Beyond Invention: How Hackers Challenge Memory & Disrupt Delivery

Timothy Alan Lockridge

Dissertation submitted to the faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
In
Rhetoric and Writing

Diana George
Carlos Evia
Shelli Fowler
Katrina Powell
Cynthia Selfe

March 29, 2012
Blacksburg, VA

Keywords: Circulation, Delivery, Distribution, Hacking, Memory

Beyond Invention: How Hackers Challenge Memory & Disrupt Delivery

Timothy Alan Lockridge

Abstract

This dissertation uses a case study of *2600: The Hacker Quarterly* to consider how the practices of a hacker public might be theorized as a rhetorical activity. The project is contextualized within a history of hacking (building from a narrative that centers on Levy's 1984 book *Hackers*) and within the arc of recent copyright legislation, specifically the Digital Millennium Copyright Act (DMCA) and the 2011-12 Stop Online Piracy Act (SOPA) debates. Within this framework, the dissertation examines how specific patterns and cases within *2600* might further our understanding of the rhetorical canons of memory and delivery and of dissent in digital spaces.

Specifically, the project presents three practices of memory at work in *2600*: Aggregating, Fingerprinting, and Narrating. Drawing on the work of Collin Gifford Brooke and Mary Carruthers, among others, the dissertation examines how texts printed in *2600* present memory not as an inert technology but rather as a practice and a pedagogy—a response to the increasing commercialization of technology. The dissertation then uses Jim Porter's *techne* of digital delivery to analyze three specific moments in *2600*'s history (the 1985 U.S. Government raid on New Jersey hackers, the E911 lawsuit, and the DeCSS narrative), illustrating how our spaces of textual production have become increasingly regulated and commercialized and considering how that regulation/commercialization affects our understanding of ownership, circulation, and the public sphere.

Building on Michel de Cereteau's concept of strategies and tactics and Michael Warner's theory of (counter)publics, the dissertation ultimately argues that a history of hacker publics offers one way to reconceptualize and reintegrate theories and technologies of digital circulation into our scholarly work and curricular goals.

Dedication

In memory of my grandfather, Curtis Roy Hunt, who told me to never stop learning.

Acknowledgments

First, thanks and acknowledgments are in order for my dissertation committee: Diana George, who put so much faith and energy into my work and who taught me so very much about teaching, researching, and thinking; Carlos Evia, who was always willing to offer close readings and feedback; Shelli Fowler, who was a source of invaluable support; Katy Powell, who offered ongoing enthusiasm and thoughtful critiques; and Cynthia Selfe, who was always at the ready with important insights and endless generosity. In short, I've been blessed with a set of incredible mentors, and I'm very thankful for the time and energy that they have invested in my scholarship and professional development.

I would also like to thank Carolyn Rude, Paul Heilker, Kelly Pender, Kelly Belanger, Matthew Vollmer, Erika Meitner, Gardner Campbell, and Fred D'Aguiar for offering valuable support and advice when I needed it. I am also thankful for the support of many colleagues in the field of Rhetoric and Writing. John Trimbur, Paula Mathieu, Gail Hawisher, Derek Ross, Quinn Warnick, and Ryan Trauman all helped to develop my thinking on this project, and I appreciate their support.

Additionally, Amy Reed, Dan Lawson, and Libby Anthony sat through many drafts of and conversations about this dissertation, and they should each be applauded for their patience and insight. I've found a wonderful group of peers, friends, and colleagues at Virginia Tech, and although I will be sad to leave them, I look forward to hearing of their many future successes.

Finally, thank you to my friends in Indiana and—most importantly—my family. You have been so very supportive of my education and professional development, and I can't thank you enough.

This dissertation was written in Byword and Scrivener, using John Gruber's Markdown syntax. Dustin O'Halloran's piano solos provided the soundtrack for composing. Coffee provided the fuel. And the above listed people, among many others, provided the support. Thank you all.

Table Of Contents

List of Figures

Chapter One: Introduction

> "We have, as a culture, watched the twin strands of technology and literacy become woven into the fabric of our lives—they are now inscribed in legislation, in the law—in the warp and woof of our culture. But, recognizing this context, we cannot allow ourselves to lose sight of either formation." (435)
>
> —Cynthia Selfe, from "Technology and Literacy: A Story about the Perils of Not Paying Attention"

> "The slogan of the hacker class is not the workers of the world united, but the workings of the world untied." (006)
>
> —McKenzie Wark, from *A Hacker Manifesto*

Where We Begin: SOPA, DNS, and Digital Literacies

It seems appropriate to begin this dissertation with one of the major technological news stories of 2011: The controversy surrounding the Stop Online Piracy Act (SOPA). Introduced in October 2011 by representative Lamar Smith of Texas, the SOPA bill included a number of provisions that would allegedly help the United States government manage the threat of international[1] piracy. To date, the burden of managing copyright infringement has typically fallen on the copyright owner: A copyright holder, upon discovering or being alerted of an

---

[1] The bill—and the talking points of its proponents—regularly presented piracy as an external threat. The subtitle of the bill, for example, states that its purpose is "To promote prosperity, creativity, entrepreneurship, and innovation by combating the theft of U.S. property"—rendering piracy as a problem imposed on the U.S. and its seemingly natural state of prosperity and innovation. Additionally, the bill included provisions regarding sites that sell unauthorized prescription drugs, listed under a section that had provisions for sites that "endanger public health"—again, positioning digital threats as something beyond an internal/domestic and sanctioned system.

infringement, must send some sort of notice to the owner of the site where the duplicated content is distributed. This system was introduced as part of the (1998) Digital Millennium Copyright Act, and various startups and young companies have argued that this current system of infringement reporting allows new business models to grow and thrive without fear of litigation, as a service like YouTube isn't responsible for policing each video uploaded to the site. Such policing, they argue, would place a tremendous burden on a young company and stifle growth.

The SOPA bill was a challenge to that model, proposing that sites holding infringing content should be blocked by Internet Service Providers and banned by advertising services. Specifically, the SOPA bill required that "a service provider shall take technically feasible and reasonable measures designed to prevent access by its subscribers located within the United States to the foreign infringing site" (United States HR 3261) by disrupting the Domain Name Service (DNS) link to a site. Although the Web's ease-of-use centers on human readable addresses (www.vt.edu, for example), those addresses resolve to specific, numeric IP addresses (198.82.183.54)—and that translation happens through DNS. DNS facilitates a readable system of web addresses rather than strings of digits, and it also offers a degree of mobility; the numeric address of a site can change, but a system administrator can simply update the site's DNS record and an end-user is never the wiser. This also, however, introduces what Tim Berners-Lee (the often-cited inventor of the Web) sees as the Web's "one centralized Achilles' heel by which it can all be brought down or controlled" (126). Because the Web needs an index and an operator to manage the many domain addresses, it has a potential point of disruption. The SOPA bill was an attempt to extend the U.S. Government's (and private industry's) control over that single point.

This can all sound exceedingly technical, and that is part of the problem: The DNS system—and others like it—was built to facilitate a flexible and user-friendly Web. But that ease-

of-use ultimately renders the Web transparent, its workings deemed too complicated, too impenetrable, or too irrelevant to the interests of the casual user. For many users, the Web browser or the Google search field is the whole of the Internet, and a technology like DNS—which is, all in all, a relatively simple concept—remains a mystery.

For many technology bloggers, scholars, and journalists, the perceived lack of technological literacy among legislators was a major problem with the SOPA bill. In the SOPA judiciary committee hearings, the congressional representatives who discussed and evaluated the bill seemed to have little knowledge of the connected technologies. Rep. Mel Watt, in defending his ignorance of these technologies, positioned himself "as one who acknowledged in his opening statement that he was not a nerd and doesn't understand a lot of the technological stuff," and Rep. Jason Chaffetz, in criticizing the bill, suggested that "maybe we ought to ask some nerds what this thing really does" (United States *Markup of HR3261*). In the SOPA discussion, an understanding of the relevant technologies was seen as nerdy and needless, a nuisance that was immaterial to the legislation's core concerns of property and ownership.

Although many of my colleagues are great deal more savvy than Reps. Chaffetz and Watt (and might even be some of the nerds of which they speak), I can't help but see an analog in the congressional discussions of SOPA and the lineage of our field's academic approaches to text. The field of Rhetoric and Writing has done much to evaluate core concerns of textual ownership, expanding our understanding of transmission and materiality beyond just that of the print book or alphabetic text—especially in regards to issues of property, fair use, and copyright. However, we still haven't thoroughly engaged the economies and technical realities of textual transmission in digital spaces. And as Kathleen Welch has argued, this approach to texts (specifically, an approach that has deemphasized delivery) enabled the growth of current-traditional pedagogy

and falsely presented language as something outside ideology (145). In some ways, this tradition seems like a lingering effect of print's influence; the materiality and distribution channels of the book (deceptively) seemed obvious and straightforward. If concerns of memory and delivery were traditionally outsourced to publishers, one might argue, couldn't the digital be seen as a simple extension of that?[2]

The primary project of this dissertation is to challenge that question and to reassert the importance of digital delivery technologies to the teaching of writing. I do this through a case study of *2600: The Hacker Quarterly*, a hacker publication founded in 1984 and still in print today. *2600*, as I read it, is an enthusiast publication, a magazine written and read by the above-mentioned "nerds"—a digitally savvy public. *2600* also exists within a lineage of hacker texts dating back to the *Youth International Party Line*, a 1970s collaboration between Abbie Hoffman and phone "phreakers." If the work of our field has traditionally veered away from the technologies of textual transmission, I argue, this history of hacking might offer one way to reconceptualize and reintegrate those technologies into our scholarly work and our curricular standards.

In this first chapter, I outline the scope, exigence, and methods of my project. I begin by continuing my discussion of the SOPA bill, describing the roles of corporate and individual resistance to the proposal and grounding those activities in Michel de Certeau's concept of tactics and strategies. Next, I discuss this project's methods, methodologies, research questions, and limitations. Because the project (and thus my methods) is centered in issues of publics, I outline Michael Warner's reading of publicness and address the concepts of both publics and

---

[2] This stance isn't limited to academic circles; it is the same approach used by "old" media companies to determine digital market models and to situate the legislation of digital spaces. Hence, SOPA.

counterpublics, focusing on how those publics function within a system of strategies and tactics. Because chapters three and four focus largely on questions regarding the rhetorical canons, I also briefly address how the canons influence this project and discuss my decision to use them as a major construct. As part of this discussion, I will turn to Prior et al.'s argument for a reconsideration and restructuring of the canons, work which I use to situate my project and to underscore my decision to use the canons in their classic form. Finally, the chapter ends with a brief overview of the dissertation's arc and a narrative regarding my connection to *2600* and my position as a researcher.

In the scope of this project, I don't want to problematize without praising. Our awareness of the digital—in terms of both scholarship and pedagogy—has significantly increased in recent years. As part of that increased awareness, however, our reliance on commercial technologies has grown. Our universities purchase expensive Blackboard licenses, our academic journals still exist within proprietary databases, and our students work with many commercial tools, from Microsoft Word and Adobe Photoshop to Twitter and Tumblr. For the most part, our reliance on these technologies is unavoidable; they're firmly woven into our digital spaces and culture. Many of these technologies also offer networked opportunities and advancements that were simply impossible in years before (Google Documents, for example, offers a type of real-time collaboration that can't be recreated with paper), and our work is richer for them.

My concern, however, rests in a lack of understanding of how these technologies work. Even the most basic Web concepts—DNS and IP, for example—are largely absent from the ways we teach and talk about text. And, to me, it is no surprise that these are precisely the technologies upon which the legislation and regulation of our digital spaces is centered. If we follow scholars like Andrea Lunsford who rightly assert that the Web has sparked an unprecedented growth in

the production and consumption of text, we must also consider how a critical awareness of those technologies becomes central to the discussion and distribution of texts. The work of hacker publics and of texts like *2600: The Hacker Quarterly* offers one way to think about that awareness. I hope that others will follow.

