members of EDT 2.0, the political act of producing their art and code drives them. For Cardenas, hacking was never solely about technology, but was also an act of empowerment, “about wresting power back from corporations and governments.” Carroll, contemplating the poetry for the TBT, found contrast in North American writing, which focuses on aesthetic, and Latin American tradition, which is more outwardly political. She mirrors the latter trend, writing poems about heatstroke and the barrel cactus, endowing travelers with both a cultural experience and practical information for their journey.

Even in poetry and programming, which may not be directly political acts, Cardenas and Carroll find motivation in politics. This drive conforms with the political motivations of the actors established in the previous case studies.

**Breaking the Hacker Archetype: Gender**

More significantly, though, the Electronic Disturbance Theater 2.0 significantly breaks the hacker archetype with their diverse experiences of gender, lending them a unique perspective for their work, which falls in a category that they term “queer technology.” Their collective includes representation of women from diverse

---

234 Tanczer, “Hacking the Label.”
235 Ibid.
236 Marino, “Code as Ritualized Poetry.”
backgrounds, including both cisgender and transgender women\textsuperscript{237} who bring different perspectives to the group’s work and share a belief in progressive, all-inclusive feminism. Their identities lend them each a different perspective on gender in the tech industry and hacking community. Carmin Karasic, a black cisgender woman, participated in the original EDT but not 2.0. She moved from working as an IT manager to working as a digital artist. In her former career, she felt she had to “outperform” her colleagues to be respected for her technical skills, but in her shift into the art world, the daily racism and sexism she encountered were minimized. Because she did not look like the white male archetype of a hacktivist in tech circles, she found more room in the art world to fit her hacktivism.\textsuperscript{238} A member of EDT 2.0, Micha Cardenas also experienced challenges as a Latina transgender woman in tech. She joined work on the Transborder Immigrant Tool because of her technology experience and her activism on borders, immigration, and freedom of movement. When criticism of the TBT began, it also targeted its creators specifically, including Cardenas, who had previously experienced transphobic and homophobic harassment at hacking conferences. While attacking the TBT, anti-immigration activists threw ad hominem insults at Cardenas and Carroll for their gender expressions and at Dominguez for his ethnicity.\textsuperscript{239} From her transgender identity, though, Cardenas draws strength and inspiration for her contribution to the project:

“The trans in transborder and transgender can signify a crossing, but also a hope and a bravery in crossing. As a trans person, I am familiar with the hope of crossing over to a new place, the place of a new body. I think that this is

\textsuperscript{237} Cisgender refers to people whose gender identities align with the genders they were assigned at birth. In this case, a cisgender woman refers to a woman who was assigned female at birth. Transgender women were assigned male at birth but understand their own gender to be female.

\textsuperscript{238} Tanezer, “Hacking the Label.”

\textsuperscript{239} Ibid.
something I share with those who hope to find a better life by moving their bodies into a new place, across an international border.”

While she does not equate the challenges faced by transgender people and immigrants, Cardenas draws on her own gender experience to empathize with immigrants’ struggles. Her identity strongly influences her experiences in the tech world and gives her a unique perspective in participating in EDT 2.0’s activism.

Beyond their personal identities, the members of EDT 2.0 subscribe to an inclusive, progressive definition of feminism. Cardenas acknowledges that solely using the label “feminism” is often associated with white, cisgender, middle-class feminism inaccessible to people like herself. In particular, she cites her belief in the definition of black feminist author bell hooks, who says that “feminism is about dismantling and ending all systems of domination.” Carroll also draws on the work of feminists of color in her contribution to the Transborder Immigrant Tool, as the idea of poetry as sustenance derives from queer female poets of color Cherrie Moraga, Gloria Anzaldua, and Audre Lorde in particular. The group’s political beliefs about gender also shape their work, in addition to their personal experiences.

With the group’s experiences with gender comes the influence of queer theory in their work. The term “queer” is typically used as an umbrella term for lesbian, gay, bisexual, transgender (LGBT), and other non-normative sexualities and gender identities. Queer theory, which originated with the study of categories of gender and sexuality, disrupts the dichotomy of normal and abnormal categories, and questions what normal and abnormal themselves even mean. For example, a queer theorist would reject the

---

241 Ibid. Note: hooks’ name is intentionally spelled in lowercase.
242 Reed, “Queer Provisionality.”
binary division between masculine (dominant, or “normal”) and feminine (oppressed, or “abnormal”) identities, or between heterosexual and homosexual, arguing instead for fluidity and flexibility between the two.\textsuperscript{243} When the word queer is applied to technology, then, it refers to unconventional use of technology, here the use of technology theatrically rather than practically. TBT also works by “inventing space,” or creating entirely new options for resistance that exist outside of the “normal.”\textsuperscript{244} Cardenas describes the technique as creating a new space for protest: “It is not like marching through the street. It is like saying that we are going to create a different street.”\textsuperscript{245} Their experiences with gender and belief in queer theory lend the members of EDT 2.0 a distinct perspective that shapes their work. Directed by this uniqueness, they disrupt the idea of “normal” technology with the invention of the Transborder Immigrant Tool.