SOPA Blackout, DDoS, and the Technologies of Resistance

The Congressional SOPA hearings generated a great deal of interest within the Web industry. Companies like Google, for example, circulated documents encouraging lawmakers to "End Piracy, Not Liberty," arguing that the SOPA bill would "censor the web," would "be job-killers, because they would create a new era of uncertainty for American business," and "wouldn't stop piracy" ("More about SOPA and PIPA"). Other organizations—such as the Save Hosting coalition and ad hoc venture capital groups—echoed these concerns, generating a movement that ultimately culminated in a letter to congress from companies such as AOL, eBay, Facebook, Yahoo!, and Twitter. This letter, which was reprinted as a *New York Times* advertisement with the title of "We stand together to protect innovation," argued that SOPA would "expose law-abiding U.S. Internet and technology companies to new and uncertain liabilities" and would "pose a serious risk to our industry's continued track record of innovation and job creation, as well as our nation's cybersecurity" (Blagdon). The ad's focus on innovation firmly centered the SOPA debate in economic terms. Positioned as such, SOPA wasn't a challenge to democracy or to public speech, but it was rather an attack on job creation and innovation in Silicon Valley. The full-page advertisement, which closed with each company's logo in the footer, presented the SOPA bill as a battle between old media conglomerates (the media companies and organizations that supported the bill) and new media startups (the hosting

providers and social networks that distribute digital content). Considered as a narrative, the SOPA hearings were a showdown on the floor of Congress, a tug of war between two groups of corporations determining the scope of property and ownership law. This was, it seemed, a conflict between content providers and content distributors, with seemingly few points of entry for the end user.

In response to the hearings and the implications of the bill, a group of Wikipedia editors began discussing potential protests. These conversations yielded Wikimedia's "SOPA initiative," a project—organized through discussion on Wikipedia/Wikimedia pages—to develop an activist agenda in response to SOPA. In those discussions, the editors regarded Wikipedia as a unique space for education and action (specifically because of the large and general readership of Wikipedia, rather than the technologically-focused readership of many sites that initially responded to SOPA), and they ultimately proposed a day-long "blackout" of Wikipedia—taking the US version of the site offline in protest. This proposal was subject to a community vote, and more than 2,000 Wikipedia editors offered opinions. An overwhelming majority supported the blackout, with the opposition citing how the blackout would violate Wikipedia's Neutral Point of View policy, would harm the flow of information, would make Wikipedia a political tool, or would fail to achieve any sort of tangible outcome ("Wikipedia:SOPA Initiative"). After drawing significant internal support for the blackout, Wikipedia, on January 18, 2012, replaced the

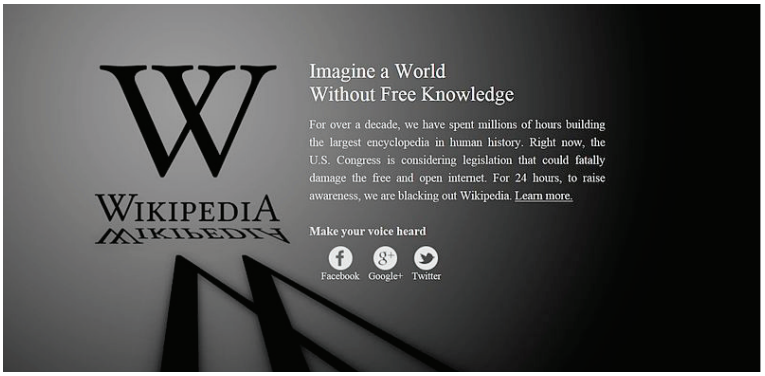

Figure 1 [fair use]
Screenshot of the January 18, 2012 Wikipedia Blackout from Wikimedia Foundation; "History Wikipedia English SOPA 2012 Blackout2"*Wikipedia;* Wikimedia Foundation; 19 January 2012; Web; 22 January 2012.

English language site's homepage with a single announcement that asked the reader to "Imagine a World Without Free Knowledge" (Figure 1). Other major sites followed (including Craigslist, Tumblr, Reddit, and others), and the project was ultimately a success, rallying a tremendous amount of media coverage and public support. Many members of Congress withdrew their support in the blackout's wake, and Rep. Lamar Smith, the bill's author, stated that "It is clear that we need to revisit the approach on how best to address the problem of foreign thieves that steal and sell American inventions and products" (Tsukayama). The impending SOPA vote was delayed, and the blackout organizers deemed the protest a success.

Part of the blackout's prominence and effectiveness stemmed from its technological simplicity, as many of the participating sites used a simple script to overwrite the home page—a quick fix for any webmaster. Sites like sopablackout.org also facilitated the blackout's growth, providing individuals with a simple line of code that, when pasted into a home page, would replace the site with an anti-SOPA banner. This functionality was then simplified and extended with the development of a WordPress plugin that allowed users of the popular WordPress blogging tool to easily join the protest. Through a simple snippet of code, the blackout movement had moved well beyond Wikipedia, into smaller commercial sites and personal blogs. By many measures, the blackout did much to raise popular awareness of the SOPA bill and to extend entry into the conversation beyond just technological enthusiasts or those with lobbying and advertising power.

This isn't to say, however, that the response to the SOPA blackout was entirely positive. In a *New York Times* editorial, RIAA[3] Chief Executive Cary Sherman took aim at the protest, arguing that Wikipedia and Google abstracted the bill into simple censorship. "The hyperbolic

---

[3] Recording Industry Association of America, a group that represents the major record labels as well as many smaller labels

mistruths," he writes, "presented on the home pages of some of the world's most popular Web sites, amounted to an abuse of trust and a misuse of power." Specifically, Sherman takes aim at the alleged neutrality of Wikipedia and Google, asserting that "Wikipedia and Google don't recognize the ethical boundary between the neutral reporting of information and the presentation of editorial opinion as fact." Sherman describes a moment where the public has been duped into participating in hacker-like obstructions—"How many knew what they were supporting or opposing?," he asks, questioning, "Would they have cast their clicks if they knew they were supporting foreign criminals selling counterfeit pharmaceuticals to Americans? Was it SOPA they were opposed to, or censorship?"—an argument that allows him to reach a question of *real* censorship:

> And how many of those e-mails [to Congressional Representatives] were from the same people who attacked the Web sites of the Department of Justice, the Motion Picture Association of America, my organization and others as retribution for the seizure of Megaupload, an international digital piracy operation? Indeed, it's hackers like the group Anonymous that engage in real censorship when they stifle the speech of those with whom they disagree. (Sherman)

Sherman is referring to one of the most contested forms of digital dissent: The Distributed Denial of Service (DDoS) attack. A DDoS attack essentially overloads a website, simulating what would happen if millions of individuals simultaneously loaded a given webpage —overwhelming the server and rendering the page useless. Typical DDoS attacks are carried out through networks of compromised computers (often referred to as "botnets"). An attacker can then use these networks to overwhelm a given site, and multiple attackers, using multiple botnets, can quickly disable the largest of sites. In recent years, with the rise of hacktivist

collectives like Anonymous, the DDoS attack has become a favorite form of digital dissent. In 2010 and 2011, hacker groups used DDoS attacks to take aim at many major companies and government agencies.

The DDoS attack, although easy to carry out, is both illegal and a subject of debate in many hacker publics. DDoS advocates claim that it is a modern, digital extension of a sit in; thousands of Web browsers effectively "sit in" a website, using a massive amount of traffic to block the site and prevent visitors from entering. Critics claim that the sit in analogy isn't appropriate, because DDoS participants don't risk their physical bodies as do traditional participants of sit in protests. Additionally, DDoS attacks don't accurately reflect participatory volume, as one attacker might control thousands of participating computers. The disruption of a website requires a significant amount of traffic, which is why DDoS attacks typically require the use of compromised networks.

Even within hacker circles, the DDoS attack is a subject of debate. As I will discuss in the following chapter, many hacking narratives define the term *to hack* as a clever solution, a new way of thinking through or solving a problem. The DDoS attack, they argue, lacks a clever approach or method. Instead, it is simply the product of an attacker wielding a network of compromised machines. Although it might be an effective form of digital disruption, it isn't, some would argue, a *hack*.

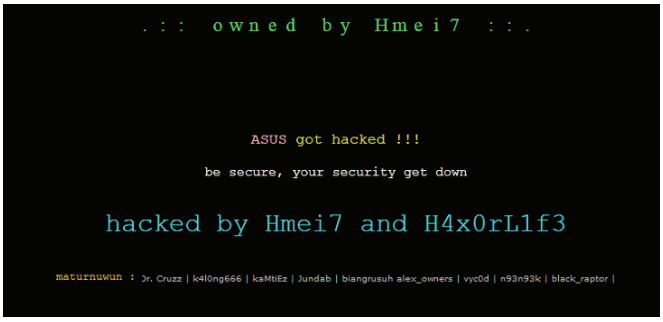

Figure 2 [Creative Commons Licensed]
Screenshot of a website defacement attack
from *Cyber War News*; "Asus Websites Hacked"*Cyber War News;* 14 January 2012; Web; 14 January 2012.

Sherman's comparison of the blackout to DDoS attacks might be off the mark, but the blackout does seem to have similarities (if only aesthetic) to the underground tradition of hacking

sites and replacing the home page with some sort of announcement (Figure 2). An attacker, gaining access to a site and compromising a server, typically replaces the home page with a note —taking credit for the attack, citing any friends who might have helped with the project, and telling the system administrator to fix the vulnerable parts of the server. Recently, activist groups like Anonymous have used these defacement announcements to raise awareness about the corporate defunding of Wikileaks or the US Government seizure of domains like Megaupload (an alleged home of pirated content).

Across the SOPA Blackout, DDoS attacks, and website defacement attacks, there is a history of home page replacement as a means to generate awareness and interest in a specific cause. This history has been especially prevalent in hacker circles. Like all facets of hacker culture, however, the approach is fragmented, distributed, and varied. The term *hacker* is not a monolith, and the approaches and ideologies often associated with *hacking* are quite divergent.

Strategies and Tactics: Thinking through Divergent Practices

My reading of hacker activity is largely informed by Michel de Certeau's concept of strategies and tactics, as outlined in his (1984) book *The Practice of Everyday Life*. De Certeau's project works to acknowledge consumer agency within processes that are sometimes labeled as simple consumption, and his work has thus informed a number of popular culture theorists— most notably Henry Jenkins, whose notion of fan-based "participatory culture" draws directly from de Certeau's theory of poaching (rather than consuming). Much of de Certeau's work offers a frame for thinking through collective action and agency, especially in digital—and often consumption-driven—contexts.

My project draws on de Certeau's understanding of *strategies* and *tactics*, his way of thinking through power relationships in everyday practice. A strategy, based on a reading of de Certeau, is "the calculation (or manipulation) of power relationships that becomes possible as soon as a subject with will and power (a business, an army, a city, a scientific institution) can be isolated" (35-36). Strategies are a set of actions that determine the rules of engagement, using a systematic power to determine spaces and to impose norms. "Every 'strategic' realization," de Certeau writes, "seeks first of all to determine its 'own' place, that is, the place of its own power and will, from an 'environment'" (36).

Tactics, in comparison, lack a space. They are momentary, impromptu, "a calculated action determined by the absence of a proper locus" (37). If strategies determine the rules and boundaries of spaces, then tactics function in the cracks of those systems, searching for opportunities within fissures. Where strategies are present and imposing, tactics are mobile and momentary—what de Certeau refers to as "the art of the weak" (37). Tactics hinge on awareness, on the ability to see and exploit opportunity. They are, as de Certeau writes, "clever tricks" (xix) and "a guileful ruse" (37). Because of their opportunistic and momentary nature, tactics have a distinct impermanence. They aren't strategies. Tactics might shift the behaviors or focus of strategies, but they privilege the moment over the place.

When considered as such, de Certeau's concept offers a rich theoretical framework for the reading of hacker (and enthusiast/hobbyist) publications and activities. As I'll note in a later chapter, the practice of hacking is fundamentally a practice of response: A hack requires a hackable object. The hack is a clever approach to a technology or a problem or a policy—a momentary unwinding of a tool or a system. That unwinding, however, often provokes some sort of response in the strategy, a change in the terms of engagement. That response also effects a

shift in the system and a negation of the hack. In some instances, the hack might be subsumed into the system. This is often evident in the iPhone jailbreak community, where unauthorized modifications of the iPhone's operating system can lead to the inclusion of those very features in future official releases. In other instances, however, the system simply adjusts to the hack or remedies the vulnerability through which the hack operated. This is often the case with software exploits.

Although it wasn't necessarily a *hack*, the SOPA Blackout functioned in much the same manner, and it is representative of a hacker history that is centered in conflicts with Bell Corporation. As I will discuss later in the dissertation, there is a long lineage of tension between the Bell Corporation and computer hobbyists. Specifically, hobbyist attempts to explore the phone system were regularly thwarted by Bell, generating a long interchange of tactics (in which, for example, phone hobbyists of the 1950s found technical manuals in university libraries, photocopied them, and then distributed them) and subsequent adjustments to the Bell strategy (in which Bell would no longer archive technical manuals in university libraries). The SOPA blackout, considered in terms of tactics and strategies, could be read in a similar manner. Various publics organized and aligned in protest, and using a tactical approach—a snippet of code that disrupted the viewing experience—they were able to negate the SOPA bill, shifting the strategy of media organizations and the governmental regulation of those organizations. However, like many of the tactics used by hacker publics, the effects are tenuous. Although the strategies will shift in response, they remain the dominant, space-driven construct. Sherman illustrates this in his *New York Times* editorial, writing that, "It has become clear, at this point, neither SOPA, PIPA, nor OPEN is a viable answer." The tactic has worked. But he follows that assertion with the promise of a shifting strategy: "We need to take a step back to seek fresh ideas and new

approaches" (Sherman). The regulatory strategy will adjust for the tactic and a new bill will surely enter the legislature, requiring a new momentary awareness and a new tactic.

Through this lens, the work of hackers becomes something more than vandalism or simple subversion; instead, hackers push against a capitalist computing culture that promotes the corporate ownership of code and user data and then licenses limited use of that code (or leverages the users and their data as advertising commodities) for profit. The positions and projects endorsed by this dissertation's publics and texts are tactics, what de Certeau sees as a "use of the cracks that particular conjunctions open in the surveillance of the proprietary powers" (37). These texts then offer a set of tactically and rhetorically situated artifacts, a product of the strategies employed by a commercial system of power. The writers in *2600*, for example, are similar to the textual nomads that de Certeau describes—individuals that move within a vast system but that also use their nomadic position to momentarily disrupt that system.

Hacker Publics: Theorizing Divergent Texts and Activity

Situated in the work of strategies and tactics, my methodological framework connects de Certeau's reading of that activity to Michael Warner's structures of publics and counterpublics. This position is informed by a cultural studies lens, a tradition that, as Stuart Hall notes, focuses on "the centrality of texts and discourse and the practices of representation" and which "[appropriate] historical methods of research on archives, documentary, and other sources" (41). This is an academic tradition that extends into many contemporary studies of popular culture practices (for example, the work of Fiske and Jenkins) and it provides an important critical framework for this project. Likewise, a cultural studies lens allows me to consider this

dissertation's texts beyond the boundaries of the page, contextualizing the ways in which "subcultures are produced by a dominated culture, not by a dominant culture" (Cohen 85).

From this cultural studies position, I use Michael Warner's concept of the public as a key lens for my study. Warner's understanding of a public situates both discursive address and identity within the circulation of texts, offering a means of theorizing self-published texts and activism as a type of rhetorical activity. Warner provides a necessary frame, as the term *hacker* is highly problematic. Under the hacker umbrella, for example, there are countless individuals and activities: hobbyists, activists, and criminals among them. Although many writers have attempted to explore and examine the activities typically associated with *hacking*, I find it more helpful to situate my analysis within one *hacker public*. My reading thus requires a grounding in publicness, a framework I adapt and extend from Warner.

For Warner, there are three major conceptions of "public": First, there is *the* public, "a kind of social totality" (65); second, there is the public of "A concrete audience, a crowd witnessing itself in visible space," a public that "will have a sense of totality, bounded by the event or the shared physical space" (66); and third, there is "the kind of public that comes into being only in relation to texts and their circulation—like the public of this essay" (66). Warner focuses on this third type of public, and his understanding offers a helpful conceptual framework for my project—situating the hacker publication and its circulation in relation to a public. I therefore think it is helpful to consider and contextualize Warner's understanding of this third type of public.

Warner presents seven major facets of this public:

1. A public is self-organized.
2. A public is a relation among strangers.
3. The address of speech is both personal and impersonal.
4. A public is constituted through mere attention.

5. A public is the social space created by the reflexive circulation of discourse.
6. Publics act historically according to the temporality of their circulation.
7. A public is poetic world making. (67-114)

The key terms in this list speak both to the cultural work of activism and to the material processes of self-publishing. Consider, for example, a notable difference between a traditional magazine and a self-published zine. When a reader subscribes to *The Atlantic*, she does so through any number of distribution channels: A website, a phone number, or the tiny cards that (rather annoyingly) fall from existing copies. Traditionally, zines have lacked those normal distribution processes, and copies might be acquired through photocopy exchanges, conventions, or small bookstores. Only the largest zines have a regular publishing schedule and offer subscriptions. Even then, however, the receipt of that zine—and thus the public of it—is fundamentally different. With a publication like *The Atlantic*, there are regular writers/columnists, and those writers are specifically divorced from the readers. Aside from the possibility that *Atlantic* readers might someday become *Atlantic* writers or columnists, there are specific spaces for reader contributions (the brief "Letters" section) and a space for writer/editorial contributions (the rest of the magazine). More so, letters from readers rarely exist in conversation with other letters, and editor/writer responses are occasional and occur mostly when the reader's question or concern can be addressed with only a few sentences. The conversation ends at that point. In a publication like *2600*, however, reader contributions are the primary source of content. Similarly, letters to the editors serve a different purpose and seem to work in a more conversational manner, creating a different sort of artifact—and thus a different sort of public. Although the term *hacker* is diffuse and problematic, by positioning the readers (who are also the writers) of *2600* as a *hacker public* I am able to discuss hacker activity in one specific context, in relation to one specific text.

The other half of Warner's public construction, the counterpublic, initially seemed like a helpful theoretical tool for this project. However, after spending some time with *2600*, I was hesitant to position the *2600* public as *counter*. Warner describes counterpublics as a public "defined by their tension with a larger public" and a public with "an awareness of its subordinate status" (56). Although the public of *2600* has surely existed in tension with several commercial and governmental entities, it has also regularly stated that the publication isn't an underground endeavor; the editors of *2600* see it as a normal hobbyist publication—a stance reinforced by the publication's acquisition of a barcode and distribution through major booksellers. Additionally, the readership of *2600* includes managers, developers, and technological specialists who work for major computing corporations and for the government—entities that determine the strategies of mainstream computing.

I thus see the readership of *2600* as a public—"the kind of public," as Warner says, "that comes into being only in relation to texts and their circulation" (66). Individuals within the *2600* readership surely belong to other publics, but their participation in *2600* makes them part of the circulation and discourse within one specific hacker public.

Research Questions

If, following Warner, this project views *2600* and its readership as a hacker public, the primary research question considers *how* the role of the publication within the public:

> *Research Question 1:* How do hacker publications generate a public, the political stances of that public, and provide a context for and concept of political action within that public?

The first major hacker publication (*The Youth International Party Line*) was a product of both a political movement and an anti-war moment. By exploring that publication, its context, and its development (as well as that of the publications which followed it), how might we trace the development of those political ideas and the ways that they've enabled a public?

Similarly, these hacker publics place an emphasis on instruction, both in terms of technical walkthroughs (how to understand and exploit a given piece of software) and in terms of activism. The second research question then considers the role of instruction within the public:

> *Research Question 2:* How do hacker publications teach? How do they inspire—or actually call—for action? How do they unify/organize a community?

These first two questions situate the project's primary concerns, and they guide much of the inquiry. Two additional questions, however, have also shaped the project.

When I began this project, a single question hovered in the periphery: *Why would these hobbyists, a digitally-savvy and sophisticated public, produce a print publication? Why not digital?* While I quickly found answers to this question[4], the role of print technologies still seemed of significance to the study:

> *Research Question 3:* How did print technologies contribute to the production and distribution of the publication and its public? How might digital technologies be employed in a similar manner?

And finally, in connection to both the arc of these publications and to the current moment of digital activism and dissent, questions regarding the materiality of print—and its role in both protest and in the academic conversations surrounding writing instruction—also inform this project:

---

[4] As I discuss in subsequent chapters, print technologies have offered *2600* a deal of legal and journalistic protection. Digital publications, especially in the 1980s and 90s, did not fare as well.

Research Question 4: What might print hacker publications tell us about the ways in which a public conceptualizes and organizes itself? How might they better help us think about digital spaces and their capabilities for organization and dissent?

To what degree is a facet of print production—like that of the anonymity offered by photocopiers and non-traditional distribution channels—essential to its message? How does this connect to a digital space? Within the scope of this project, those concerns seem especially important to both the work of *digital* activism and to future work in the field of Rhetoric and Writing.

Methods

Historical research methods, it seems to me, can be a blurry business. Although our field has produced a few helpful essays for the first-time historian, there's often little said in terms of the actual steps involved in archival work. Typically, the advice for historical work often centers on some variation of "let the archive speak to you"[5]. I thus entered this project with a great deal of trepidation and a number of questions, including, most pressingly, *How exactly do I let the archive speak to me?*

Additionally, in moving through this project I've resisted a standard coding process of quantitatively reading my source texts for a predefined set of keywords. Following Lynée Lewis Gaillet's assertion that "storytelling—with a purpose, based on painstaking research, tied to a particular cultural moment, making clear the teller's prejudices—is the real task of the historian, regardless of the negative connotations often associated in academia with storytelling" (36), I've approached this project through a reading of history and of narrative, attempting to contextualize a hacker public within a history and also within my understanding of the present moment.

---

[5] Connors' "Dreams and Play" immediately comes to mind

To complete this project, I acquired every issue of *2600: The Hacker Quarterly*—from the first issue (January 1984) to the present. I initially planned to read through these issues and to make notes in a matrix (a table-based hypertext document that I developed) with fields for documenting internal references to other issues, external works cited, and popular/political events referenced. After using the matrix to read the first four years of *2600*, however, I felt that the matrix was both straining the project and my ability to read and synthesize the texts. I wasn't quite sure what I was reading the texts for, and although the matrices created the semblance of a methodologically sound approach, I didn't feel as if they were helping me gain an understandings of the texts or their public.

Still in the early stages of my work and frustrated with the approach, I began assembling some preliminary thoughts for a presentation at the 2011 Conference on College Composition and Communication. While at the conference, through the conversations about my project, I began to realize that my questions and the texts spoke to the rhetorical canons of memory and delivery. I had previously given talks on the role of digital delivery in enthusiast writing groups, and several colleagues noted that the *2600* project had connections to those concerns of delivery and circulation.

After the conference, I began re-reading *2600* for connections to memory and delivery. I documented articles that connected to *practices of memory* (informed by Collin Brooke's use of the term), searching for patterns in those activities. I also read for narratives of delivery, which was a more complex task: The whole of *2600* is, in a way, focused on digital delivery. I focused my reading by returning to my research questions, considering how the narratives—and the discussions they fostered in the text—worked to build, educate, and motivate the readership. Where available, I triangulated these narratives with major news articles and popular nonfiction

texts about hacking, using the LexisNexis database and journalistic considerations of hacking as a means of extending and complicating the stories in *2600*.

There is, I think, room for a future study (likely, a multimodal text) within the initially proposed matrix-driven project. For this dissertation, however, a more general reading of memory and delivery has helped me to better consider how the narratives and practices of *2600* might inform, challenge, and shift the ways we teach and talk about texts.