**Psychological Acceptability and Shifting Perspectives**

The Transborder Immigrant Tool differs from previous examples as it is accepted as civil disobedience but not as hacking, partially due to the group’s own framing. Not insignificantly, the Electronic Disturbance Theater calls their work electronic civil disobedience. By naming their practice as such, they associate themselves with a history of civil disobedience, which then makes their work seem more justified as an act of protest.\textsuperscript{246} Their lack of anonymity also differentiates them from many traditional hackers, distancing them from society’s mental image of computer criminality. But while


\textsuperscript{244} Nadir, “Poetry, Immigration and the FBI.”

\textsuperscript{245} Tanezer, “Hacking the Label.”

\textsuperscript{246} Liljeblad, “Understanding the Complexities of Civil Disobedience,” 199.
their work is acknowledged as civil disobedience, it does not garner the same respect from hacker communities. As discussed in the history of FloodNet, some hackers insulted the technology as “wimpy.” This word choice targets the gender diversity of the group and reflects the prevalent sexism in hacking communities. “Wimpy” implies weakness associated with femininity, here suggesting that EDT’s non-destructive tactics did not fit with the masculinity of hacker culture. Insults of the TBT were even more explicitly gendered. One email made public by EDT 2.0 read, “You fucking anti-American CUNT!!!! I hope you die the worse [sic] death possible you horrible, disgraceful BITCH! GET THE FUCK OUT OF THIS COUNTRY YOU WHORE!!!!” An excerpt from another read, “Hold still just a little longer while I center these cross hairs on your faggot liberal scum bag head.” Other threatening emails the group received reflect similar word choice. The use of “cunt,” “bitch,” “whore,” and “faggot” target the group with degrading words specifically referring to femaleness and homosexuality, suggesting the senders’ perception of femininity as lesser. The group’s non-archetypal experience with gender means that outsiders view their work differently, in this case as inferior to more traditional, destructive, and masculine hacking. Both the members of EDT 2.0 and their queer technology do not fit into other hackers’ perception of what hackers and hacking typically look like, so other hackers would not place the TBT in the category of hacking.

---

247 One 1998 study of students categorized the insults directed at people of male and female genders. The two most frequent types of insults toward men were “mistreats others” (e.g. asshole, jerk) and “stupid” (e.g. bonehead, doofus). Both of these categories had female equivalents. The third most frequent category of insult directed for men was “weak in character/like a woman,” which also included insults implying a man was gay, as homosexuality was associated with “weak/like a woman.” This category included words like “pussy,” “sissy,” “weakling,” “wimp,” “femme,” and “nancy-boy.” The use of these insults implied an inferiority associated with the female gender. Further reading: Deborah James, “Gender-Linked Derogatory Terms and Their Use By Women and Men,” *American Speech* 73, no. 4 (Winter 1998), 399-420.

248 Electronic Disturbance Theater/b.a.n.g. lab, *Sustenance: A Play for All Trans [ ] Borders* (New York City: Printed Matter, Inc., 2010).
Thus, while the TBT might be psychologically acceptable as a tool of civil disobedience, hackers do not view it as legitimate hacktivism. EDT themselves deemphasize the technology of their work by repeatedly framing it as art first. In combination with hackers’ negative gendered perceptions of EDT 2.0, this approach further distances the group from traditional hacker communities.

As Cardenas suggests, efforts should not necessarily be directed to making hacktivism more inclusive but rather to changing definitions. The premise of making tech spaces more inclusive puts the onus on privileged people to accept people with historically oppressed identities. Instead, she proposes changing the way people think about technology. Cardenas defines hacktivism as “political hacking” and “the combination of technological creativity and imagination with activist campaigns and projects.”

One unconventional example she provides is women of color who participate in Maker Faires, a movement of gatherings that bring together people with do-it-yourself mentalities and interests in “science, engineering, art, performance, and craft.” These women they are not part of traditional hacking communities, but they work on projects to use technology in creative ways all the same. They provide an example of the potential for activism through technology, if one expands the perception of technology beyond the currently limited scope of conventional hacking. Further, the internet is still primarily a resource for developed countries and for white men who are encouraged to pursue technical fields.