Although in Chapters Three and Four I address the rhetorical concepts of memory and delivery, and, more specifically, readings and re-readings of them, I do want to here note one major contemporary reconfiguration of the canons. In the "core text" section of their "Re-situating and re-mediating the canons: A cultural-historical remapping of rhetorical activity" webtext, Prior et al. write that although the canons "have offered a map for rhetors and a frame for rhetoricians for at least two millennia" (1), they "suggest that the canons offered only a partial map even of the rhetorical and political worlds of Ancient Greece" (3). Acknowledging the contemporary scholarly reconsiderations of delivery, they write that, given classical concerns and the contemporary focus on media, "it makes more sense to begin remapping rhetorical activity, to trace distribution and mediation, than to attempt to retrofit this ancient tool to do varieties of work it was never designed to address" (8). Through cultural-historical activity theory, Prior et al. offer a remapping of the canons.

The argument is compelling, and I agree with the assertion that our focus should be shifted to concerns of distribution and mediation, moving beyond the notion of delivery (an issue I address in the fifth chapter). For the core of this project, however, I'm interested in the lineage and influence of memory and delivery—specifically, a cultural influence that has shifted our understanding of textual technologies toward a perspective that privileges property and capital.

Although remapping attempts are useful and should be pursued, I argue that the traditional deprivileging of memory and delivery has had significant impacts on both our production of text and the technologies of that textual production.

Limitations

Due to the scope of this project and its methods/methodologies, there are several notable limitations to the work. First, this is largely a case study of *2600: The Hacker Quarterly*. Although I do attempt to generalize and extend my findings beyond this specific case, it is important to note that this is one hacker public among many. As a hacker public, *2600* differs from groups like Anonymous which are more visible, fragmented, and activist-oriented, and I don't think the practices found in *2600* are necessarily applicable to Anonymous or to any other hacker public. In terms of generalizing my work, I'm more interested in how *2600* might help us rethink the ways that we teach and produce texts. In that regard, I think we might draw valuable lessons from the texts studied.

There are also limitations connected to the theoretical frames used in this project. As I've approached this project with an eye on cultural theory, publicness, and texts, I've limited my approach to a specific kind of reading. Another theoretical frame, such as Actor-Network Theory, could yield a different result. In regards to the applied frame, however, I've also stepped away from an extended look at public sphere theory. This, in connection to my use of Warner, limits the work, and a future project might place the texts of *2600*—or perhaps a larger hacker public—within a more detailed examination of the public sphere. But due to the scope of this project and the direction of its findings, I've limited the amount of focus on which I give theoretical considerations of the public sphere, placing the bulk of that (somewhat brief) consideration in

Chapter Five. As I note in that chapter, I follow Clay Shirky's assertion that the Web is "a corporate sphere that tolerates public speech" (qtd. in Vance and Helft), and I read *2600* as a publication—and a public—moving through a set of privatized and increasingly-commercialized spheres.

Finally, I see the print and alphabetic form of this dissertation as another limitation worth noting. Although it might seem that this dissertation follows the print and alphabetic text-centric model of *2600*, I think there is an important case for furthering digital and multimodal scholarship, especially at the dissertation level. That said, the current form of this dissertation is quite connected to the material realities of a genre like the dissertation, especially one that is completed within a very compressed timeframe and within specific institutional constraints. Although this dissertation is a call for extending our understanding of texts and their circulation, it is also quite situated in the economic and material constraints of its creation—a reminder of how any text is positioned. I hope that the findings presented are considered within such a context, as I'm acutely aware of the many institutional pressures on the teaching and production of texts in digital spaces.

A Brief Outline

As I mentioned earlier, this dissertation is focused on the importance of digital circulation to the teaching of writing. To develop this specific case and to work toward an argument, the remaining chapters are organized as follows:

Chapter Two - The Growth of Hacker Publications: In this chapter I examine and reconsider Steven Levy's *Hackers*, a much-discussed book which describes the rise of hacking and the computer industry. Within Levy's narrative, I situate *2600: The Hacker Quarterly*,

discussing another view of a hacker public and hacker culture. I offer an alternate hacking history by beginning with phone "phreakers" in the early 1970s. I situate these publics (and their publications) within a protest of AT&T and the Vietnam War, ultimately extending that arc through the hacking culture of the 1980s and 90s. Additionally, I use this chapter to discuss several popular press books which document the problems with copyright laws and privatization of the Internet. I close the chapter with a consideration of the law (especially the Digital Millennium Copyright Act) and its relation to memory and delivery.

Chapter Three - Hacking and Memory: In this chapter I consider the canon of memory, particularly in regards to technology, and I argue that hackers use the commercial assumptions about memory to then exploit the commercial technologies and ventures that rely on a closed system of memory. I first situate a rhetorical understanding of memory within *practices* of memory, borrowing from Collin Brooke and Mary Carruthers, rather than simply regarding memory as a technology of storage. I use examples from *2600: The Hacker Quarterly* to develop this argument, focusing on three types of activity documented in *2600*: Aggregation, Fingerprinting, and Narrating. With these three activities, *2600* functions as a practice of memory —a way of seeing memory not as an inert technology, but rather as a cultural practice.

Chapter Four - Hacking and Delivery: Building on the Chapter Three, I consider the canon of delivery as it connects to both hacking and the self-publication/distribution of texts. This context situates one of my initial questions: "Why would a digitally-savvy hacker public produce a print publication—and maintain it for twenty-seven (and counting) years?" To answer this question, I focus on several key cases across the history of *2600*: The 1985 government seizure of *2600*'s private bulletin board system, the 1989 distribution of a document related to Bell South's 911 Emergency Systems, and the 2000-2001 distribution of the proprietary code that

prevents unauthorized DVD duplication. Through a consideration of these events, I'm able to trouble assumptions regarding delivery and explore the hacker practices enabled by those assumptions.

Chapter Five - Property, Circulation, Publics: In this chapter I extend the case into both the field of Rhetoric and Writing and the larger scope of digital discourse. For some time, our field (and others like it) has focused on concerns of ownership and intellectual property, a legacy, I think, of our traditional approach to text and to citation. The economies and technical concerns of textual transmission, however, have been marginalized. I argue that we can't continue to see text as decontextualized and abstracted from the material means of digital circulation, and a consideration of those technologies should have a stronger presence in our work. To develop this argument, I draw upon this project's findings as well as work from Rhetoric and Writing scholars such as Selfe and Stolley and public sphere theorists such as Calhoun and Dean. By situating this argument in both the field and in the political concerns of the moment (such as SOPA), I hope to show how the current questions of digital ownership and transmission are also questions of textual circulation. As writing scholars, we have much to offer to that conversation—and to the policies that govern it.

My Position As Researcher: A Narrative and a Stance

Finally, I close this chapter with a narrative which I hope will help to better situate me as a researcher and also clarify my relationship with *2600*. While, until the start of this project, I wasn't a recent reader of *2600*, the publication was a major part of my youth and of my early understanding of computers and networked technologies. A discussion of that relationship seems like an important component of the dissertation.

That relationship begins in 1994. I didn't yet have a driver's license, so I relied on Eric—a family friend—for occasional rides to the comic book store. Eric was a few years older and much cooler than me: He had a car and a leather jacket and a backseat full of punk rock records. He would occasionally dub cassettes for me—The Clash, The Descendents, Bikini Kill—and one weekend, rather than heading straight to the comic shop, we took a detour to The Abyss.

The Abyss was a small independent bookstore located near the University of Evansville. The shop itself was located in the basement of a hair salon, and the building had no signs, no windows, and no visible address; the only thing marking the entrance (an unassuming door painted flat back and recessed in the small space between the hair salon and a sandwich shop) was a sign—maybe a foot long, hanging above the black doorway—illustrated with only an iconic hand pointing toward the door. To enter the Abyss, you had to either show up on the occasional day where they would place a black sandwich board sign on the sidewalk ("Sell Your Books to the Abyss!") or know that the black door existed (it was hard to see) and know that it went somewhere.

Behind the door was a set of uneven and poorly maintained wooden stairs. The downward-sloping ceiling was also painted black, but the stairwell walls were covered with photocopied flyers from years of underground rock shows, and by moving down the long staircase and looking left and right, one could quickly get a history of independent music in the Midwest. The stairs bent to the right at the bottom, and they opened into a refashioned basement whose walls were lined with bookshelves. The perimeter was dedicated entirely to what were probably used books bought from and sold to students from the neighboring University of Evansville: Vonnegut novels, beat poetry, political theory. The center of the store spilled with clothing racks, filled mostly with secondhand flannel and Ramones t-shirts. In the evenings, after

the salon above closed, the clothing racks would be pushed away and the store would transform into a makeshift music venue: Bands would fill the floor with musical gear and eager college students would push into the remaining space, the music shaking the ceiling and spilling out into the street. The Abyss was, at least for a few years, the heart of underground (counter)culture in my hometown.

The most compelling part of the store, however, the part that brought me back again and again during my high school and college years, was a small rack filled with zines. From stapled and folded paper to mass-produced newsprint, the zine rack included small, local publications (I remember Mat Martin's *Life with Roaches*, a photocopied collection of ramblings and comics) as well as major, nationally distributed zines. I can vividly recall my first visit to the store, where I purchased a copy of *Maximumrocknroll*—arguably the most well-known and influential punk zine. I was fourteen and had a handful of punk albums—I knew of The Clash, The Ramones, and Green Day—but *Maximumrocknroll* presented punk as something entirely different, something brash and political and full of life. The zine connected me to punk rock across the world, and—in an era before blogs and message boards—it turned music into a conversation that was more than just sound and style. I would soon become a monthly reader, fingers stained with black ink from the cheap newsprint.

Doug, the owner of the store, pointed me to many music purchases, but he was also especially knowledgable about computers, always speaking of a new Linux kernel or a Telnet connection. My parents had recently purchased a Packard Bell i486, and I was learning MS-DOS and Windows 3.1 and was intrigued by Doug's decidedly more advanced tools. One day, Doug directed me to the zine rack and to *2600: The Hacker Quarterly*. I left with a copy and with directions to the nearest campus computer lab.

For the remainder of the 1990s, I was an avid reader of *2600*. Much of the material was beyond my knowledge or interests (I had, for example, no desire to read about telephones), but—like *Maxmimumrocknroll*—*2600* presented technology as something complicated and compelling and alive. At that point, my knowledge of technology was largely based on library books, an after-school PASCAL club, and my own MS-DOS discoveries. With *2600*, however, I saw how the use of technology could be rebellious and how it could connect to a punk ideology and ethos. For a kid in rural Indiana, this was revelatory.

As I moved through college, I eventually stopped purchasing issues of *2600*, and when I started this project, I was sure it had simply ceased printing. (I was surprised and excited to see that this wasn't true.) When I began reading the texts for this project, however, I was reminded of my connection to the publication and its influence on my early understanding of technology. I am not a neutral researcher.

That said, my research questions and my interests are an investigation of this (and my) history. As *2600* informed my early understanding of technology and connected me to a larger enthusiast public, my questions are a consideration of *how* that connection happens and why, for nearly three decades, it has happened in print. Additionally, I see advocacy and education as a major component of *2600*'s history. By critically considering those practices, I hope to help a public to which I belong today—that of Rhetoric and Writing scholars—better understand the implications and importance of digital circulation.

Chapter Two: *YIPL*, *TAP*, and *2600*: The Growth of Hacker Publications

> "Our civilization runs on software. Yet the art of creating software continues to be a dark mystery, even to the experts. Never in history have we depended so completely on a product that so few know how to make well." (9)
>
> —Scott Rosenberg, from *Dreaming in Code*

> "If DIY had made music available to people who'd previously believed that being in a band was off-limits or beyond their capacity, zines and small presses made writing as a vehicle for self-expression and even self-transformation and communication with like minded people accessible to anyone." (81)
>
> —Kaya Oakes, from *Slanted and Enchanted: The Evolution of Indie Culture*

In *The Master Switch*, Tim Wu builds a history that focuses on a recurring pattern in twentieth-century technologies, what Wu calls "the Cycle" (6). In the Cycle, technological industries move between periods of open and closed states. For example, as Wu documents them, multiple inventors often arrive at a new discovery at the same time. "There was, it is fair to say, no single inventor of the telephone," Wu writes, "And this reality suggests that what we call invention, while not easy, is simply what happens once a technology's development reaches the point where the next step becomes available to many people" (19). According to Wu, after that initial stage of discovery, there is often a period of openness, a space in which experimental and amateur/hobbyist use of the technology reigns. This period of openness, however, is a disruptive

one, and it finds the new technology challenging the existing/dominant structures. A "winner" of sorts then emerges from this disruption, beginning a period of closedness. The disruption and the continued tension between technologies is a hallmark of Wu's Cycle.

Wu traces the Cycle through each of the twentieth-century's major communicative inventions: the telephone, the radio, the cinema, cable television, and the Internet. What strikes me about each of these technologies, however, is the importance of disruptive uses (a history and usage that Wu doesn't necessarily account for). If each of the twentieth century's major technologies moved through phases of growth and regulation/contraction, how did these phases enable user involvement and resistance? And if the narrative of technological advancement is built on a specific type of commercial growth, how do individuals maneuver within and work against that system of power? Within Wu's history, pirate radio seems a relevant example. He writes:

> Radio in the 1920s was a two-way medium accessible to most any hobbyist, and for a larger sum any club or other institution could launch a small broadcast station. Compare the present moment: radio is hardly our most vital medium, yet it is hard if not impossible to get a radio license, and to broadcast without one is a felony. (39)

Wu's cycle shows how the move from openness to closedness renders systems of activity illegal (here: broadcasting without a license); however, the regulation and closing of those systems has hardly thwarted usage.

Within the movements of these systems, as I will argue in the third and fourth chapters of this dissertation, are tensions in the rhetorical canons of memory and delivery. That discussion,

however, needs to be contextualized in two specific technologies: the telephone and the computer.

In this chapter I build a history of hacking, focusing specifically on the development and influence of hacker publications. To begin, I address Steven Levy's influential 1984 book *Hackers*, which documents the birth of post-war computing at MIT and traces the growth of those first hackers as they established the contemporary computing industry. In many ways, Levy's narrative echoes Wu's Cycle: early hacking activity at MIT yielded a stage of experimentation (throughout the 1960s and 70s) which ultimately led to a period of commercial growth and, today, a computer industry dominated by a handful of corporations. After considering Levy's narrative (and the "hacker ethic"—Levy's major contribution), I next turn to the growth of subversive hacking. Although there are many narratives that extend, parallel, and/or counter Levy's (the development of 1980s and 90s open source software communities, for example), I place my focus on the rise of telephone *phreaking* in the 1960s and 70s. Phreakers were/are hobbyists that study (and exploit) telephone systems, a group who gained late-60s notoriety with the "blue box"—an easy-to-assemble piece of hardware that enabled free telephone calls. Blue boxing brought phreaking to the mainstream, and a small group of phone phreakers and political activists produced the *Youth International Party Line* (*YIPL*), an underground phreaker newsletter, and its successor, *Technological American Party* (*TAP*). Through *YIPL* and *TAP*, phone phreakers organized and shared information. *YIPL* and *TAP* were succeeded, in 1984, by *2600: The Hacker Quarterly*, a hacker publication still in print today. Although *2600* is a major part of the following chapters, I here present a brief history of *2600* in order to place it within a context of hacking as dissent. After tracing *YIPL*, *TAP*, and *2600*, I close the chapter with a brief consideration of hacker publications as key to a hacker public

(considered within Michael Warner's use of the term) and within a system of de Certeau's strategies and tactics. I place that theoretical lens at the conclusion of the chapter in order to foreground the hacker narratives and to better build a transition between this chapter and those that follow.

Ultimately, I argue, hacking—and thus hacker publications—offers a way of looking at productive dissent within the technologies of textual production and distribution. This dissent, and the practices embedded within it, can further our understanding of media (both old and new) and inform our practices of producing texts.

Steven Levy and the Hacker Ethic

Steven Levy's (1984) *Hackers: Heroes of the Computer Revolution* documents the rise of post-war computing at MIT, and Levy's book—culled from more than 100 personal interviews—is an influential documentation of the contemporary computing industry. In particular, Levy traces the origins of hacking to the MIT Tech Model Railroad Club (TMRC), a group of MIT students and model train enthusiasts in the late 1950s who shifted their attention to computing when the first TX-0 computer arrived on campus. Access to computing time was limited, and the group would use campus computer labs at night, learning the machine's boundaries during off-hours. The group, lacking formal instruction in the use of these computers, collectively probed the machines, developing programs and pushing boundaries. As Levy describes, it is from this group and this context that the term "to hack" is derived:

> The word 'hack' had long been used to describe the elaborate college pranks that MIT students would regularly devise, such as covering the dome that overlooked campus with reflecting foil. But as the TMRC people used the word, there was

> serious respect implied. While someone might call a clever connection between relays a 'mere hack,' it would be understood that, to qualify as a hack, the feat must be imbued with innovation, style, and technical virtuosity. Even though one might self-deprecatingly say he was 'hacking away at The System' (much as an axe-wielder hacks at logs), the artistry with which one hacked was recognized to be considerable. (10)

Many members of the club quickly lost sight of school and devoted all of their time to learning how these machines worked. From this fervor, Levy writes, a set of principles emerged —what Levy terms *the hacker ethic*. As Levy situates it, this ethic is built on several key principles.

First, "access to computers—and anything that might teach you something about the way the world works—should be unlimited and total. Always yield to the Hands-On Imperative!" (28). Lacking much formal instruction in computers, these first hackers learned the machines through a process of exploration and reverse-engineering. Likewise, through this process, they quickly found ways to adjust and improve the technology. In this sense, any technology should be available for manipulation; any object or system should be studied, scrutinized, and explored.

Second, "All information should be free" (28). Connected to the first principle, the hacker ethic suggests that invention and innovation benefit from a free flow of information, and the spirit of collaboration that fueled hacking was a spirit steeped in the free flow of information.

Third, "Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position" (31). Levy, for example, notes how the TMRC was a meritocracy and quick to welcome non-students who could demonstrate their computer skills or aptitude.

Fourth, “You can create art and beauty on a computer” (31), which seems something like an obvious conclusion today, but was actually rather revelatory in the late 1950s. At the time, computers were programmed with punchcards and assembly language, meaning that human-computer interaction was fairly complex. In no time, however, the TMRC had developed games using the computer’s status lights and programmed music through the machine’s speaker. However, as Levy notes, this perception of art and beauty also extended into coding: The best hacks, meaning the minor improvements to code that reduced memory usage or prompted a more elegant means of accomplishing a task, were considered to be things of beauty. Beautiful and elegant code, according to the hacker ethic, was a kind of art.

And finally, the last principle states, “Computers can change your life for the better” (32). The TMRC saw computers as a means of shifting not only our interactions with technology, but also our perspective on the world: “And wouldn’t everyone benefit even more by approaching the world with the same inquisitive intensity, skepticism toward bureaucracy, openness to creativity, unselfishness in sharing accomplishments, urge to make improvements, and desire to build as those who followed the hacker ethic?” (37). In the eyes of those first MIT students, the computer offered a way to challenge so many of the habits and practices that other (and perhaps less-malleable) technologies had shaped.

Though Levy doesn’t make the connection, much of the hacker ethic resonates with the 1940s/50s post-war visions of and approaches to computing. Vannevar Bush (1945), drafting a plan for post-war science (which would lead to the development of the NSF), noted how scientists had “left academic pursuits for the making of strange destructive gadgets, who have had to devise new methods for their unanticipated assignments” (37). Charting a technological path away from that destruction, Bush proposed the development of a “memex,” a machine that

could store texts and annotations, offering the user a sort of personal library that could assist with research and prompt invention by highlighting the associative connections in texts. Norbert Wiener, in "Men, Machines, and the World About" (1954) also situated post-war thought within the space and potential of technology: "If we can live through it and keep our heads, and if we are not annihilated by war itself and our problems, there is a great chance of turning the machine to human advantage, but the machine itself has no particular favor for humanity" (72). And though Levy's ethic doesn't cite Wiener, "Men, Machines, and the World About" echoes the hacker ethic (and the trajectory of technology), asserting that "If we want to live with the machine, we must understand the machine" (72). Finally, Wiener offers a nod to the contemporary intersections of hacking and government transparency: "We shall have to do this unhampered by the creeping paralysis of secrecy which is engulfing our government, because secrecy simply means that we are unable to face situations as they really exist. The people who have to control situations are as yet in no position to handle them" (72). So although Levy's hacker ethic seems like it is built on a trajectory that extends from MIT, it might also represent the larger orientation of post-war computing—a belief that a massive investment in computing technology could change, for the better, how we interact with knowledge, artifacts, and each other.

The hacker ethic wasn't explicitly stated or formally realized by the hackers of the 50s/60s/70s, but it was rather synthesized by Levy in his 1984 book. (The hacker ethic does, however, carry some strong connections to a text like Ted Nelson's 1974 *Computer Lib/Dream Machines*, which talks of "Thinkertoys," imagines a hypertext environment named "Xanadu," and argues that "You can and must understand computers NOW.") A full understanding of the hacker ethic potentially had a stronger influence on post-1984 computing—especially as seen in

the growth of open-source software communities—than it did in any of the pre-*Hackers* collectives.

Levy's book moves from MIT to the California hobbyist communities of the 1970s, describing the computer clubs that inspired the likes of Steve Wozniak, Steve Jobs, and Bill Gates, and setting the stage for the growth of the modern computer industry and the home computer. At this point in the narrative, the MIT pioneers have dispersed (to places like Stanford, Carnegie Mellon, and industry), and the hacker spirit has shifted to groups like the west coast Homebrew Computer Club. Through the assembly and programming of early home computers, these hobbyist groups carried forward many of the hacker philosophies first demonstrated at MIT. The Homebrew Computer Club, Levy writes, was a space for invention and collaboration:

> The increasing number of Homebrew members who were designing or giving away new products, from game joysticks to I/O boards for the Altair, used the club as a source of ideas and early orders, and for the beta-testing of prototypes. Whenever a product was done you would bring it to the club and get the most expert criticism available. Then you'd distribute the technical specifications and the schematics—if it involved software, you would distribute the source code. Everybody could learn from it, and improve on it if they cared to and were good enough. (221)

In observations like this one, these early hobbyist groups seem like a sort of intellectual utopia; the groups centered on a collective approach to technology—a space for both constructive critique and for the sharing of ideas. Each new idea and invention was fodder for the next, a collective platform to which each group member contributed and built from. This collaborative approach, however, found friction with the development of the first computer

companies. In a now-famous anecdote, a young Bill Gates, in 1975, coded a version of the BASIC programming language for the Altair 8800 microcomputer (a home computer developed by Micro Instrumentation and Telemetry Systems—MITS). The Homebrew Computer Club, however, after obtaining a pre-release version of the program, quickly distributed it among group members for free, requiring only that "if you took a tape, you should make copies and come to the next meeting with *two* tapes" (232). For the Homebrew Club, programming was a collaborative effort, and the BASIC language had immense potential—and should be shared. Hardware cost money, the group's logic seemed to state, but software should be free. Gates, however, upset that his software had been distributed for free, penned the now-famous "Open Letter to Hobbyists." In his letter, Gates lamented the lack of "good software courses, books and software itself," and he attributed a $40,000 value to the time spent developing Altair BASIC. He wrote:

> The feedback we have gotten from the hundreds of people who say they are using BASIC has all been positive. Two surprising things are apparent, however. 1) Most of these "users" never bought BASIC (less than 10% of all Altair owners have bought BASIC), and 2) The amount of royalties we have received from sales to hobbyists makes the time spent of Altair BASIC worth less than $2 an hour.
>
> Why is this? As the majority of hobbyists must be aware, most of you steal your software. Hardware must be paid for, but software is something to share. Who cares if the people who worked on it get paid?
>
> Is this fair? One thing you don't do by stealing software is get back at MITS for some problem you may have had. MITS doesn't make money selling software. The royalty paid to us, the manual, the tape, and the overhead make it a

> break-even operation. One thing you do do is prevent good software from being written. Who can afford to do professional work for nothing? What hobbyist can put 3-man years into programming, finding all bugs, documenting his product and distribute for free? The fact is, no one besides us has invested a lot of money in hobby software. We have written 6800 BASIC, and we are writing 8080 APL and 6800 APL, but there is very little incentive to make this software available to hobbyists. Most directly, the thing you do is theft. (Gates)

The narrative of Gates' conflict with the hobbyist community is well-known, but I cite it at length because, as I read it, this moment is a key one within Levy's narrative and within the growth of commercial computing. In his letter, Gates draws firm lines between the rules and potential of professional/commercial software development and that of hobbyist development. Gates sees the relegation of computing to a hobbyist status as a problem connected to the lack of professional software and training. For the the influence of computing to develop, he implies, it must be professionalized; the amateur practices of collaboration stifle development: "One thing you [hobbyists] do do is prevent good software from being written."