---

249 Tanczer, “Hacking the Label.”
250 Ibid.
252 Tanczer, “Hacking the Label.”
hacking includes other productive activist work in the understanding of electronic civil disobedience, making ECD more accessible to more people as a potential avenue of activism.
Conclusion: A Future Direction for Electronic Civil Disobedience

Potential practitioners of electronic civil disobedience face two major issues that must be addressed in conjunction. The most widely accepted techniques of electronic civil disobedience in hacking communities, such as distributed denial of service attacks, fail to meet philosophy professor Brian J. Huschle’s well-delineated framework for electronic civil disobedience and are seen as criminal by law enforcement. Conversely, the forms of electronic civil disobedience that satisfy Huschle’s framework and are acceptable to law enforcement are not seen as true hacking by the hacktivist community. Currently, the options for civil disobedience in cyberspace are narrow.

Classifying an action as civil disobedience is important in granting it legitimacy, as it situates an act of protest in the lineage of a well-respected American political tradition. The classification is also of use to activists, beyond aiding their interaction with law enforcement. If activists have made the calculation to engage in civil disobedience, incorporating an electronic form of the same concept would not be a risky leap for them to take. If they have already decided that civil disobedience is the tactic best suited for their work, they can logically extend their work into the cyber realm.

Expanding options for potential electronic civil disobedience requires shifts on behalf of both the legal system and hackers. Existing research, including the aforementioned work of Tiffany Marie Knapp, Joshua Adams, and Andrew T. Illig, has built extensively on Huschle’s framework to propose changes to the Computer Fraud and Abuse Act. These proposals include shifts that would offer leniency in sentencing or particular guidelines to follow for a hack to be considered free speech. This shift is important but alone is not enough, particularly when acknowledging the lag of
bureaucracy. A second shift on behalf of hackers will further expand possibilities for ECD, and the shift proposed by this research incorporates the effects of gender biases in hacking communities. *(These shifts are illustrated in Appendix Three.)*

In postdoctoral researcher Leonie Maria Tanczer’s leading-edge research on gender in hacktivist communities, she interviews a woman who identifies as a hacker and an activist but not a hacktivist. The woman notes that skills and contributions seen as feminine are “not thought of as real work.” This is largely true of any work seen as “women’s work.” For example, housework and childrearing, traditionally female tasks, are not seen as real jobs and are not as valued as men’s contributions outside the home.\(^{253}\) Despite women’s significant contributions to society and the economy, their gender makes others view their work as lesser. This remains true in hacktivist communities. Acts viewed as more feminine are undervalued and not seen as real hacking. The prevalence of sexism in the male-dominated field of hacking limits hacktivists’ perceived options for protest. Particularly in a legal system where conventional approaches to electronic civil disobedience receive excessively harsh sentences, the hacktivist community must explore new options for protest.

Tanczer also notes that women more often oppose DDoS attacks and other destructive and illegal approaches to hacking. If women choose not to engage in these prevalent tactics, they will find other alternatives to protest in cyberspace. The spirit of hacking is the unconventional. Women adopt the broader definition of hacking: the

unorthodox use of technology, or the use of technology for ways other than it was intended.

My research bridges two existing fields in the study of hacktivism to suggest a broader range of options. Huschle’s framework outlines the use of electronic civil disobedience as a subset of hacktivism, and he specifies a small but important space where true civil disobedience can occur online. Tanczer innovatively links gender and hacktivism, studying how the gender biases of a male-dominated field impacted women’s identities as hacktivists. I tie these two lines of research together, suggesting that a broader, feminist view of hacktivism is the solution to meeting Huschle’s narrow specifications of legitimate civil disobedience. This fulfills the second shift required, beyond reforming the CFAA, to create an adequately large possibility for electronic civil disobedience. With my three case studies, I provide examples of masculine hacking that does not fit Huschle’s framework and feminine hacking that does.

If destruction is masculine, then its counterpart of creativity is feminine. The Transborder Immigrant Tool, designed and built by a gender diverse group, exemplifies the use of creativity in electronic civil disobedience. The tool and the Electronic Disturbance Theater were targeted with gendered insults and criticized for weak, illegitimate hacking. Nevertheless, the TBT is the only case study that satisfies Huschle’s criteria for the translation of civil disobedience to cyberspace. Their approach is direct disobedience and does not violate the ever-looming CFAA. Creative, nondestructive electronic civil disobedience offers more options for legally defensible acts of protest.