As we know, Gates would move on to develop Microsoft Windows and have a profound influence on the growth of computing. Specifically, the move toward proprietary software—and the market dominance by companies like Microsoft, Apple, and Adobe—would push computing toward a direction of competition, not collaboration. And although there are many open source platforms and alternatives today, our computers and our classrooms often testify to the impact of Gates' vision and the growth of proprietary and commercial computing.

Although there has been much written about collaboration and open-source software, Richard Sennett offers one particularly compelling way to consider the relationship between the

hacker ethic and commercial software. Sennett, in his exploration of *craftsmanship*, argues that the production of Linux (an open source operating system) is "a public craft" (24). He writes that:

> When established in the 1990s, Linux sought to recover some of the adventure of the early days of computing in the 1970s. During these two decades, the software industry has morphed within its brief life into a few dominant firms, buying up or squeezing out smaller competitors. In the process, the monopolies seemed to churn out ever more mediocre work. (25)

Sennett sees the move toward closed systems of software as a step toward monopolies that function—and languish—in secret. Whereas an open source (and the pre-1970s) model of programming centers on the joy of both *problem finding* and *problem solving*, closed systems are lost in a maze of bureaucracies and procedures. Sennett extends his consideration to the collapse of the Soviet Union and the growth of capitalism, noting that this growth carried with it a narrative in which collectivism was flawed and competition was the primary means of increasing the quality of goods. "We need to look more deeply at this triumphalist view," he says, "because it obscures both the roles competition and cooperation actually play in getting good work done and, more largely, the virtues of craftsmanship" (32). Levy's narrative, or at least his hacker ethic, both speaks to and works in conflict with the relationship between competition and collectivism—as many of those first-generation hackers were the individuals who contributed to the growth of commercial and closed computing. Levy's narrative concludes with the shift from hackers to programmers, to the graphic interface-driven computer that obscures its inner workings. While, in 1984, the open source movement was beginning to gain a bit of traction, it

grew in the shadow of Apple and Windows and the world of proprietary and copyrighted software in which we now work.

Hacker Culture

Douglas Thomas (2002) offers a significant critique and expansion of Levy's narrative, situating hacking within a context of secrecy. Thomas reads hacking itself as a kind of technology, and he distances that technology from those typically associated with hacking—the phone, the computer, and the digital network. Instead, Thomas argues, "what hackers and the discourse about hackers reveal is that technology is primarily about mediating human relationships, and that process of mediation, since the end of World War II, has grown increasingly complex. Hacking, first and foremost, is about understanding (and exploiting) those relationships" (xxi).

Key to Thomas's reading is the elapsed time between his work and Levy's, a space (the 1980s and 90s) in which hacker culture—and the popular depiction of it—dramatically shifted. Thomas notes, for example, that the hackers of the 60s and 70s were inspired by the work of Isaac Asimov and Philip K. Dick, "writers who depicted a future of possibility, who wrote cautionary tales" (20). Hackers in the 90s, however, found inspiration in the work of writers like William Gibson, novelists who depict dystopias in which opportunity has been lost. "In part," Thomas writes, "this is the result of the increasing commodification of information, which has created a media that [hackers] describe as 'the propaganda vending machine of today,' which, 'as a whole, trip over themselves, feeding lies to the ignorant'" (23). Thomas also notes how, although the tone has shifted, 90s hackers still worked against the same thing as the 50s/60s hackers: Secrecy. When the first machines arrived at MIT, their inner workings were a secret to

be explored and exposed. By the 1990s, the cyberpunk-influenced hackers had extended that philosophy well beyond computers: "Curiosity is precisely what threatens secrecy, and in doing so, it challenges the economic structure, the commodification, of information" (23).

Perhaps the key takeaway of Thomas's reading is the recursive nature of hacking and secrecy. Secrecy is the counterpoint to the hacker ethic, the concept against which hacking reacts. The whole of modern computing, however, is born from the military-industrial complex and secrecy within government—specifically World War II code-breaking and subsequent advances in defense technology (13). For the early MIT hackers, secrecy was entirely decontextualized; Thomas notes that those hackers were either oblivious of or willfully ignorant about their role in the military-industrial complex (16). Secrecy was thus an abstraction, and credos like "information wants to be free" situated information as a contextless concept with a will. As the hacker ethic extended across decades, however, it became contextualized and embedded within cultural systems of commerce and power. Still, both of these hacker generations work within and against secrecy. And this project, as Thomas notes throughout his book, is paradoxical, as hackers work against secrecy but are also enabled by it. "Although hackers philosophically oppose secrecy," he writes, "they also self-consciously exploit it as their modus operandi, further complicating their ambivalent status in relation to technology and contemporary culture" (xxi). In Chapter Three, I will extend Thomas's assertion and position hackers as a *responsive public*. Hacking, I will argue, is always an act of responding—*hacking* requires an object *to hack*. As we look across years of hacker narratives, from Levy's MIT students to Thomas's cyberpunk-influenced factions to open-source software communities, we can consistently read hacking as a type of response.

Most compellingly, that act of response is often tangled with some sort of resistance.

The Rise of Phreaking: YIPL and TAP — The Youth International Party Line

In *Hackers*, Levy mentions how a young Steve Jobs and Steve Wozniak were, in 1971, inspired by an *Esquire* article about a phreaker named John Draper—better known by his phreaker handle of "Captain Crunch" (251). Draper had found that a toy whistle, included in boxes of Captain Crunch cereal, emitted a tone of 2600 hertz—the same tone used within the phone system to route long distance calls (254). An enterprising phreaker could then use that tone to place free calls and explore service areas of the phone system. Draper's discovery soon enabled the production of "blue boxes," small hobbyist devices that emitted the 2600hz tone. Jobs and Wozniak, as the story goes, built their own blue boxes and sold them on the Berkeley campus (251).

Blue boxing found popular attention courtesy of "Secrets of the Little Blue Box," Ron Rosenbaum's (October 1971) story in *Esquire* magazine[6]. Rosenbaum interviews several notable phone phreaks, detailing blue box usage and documenting the communities that emerged from phone system exploration. In one of the piece's most compelling moments, Rosenbaum speaks with Draper, who says:

> "I don't do that. I don't do that anymore at all. And if I do it, I do it for one reason and one reason only. I'm learning about a system. The phone company is a System. A computer is a System. Do you understand? If I do what I do, it is only to explore a System. Computers. Systems. That's my bag. The phone company is nothing but a computer." A tone of tightly restrained excitement enters the Captain's voice when he starts talking about Systems. He begins to pronounce

[6] Levy notes that this particular story is the one that inspired Jobs and Wozniak to build their own blue boxes (251).

> each syllable with the hushed deliberation of an obscene caller. “Ma Bell is a system I want to explore. It’s a beautiful system, you know, but Ma Bell screwed up. It’s terrible because Ma Bell is such a beautiful system, but she screwed up. I learned how she screwed up from a couple of blind kids who wanted me to build a device. A certain device. They said it could make free calls. I wasn’t interested in free calls. But when these blind kids told me I could make calls into a computer, my eyes lit up. I wanted to learn about computers. I wanted to learn about Ma Bell’s computers. So I built the little device. Only I built it wrong and Ma Bell found out. Ma Bell can detect things like that. Ma Bell knows. So I’m strictly out of it now. I don’t do it. Except for learning purposes.” (120-121)

In the ensuing decades, phone phreakers would often be labeled as, at best, mischievous youths trying to find ways to make free long distance calls, or, at worst, technologically-savvy deviants committing interstate fraud. Draper’s remarks, however, remind us both of the role of curiosity in phreaking and of the importance of the phone system as an antecedent to hobbyist computing and hacking. The phone system was a national network, and the early advances in switching technology found Bell Corporation at the center of technological innovation. Additionally, the phone system was a nation-spanning network connected to individual homes—but a network with specific and sanctioned types of uses. It seems fitting, then, that histories of hacking are firmly entwined with the exploration and manipulation of the phone system.

Additional articles about phreaking (for example, Maureen Orth’s 1971 *Los Angeles Times* piece “For Whom Ma Bell Tolls Not”) appeared in mainstream news venues throughout the early and mid-70s, driving hobbyist interest in blue boxing and phreaking culture. And just as phone phreaking began to gain mainstream notoriety, it also gained traction in underground

communities. In June of 1971, Abbie Hoffman and a phreaker named Al Bell produced the first issue of the *Youth International Party Line*, a Yippie-produced zine for phone phreakers. The Yippies, a loosely organized activist group formed by Hoffman in 1967, were especially concerned with media spectacle and disruption as ground for dissent—for example, Hoffman dropping money (from a balcony) onto the trading floor of the Stock Exchange or the group's attempts to use outlandish protest as a means of drawing television coverage away from the 1968 Democratic convention (Joselit 64). As Aniko Bodroghkozy notes:

> Under the charismatic, some would say clownish, leadership of Hoffman and Rubin, the Yippies became the most widely known figures associated with the youth movement of the late sixties and early seventies. They saw television as their conduit to a mass public. The medium, in turn, helped to make them both famous and infamous. Hoffman and Rubin became the first American radicals and left-wing revolutionaries to find themselves celebrities and household names—all through the magic of television. (99)

Given the group's interest in media manipulation as a means of social action (as well as Hoffman's anarchistic leanings), the June 1971 publication of *The Youth International Party Line* (YIPL) found the Yippies heavily invested in print culture and specifically targeting the Bell Company. The first issue (with its text shaped into a bell pattern) notes that 10,000 flyers were distributed, and that the promotion yielded 50 subscribers. "We may not have done well percentage-wise," the editorial states, "but the fact that there are 50 people all over the country willing to fight back speaks for itself." And if the Yippies were first focused on televised spectacle, *YIPL* initially expresses remorse—"The disappointment we feel toward Amerika has turned to hatred as we saw the the futility of the movement to improve it, and to frustration as

our outside efforts were repressed and forbidden"—and then turns to a very specific target: "YIPL will show you why something must be done immediately in regard, of course, to the improper control of the communication in this country by none other than the BELL TELEPHONE COMPANY." Noting specifics and advocating for education, the editorial continues:

> So if your friends want to get in on the fun, let them read your newsletter, and you might want to research your own questions in your local library, and help to start the education of your community of the phone company's part in the war against the poor, the non-white, the non-conformist, and in general, against the people. Show your neighbors, friends and the representatives of your area how the Bell System and the Amerikan government are co-conspirators. ("The Youth International Party Line's First Issue")

The contents of the first *YIPL* issue seem equally focused on technological concerns and activist/anarchist opportunities: A diagram explaining how to enable conference calling on a home phone, calling card codes, letters to the editor, and ways to opt out of the war tax. Many of these sections would continue to appear in future issues and in the zines that followed *YIPL*. But the latter section—the war tax exemption—might be the most unique and indicative of the moment at which *YIPL* was founded. The specific text reads:

> In April of 1966, as the government was escalating the Vietnam war, Congress passed a law raising the Federal tax on telephone service to 10%. "It is clear," said Rep. Wilbur Mills, Chairman of the House Ways and Means Committee, "that Vietnam and only the Vietnam operation makes this bill necessary." -Congressional Record, February 23, 1966. The War Tax Resistance is showing people how to

> refuse to pay this war tax. In most cases, the IRS will come to collect with 6% interest, but your phone service will continue. But the more it's done, the more it costs Them in time, trouble and embarrassment for Uncle Sham. Do it, and tell your friends, relatives, and neighbors to do the same. Include a letter to this effect to the phone company and your congressmen. ("War Tax Resistance")

Beneath the text is a clippable, brief letter to include with the war tax-deducted phone bill.

This connection between phreaking and the anti-war effort is important. If, as Thomas asserted, the MIT hackers were part of—but also unaware of their role—in the military-industrial complex, then the Yippie involvement in phreaking offers a reminder of how technologies are situated within political and economic moments. Whereas Captain Crunch asserted that he was only interested in the phone network as a System and a computer network, *YIPL* #1 underscored that system's connection to the war in Vietnam. And it seems fitting that the Yippies were there to make that connection, shifting some of their attention from the television to the telephone.

This focus would be sharpened in subsequent issues of the publication, as *YIPL*'s second issue, for example, described blue box diagrams and reprinted news articles about the phone company (a feature that, years later, would become a major part of *2600: The Hacker Quarterly*). In one news article reprinted in *YIPL* #2, "The Dumbest Rip-Off", Douglas Baker takes aim at Hoffman's *Steal This Book*, specifically the sections on exploiting pay phones. "I wonder if you [Hoffman] have really thought out the implications of the grand philosophical idea of destroying the telephone company," Baker writes, later adding that "destroying the telephone company would, in fact, be a severe blow to every member of the counter-culture" and asserting that the Bell Company is "the best of all possible telephone companies for the counter culture." Hoffman, in his response, notes that the Bell Company is the largest corporation in the world, asking Baker

to “Witness their central role in the military-industrial complex!” and to consider how Bell Service is inferior to that found in the free phone systems of other countries—“Until AT&T and the other corporations really become public services rather than power and profit gobblers, we’ll continue to rip them off every chance we get” (“The Dumbest Rip-Off”).

During the early *YIPL* run, the magazine would again and again return to this mantra: The Bell Company had turned a public system into a wealthy monopoly. In Issue #3’s “Statement of Purpose,” *YIPL* would deem itself as “a Public Service,” “a non-profit organization,” and an attempt “to bridge the communications gap generated by monopolies like THE BELL SYSTEM, and American mass media, too.” Though there were independent hobbyist publications and political/anti-war publications long before *YIPL*, the politics-via-telecommunications stance of the Yippie/Phreaker collaboration seems a galvanizing moment in the growth of hacking and technologically-situated dissent.

By its sixth issue (in November 1971) *YIPL* was boasting a circulation of 500+ readers, an increase likely connected to the publication of the *Esquire* piece. The magazine’s statement of purpose is revised in the sixth issue, this time moving more toward an index of knowledge and away from specific protest or dissent:

> Here we go again. The YIPL idea is limited if the research is left up to the staff. If our readers send in information that would be useful to other readers, and that means *any* information, related to phones, food, entertainment, transportation, or anything, then we would pretty soon have a centralized information pool that would be incredibly well-stocked with useful hints. (“Statement of Purpose”)

And once more in a note to new readers in issue twelve (August 1972):

> If you're a new reader, you might be wondering just what the hell this is all about. YIPL is an anti-profit organization dedicated to people's technology, and we publish information that shows you how to to fight back at the computers that run our lives. Every YIPL reader is encouraged to be a contributing editor, and to send us ideas for stories, information from the inside, and criticism of what we do or don't publish. We're taking a big risk so help us make it worthwhile. Get as many people to join as possible, and help spread the ideas you learn from YIPL. ("New Readers!")

The shift in stance and language is compelling, as the publication's exigence shifts from a battle with "The Bell Company" to "the computers than run our lives" and as the publication adopts more formalized language (publishing "stories" and viewing a readership as "contributing editors"). During this time the publication was also becoming more technical, publishing fewer pieces about culture jamming and more complex diagrams. Where the early issues of *YIPL* encouraged phone-based mischief (offering instructions on how to make a cement-like compound that could be used to jam the coin collection boxes in pay phones), the publication was, by 1973, focused mostly on wiring diagrams and instructions for building various boxes (as the blue box had been joined by the red box as the phreaker's tool of choice).

The observations offered in these first *YIPL* issues, as I read them, set the foundation for much of the political phreaking and hacking that would follow. The development of democracy and justice, the argument goes, relies on the free and open transmission of ideas and information. The First Amendment guarantees the freedom of speech, but what it doesn't say—and what its writers couldn't predict—is that the way in which those ideas are transmitted are just as important to the growth of a democracy as are the ideas themselves. So in 1971, in that first issue

of *YIPL*, Hoffman and the critics of the Bell Corporation saw the limiting powers of that monopoly. The then-largest communication system in the world was owned by one entity, and that entity had a tremendous amount of control over the ways in which ideas and information were transmitted across the country. By the 1970s, the nature of phone-based communication was mostly obscured, and the master switch, to borrow a term from Tim Wu, was firmly in the hands (and built to be so) of one corporation. The direction of *YIPL* and its successors was largely directed by that realization.

Technological American Party

The August/September 1973 issue of *YIPL* announced that Abbie Hoffman had been arrested for selling cocaine to government agents and that the D.A. hoped "to put Abbie away for life and make a spectacle of him" ("No Fancy Excuses"). The issue also announced a name change—to the Technological American Party—and noted that "we've been receiving so much information lately about gas and electric meters, locks, even chemistry, that a name change is definitely in order" ("No Fancy Excuses"). With Hoffman arrested, *YIPL* co-founder "Al Bell" began to push the publication in a less political and more technical direction. This change accelerated through the mid and late 1970s as the Vietnam War ended and the Yippies, like much of the anti-war culture of dissent, slowly lost focus and energy. *TAP* thus "became pitilessly jargonized and technical, in homage or parody to the Bell System's own technical documents, which *TAP* studied closely, gutted, and reproduced without permission" (Sterling 47).

Al Bell would leave *TAP* in the late 70s, and the publication duties were picked up by a phreaker with the pseudonym of Tom Edison. Edison continued to steer the publication in a more technical direction, and while the publication still focused on the phone company, it also veered

into areas like lockpicking, pirate radio, and drug production. And still, despite this more technical push, *TAP* retained some of its original anarchistic leanings, juxtaposing an article about cocaine production against an overview of cable descramblers and a rant about telephone networks. If the publication wasn't political in its editorial statements, its contents surely situated it within a certain political context.

Tom Edison would soon be joined by another phreak named the Cheshire Catalyst. The Catalyst met Tom Edison at a Discreet Mail and Phone Service center, a business that offered a sort of anonymous post office box service. *TAP* was, for many years, produced and managed within that space. When Al Bell was in charge of *TAP*, he had used campus computer resources to produce the mailing labels; a Word Processor was purchased when Edison took over. As the publication moved further from the Hoffman days (and from its politically organized origins), the details of its publication, at least as they were later narrated by Catalyst, became blurrier ("TAP: The Legend Is Dead").

In August of 1983 Edison's apartment was broken into and firebombed; the TAP computers and mailing lists had been stolen in the attack. Edison, seeing a connection between *TAP* and the bombing, left the publication. Cheshire kept *TAP* afloat for five more issues (until Spring 1984), after which *TAP* folded ("TAP: The Legend Is Dead").

In his 1987 reflection on publishing *TAP* (which is the source of much of the above information), Cheshire notes how many of *TAP*'s young readers would later make their way into the computer industry: "I recently attended a communications security conference in Washington, DC where a number of exhibitors were former subscribers to *TAP*, and in fact, had gotten into the business because they had so much fun as kids with tapping and bugging gear, that they had to get into the business to legitimize their interest" ("TAP: The Legend Is Dead").

Although the readers of *YIPL* and *TAP* were engaged in a much more subversive type of phreaking and hacking than Levy's MIT hackers, the same cycle exists: phreaker/hacker experimentation facilitates some sort of conduit into industry—which then creates the conditions for the next set of phreakers and hackers.

2600: The Hacker Quarterly

Founded in the (1984) wake of *TAP*'s closure, *2600: The Hacker Quarterly*, though not specifically connected to *TAP*, offered a degree of continuity in the lineage of hacker publications. *2600*, which is still in production, has been largely produced by "Emmanuel Goldstein" (whose real name is Eric Corley, but who, borrowing from Orwell, follows in the tradition of hacker/phreaker significant pseudonyms). As Sterling notes, Goldstein, while working at a college radio station, found his way into Yippie and *TAP* circles in the 1970s and would use that interest and experience to start *2600* in 1984 (63). Sterling specifically compares Goldstein to Abbie Hoffman, and that connection seems especially apt when comparing *2600* to *TAP*. Where *TAP* had shifted to a wholly technical focus, *2600* redirected its reading public to hacking's more political concerns: hacker arrests, run ins with the FBI, and critiques of the FCC.

Considering the publication's political stance, Sterling writes:

> The values in *2600* are generally expressed in terms that are ironic, sarcastic, paradoxical, or just downright confused. But there's no mistaking their radically anti-authoritarian tenor. *2600* holds that technical power and specialized knowledge, of any kind obtainable, belong by right in the hands of those individuals brave and bold enough to discover them—by whatever means necessary. Devices, laws, or systems that forbid access, and the free spread of

> knowledge, are provocations that any free and self-respecting hacker should relentlessly attack. The "privacy" of governments, corporations, and other soulless organizations should never be protected at the expense of liberty and free initiative of the individual techno-rat. (65)

2600 quickly shifted away from a zine-like appearance and appropriated the visual conventions of more typical publications, soon adopting a magazine-like form with glossy covers and increased page counts. Compared to *TAP*, early issues of *2600* appeared to have more consistent typesetting, discernible sections, readable print, and a masthead.

At several key points in *2600*'s history, the publication notes that it is *not* an underground publication or a zine—that it is a typical print publication concerned with technology. Although this might appear as posturing (especially considering the radical lineage from which *2600* grows), the we-are-mainstream stance rings throughout the publication's history and growth. If anything, *2600* seems to argue that it is no different from a traditional publication, and that it thus warrants the protections accorded to any print publication. In a savvy way, *2600* uses the (print-centric) freedom of press to create a space for conversations about telephony and technology—conversations that might be considered subversive. This is a calculated move, and it distances *2600* from *YIPL* and *TAP*. If, in the spirit of the radical 70s, *YIPL* and *TAP* considered themselves dissident publications and within the realm of government scrutiny, *2600* reasserts its legitimacy—and thus the legitimacy of dissent—by aiming for the largest possible print circulation.

Sterling also notes how *2600* used this positioning to build a space within technology conversations and amongst technological professionals:

> Sympathizers, many of them quite respectable people with responsible jobs, admire Goldstein's attitude and surreptitiously pass him information. An unknown but presumably large proportion of Goldstein's 2,000 plus readership are telco security personnel and police, who are forced to subscribe to *2600* to stay abreast of new developments in hacking. They thus find themselves *paying this guy's rent* while grinding their teeth in anguish, a situation that would have delighted Abbie Hoffman (one of Goldstein's few idols). (65)

If the Yippie focus was on media disruption, Goldstein channeled that energy into a technology-fueled media attraction. Although he's not engaging in the types of culture jamming that Hoffman endorsed, Goldstein has managed to gain the interest of technicians and security experts. In a sense, Hoffman's vision was of hijacking the stage; Goldstein, in producing *2600*, seems to have realized that there's much more power in exposing the rigging.

This isn't to say, however, that *2600* speaks for the whole of hacking or that it is loved throughout hacking publics. A major criticism of *2600*, for example, is that the publication is not —and has never been—free. Though *2600* draws mostly from reader contributions, it still charges for subscriptions (as did *YIPL* and *TAP*). Although all three of these hacker publications cite print production and distribution costs as the reason for subscription fees, *2600*—the longest running and most visible of the three—is sometimes criticized for taking a "free" information stance and then charging for access. Bulletin boards (in the 1980s), e-zines (in the 1990s), and webtexts (today) have all provided alternate means of accessing hacker-related texts—though without the large and engaged *2600* public. Additionally, *2600* has worked to extend its reach beyond just the publication, organizing monthly public meetings in many cities as well as a hacker conference, held biennially in New York.

Douglas Thomas, in *Hacker Culture*, notes that "*2600* has always reflected a particular social and political agenda for hackers" and that "*2600* reveals a great deal about the history and commitments of hackers and hacking" (120). Thomas, whose project focuses on the hacker underground, also writes that "[2600]'s political and social message, however, tells us relatively little about the underground world of hackers as a culture" (120). To be fair, *Hacker Culture* was published in 2002, and Thomas was writing at a time when hacking was still a largely underground enterprise. The hackers of the late-90s were hugely influenced by cyberpunk and dystopia, by narratives of underground and youth culture. Today, however, I would argue that much of hacking has become a mainstream endeavor, and that the political history and lineage of *2600* can tell us much about the current work of hackers and hacktivism—and the hacker's understanding of the tools of textual production.

Although I will address *2600*'s history through the specific cases found in Chapters Three and Four, I do want to briefly address what many would say is the most significant narrative in *2600*'s history: The prosecution of Kevin Mitnick. By the early 1980s, Mitnick was known as a skilled and notorious hacker: In 1979, he logged into the North American Air Defense Command computer in Colorado Springs; in 1981 he was charged with stealing documents from Pacific Telephone Company; in 1983 he was caught while attempting to break into computers at the University of Southern California; in 1987, after being convicted for breaking into a computer network and stealing software, he was sentenced to 36 months of probation; and in 1989, Mitnick was sentenced to a year in jail for hacking into private and government systems ("Hackers in Jail"). Mitnick, however, would not reach mainstream notoriety until 1995, when he was arrested after an alleged three-year manhunt. While still on parole from his (1989) arrest, Mitnick, in 1992, allegedly wiretapped the California Department of Motor Vehicles, a hack that

allowed him to gain FBI access codes (Thomas 198). Depending on the narrative, Mitnick then fled and became a fugitive (the government's story) or simply left town when his parole period ended (Mitnick's story). The three-year search for Mitnick ended with his 1995 arrest and a number of books and films inspired by the chase. Mitnick's case, however, didn't go to trial until 1999, meaning Mitnick was held in prison—some of his term in solitary confinement—for more than four years. And the case was full of oddities: Mitnick allegedly wasn't allowed to use a pay phone because of his phreaking history, and he wasn't allowed to use a computer to see the nearly ten gigabytes of evidence against him ("Message Sent"). The four years of Mitnick's pre-trial detention, however, mobilized *2600*, a time in which the publication organized a defense fund, printed and distributed "Free Kevin" bumper stickers, and published an article about Mitnick nearly every month. Mitnick's detention further shifted *2600*'s focus to issues of criminality, the perception of hacking, and civil liberties, and—until *2600*'s run-in with the MPAA (which I discuss in Chapter Four)—their advocacy work for Mitnick surely fueled the publication's late-90s growth.

That said, I chose to not use the Mitnick narrative as a case within the scope of this dissertation. There are many texts which explore Mitnick's arrest and detention (including those written by Mitnick himself), and while the case held *2600*'s focus for a number of years, I don't see the story as especially connected to issues of memory and delivery (beyond the connections found in most hacking activities). Mitnick's case tells us much about the prosecution of hackers, and Douglas Thomas, among others, has done much to further our understanding of this facet of hacking. The Mitnick case, however, isn't a major part of this dissertation. Instead, I've chosen to work through and address the other major narratives within *2600*—events which better illustrate the patterns of memory and delivery existing within a hacker public.

Hacker Publics

Phreakers and hackers were exploring and manipulating systems before and outside of *YIPL*, *TAP*, and *2600*, but the three publications (and others like them) have done much to organize phreaker/hacker knowledge and actions. The "party line" to which the *Youth International Party Line*'s title alludes was a means of connecting multiple telephone callers to the same line, and many phreaking activities have centered on those party lines, with phreakers hopping in and out of telephone nodes and group conversations. Phreaking was first a communal exercise, a means of exploring spaces and finding conversation. But beyond advocacy and activism, *YIPL* offered a way to share and archive that knowledge—building a phreaker public. This directly connects to Warner's understanding of a public, of how "the notion of a public enables a reflexivity in the circulation of texts among strangers who become, by virtue of their reflexively circulating discourse, a social entity" (11). This isn't to say that phreakers weren't a group or a force before *YIPL*, but it does suggest that the publication shifted the group—that it helped to develop a phreaker public and an awareness of that public. We can see this sense of publicness throughout *YIPL*'s early issues, in the way that the publication addresses a growing "membership" and "organization." That membership was hybrid (part phreaker and part Yippie) and loosely organized, but it shifted and focused phreaker attention.

Another compelling facet of all three publications (*YIPL*, *TAP*, and *2600*) is the way in which the publications are guided and managed by a few individuals (Abbie Hoffman, Al Bell, Tom Edison, Cheshire Catalyst, Emanuel Goldstein), but are entirely fueled by reader contributions. In many ways, each of these publications functions like an academic journal, with an editor steering a conversation built from reader contributions. Additionally, each publication

then becomes a record of that conversation and a sort of technological history, offering—from the first payphones to the first virus—a history of technology built from the reverse-engineering of that technology.

It is also in this way that the work of hacker texts can be best understood through de Certeau's *strategies* and *tactics*. As I addressed in Chapter One, phreaking and hacking are tactical activities, they seek and exploit the cracks and fractures within proprietary computing—from poorly coded software to poor password security practices. These attacks, however, are almost always temporary; the problems are patched or resolved and the crack is sealed. *YIPL*, *TAP*, and *2600* then act as a tactical archive, a collection of technological tactics but also a means of documenting networks as composed spaces. By building a history of faults and exploits within these systems of communications, hacker publications allow us to better see the relationship between technology and communication—as well as that relationship's impact on the distribution of texts. Although the fractures in technological strategies are quickly sealed, we have much to learn from a history of them. And such a history has much to tell us about our current moment, one in which civil liberties, communication technologies, and intellectual properties seems to be in a state of conflict. Although there is a great deal to be learned from the history of the master switch, there is just as much to be learned from tactical dissent, from the publics working in opposition to the Cycle.

A history of technologically networked communication—as told through a reading of *YIPL, TAP,* and *2600*—teaches us that power circulates, that it is distributed, and that culture moves through it (realizations that are by no means new). But what it also teaches us is that these systems of power are firmly entrenched in and reproduced by the tools of textual production.

2600's tactics offer another way of reading those technologies, of again seeing the importance of memory and delivery within our own work.

Chapter Three: Hacking and Memory

> "Memory is one of the five divisions of ancient and medieval rhetoric; it was regarded, moreover, by more than one writer on the subject as the 'noblest' of all these, the basis for the rest." (9)
>
> —Mary Carruthers, from *The Book of Memory*

> "*memoria*. From classical rhetoric, the fourth part or canon of rhetoric that concerns aiding the memorization of speeches. No longer much considered in modern rhetoric." (36)
>
> —Linda Woodson, from *A Handbook of Modern Rhetorical Terms*

> "Following in the intellectual tradition of Richard Young, who reinvented invention for the twentieth century, it is time for scholars to reinvent memory and delivery for the twenty-first." (175-176)
>
> —Winifred Horner, from "Reinventing Memory and Delivery"

In her Introduction to *The Book of Memory*, Mary Carruthers opens with an observation on the perceived differences between memory and imagination:

> When we think of our highest creative power, we think invariably of the imagination. "Great imagination, profound intuition," we say: this is is our highest accolade for intellectual achievement, even in the sciences. The memory, in contrast, is devoid of intellect: "just memorization," not "real thought" or "true learning." At best, for us, memory is a kind of photographic film, exposed (we

> imply) by an amateur and developed by a duffer, and so marred by scratches and "inaccurate" light-values. (1)

Memory, the often ignored rhetorical canon, sits (with delivery) to the side of invention, arrangement, and style, the canons that best reflect the allure of imagination and the facets of creative work most valued by contemporary culture. As Carruthers notes, memory is frequently seen as an outdated technology, a tool of oral culture which has little connection to modern rhetoric or to literacy. I find this position problematic, and in this chapter I will argue for the importance of a rhetorical understanding of memory, one that is grounded in both technology and in the cultural systems of textual organization. Although I won't yet focus on delivery (delivery, the other neglected canon, is the subject of the next chapter), it is important to note that I see *both* memory *and* delivery as major components of digital rhetoric. In short: The separation of the canons of invention, arrangement, and style from those of memory and delivery reveals a great deal about our perceptions of, understanding of, and assumptions about textual production and distribution. Technological innovations and corporate ownership in the nineteenth and twentieth centuries furthered the seeming irrelevance of memory and delivery, creating a space in which invention, arrangement, and style belonged to individual authors (or authors and their co-authors, their editors, etc.) and memory and delivery were then corporatized—the purviews of printing and distribution specialists, of marketing chains and bookstore shelves. This divide, of course, is false, but a very real perception of it has significantly impacted our understanding of textual production. Likewise, in a subsequent chapter I will argue that this rift in the canons has affected the way that we, as a field, discuss, teach, and produce texts.

In this chapter I will explore the role of memory in hacking and hacker narratives, specifically discussing how stories in *2600: The Hacker Quarterly*[7] demonstrate *practices* of memory. Through these practices, hackers use the assumptions of corporate memory to exploit gaps in our cultural/corporate perceptions of ownership and technology. In *2600*, this work happens through three specific activities: aggregating (collecting and reprinting information), fingerprinting (using mass collaboration to discover and archive information), and narrating (writing narrative explanations of technologies). These activities present memory as a tool, a pedagogy, and a practice, and they demonstrate how hackers use memory to find and exploit gaps in the assumptions posed by programmers and producers of technology.

Specifically, I begin with a brief examination of the conversation about memory in writing studies. I then extend that conversation by first positioning hackers as a *responsive public* and then describing how hackers respond to the privatization of technology through the above-mentioned three practices of memory. Finally, I illustrate and analyze those practices through specific examples from issues of *2600*. These practices of memory, I hope to demonstrate, allow us to examine the ways in which technology changes how we think and talk about the canon of memory.

Memory

Perhaps the most famous dismissal of memory comes from Edward Corbett's *Classical Rhetoric for the Modern Student*, a dismissal that exists in each of the book's four editions:

---

[7] *2600: The Hacker Quarterly* is this dissertation's primary text. First published in 1984, *2600* is a hacker-produced and distributed print magazine that now claims a readership of more than 50,000. Though not loved by all hackers, *2600* has been influential in hacker culture and in the public perception of hackers. This dissertation uses the *2600* archives as its primary data set.

> The fourth part of rhetoric was *memoria* (Greek, mneme), concerned with memorizing speeches. Of all the five parts of rhetoric, *memoria* was the one that received the least attention in the rhetoric books. The reason for the neglect of this aspect of rhetoric is probably that not much can be said, in a rhetorical way, about the process of memorizing; and after rhetoric came to be concerned mainly with written discourse, there was no further need to deal with memorizing. (22)

Corbett's dismissal is one that, with a few exceptions, extends across the history of our field and which is largely still in place today. Memory is, in many ways, the neglected canon, an element whose discard is often connected to the rise of written communication over that of the spoken. And despite attempts to revive and refashion delivery, memory mostly remains ignored and excluded from conversations and curriculum. I argue here, however, that this deprivileging of memory reveals much about the relationship between—and our perception of—text and technology.

Throughout the larger dismissal of memory, however, there have been moments and instances of focus. As early as 1969, in "McLuhan in the