In contrast, Elliot in Mr. Robot is a man in a sea of men. His gender dominates technology fields, and he approaches electronic civil disobedience with a traditional,
widely-used tool of hacking. Fsociety’s tactic does not hold up to Huschle’s translation. In the lack of recognition of gender, Elliot demonstrates his internalized sexism. This limits his view of hacktivism to the destructive.

Aaron Swartz’s approach to electronic civil disobedience is less conventional than Elliot’s, but it is still destructive. Swartz’s feminism lends him a broader perspective of potential hacks. Still, he fails to satisfy Huschle’s tenets. For an approach to be so absolutely perceived as criminal means it is ineffective, as courts will not make a distinction between criminal and activist hacking. Creative hacking does not have this close association with criminality and thus poses a more realistic alternative.

The more destructive, anonymous, and revolutionary—that is, masculine—hacks do not translate well to electronic civil disobedience. Further, the Transborder Immigrant Tool is a form of direct disobedience, while the other two cases are not. The TBT directly breaks the Immigration and Nationality Act, instead of breaking an adjacent law in indirect protest. By using creative methods to build a new venue of protest—creating a new street with “queer technology”—the Electronic Disturbance Theater is able to challenge a law it disagrees with without violating the CFAA and exposing its members to the law’s harsh sentencing guidelines. Because of sexism in the broader hacktivist community, though, many hackers do not see this creative, feminine approach as real hacking.

Addressing misogyny in hacking communities is not a light task, but it should not be seen as any less important than reforming the Computer Fraud and Abuse Act. With their biases, not only do hackers exclude others’ acts of electronic civil disobedience, but they limit their own options for protesting. They do not want to be associated with
creative, feminine, lesser. Dismantling patriarchy will expand the potential avenues for electronic civil disobedience for all hacktivists, bringing an essential tactic of American political participation into the cyber age.

This research examines hacktivists primarily as hackers, and future research can draw parallels to the gender dynamics in more traditional activism for additional implications into the gender dynamics of hacktivist communities. An understanding of the psychological parallels between hackers and activists would further elucidate the motivations of hacktivists in choosing electronic civil disobedience, reinforcing the importance of maintaining this method of protest in a digital world versus other activist tactics.
Appendix One: Graph of DDoS Attack

The red line shows the spike in traffic to a website, or increased number of requests per second. At that time, more people (or botnets) were trying to access the server. The rapidly increased number of requests helps a company detect that a DDoS attack is happening. With a RUDY attack, this spike will be less significant, as there are net fewer requests. This makes detection more difficult.


https://www.incapsula.com/blog/valentines-day-traffic.html.
Appendix Two: The Political Compass

Two diagrams from the Political Compass map political alignment on economic and social scales. Modified to include mapping for Aaron Swartz.

Appendix Three: Diagram of Research Aims

The existing, minimal area for electronic civil disobedience.

The shift to reform the CFAA that other research has already suggested.

The shift suggested by this research to expand definitions of hacking.
Bibliography


Alleyne, Brian. “‘We are all hackers now:’ critical sociological reflections on the hacking phenomenon.” Goldsmiths Research Online (2011): 1-32.


*Mr. Robot*. “eps1.6_v1ew-s0urce.flv.” Episode 7. Directed by Sam Esmail. Written by Kate Erickson. USA Network, August 5, 2015.

*Mr. Robot*. “eps1.7_wh1ter0se.m4v.” Episode 8. Directed by Christoph Schrewe. Written by Randolph Leon. USA Network, August 12, 2015.

*Mr. Robot*. “eps. 1.8_m1rr0r1ng.qt.” Episode 9. Directed by Tricia Brock. Eritten by Sam Esmail. USA Network, August 19, 2015.

*Mr. Robot*. “eps1.9_zer0-day.avi.” Episode 10. Directed by Sam Esmail. Written by Sam Esmail. USA Network, September 2, 2015.

*Mr. Robot*. “Mr. Robot_dec0d3d.doc.” Special episode. USA Network, June 20, 2016.


Stanford Encyclopedia of Philosophy. s.v. “Civil Disobedience.”
https://plato.stanford.edu/entries/civil-disobedience/.


Tanczer, Leonie Maria. “Hacking the Label: Hacktivism, Race, and Gender.” Ada: A Journal of Gender, New Media, and Technology, no. 6 (February 2, 2015).


https://www.politicalcompass.org/analysis2.


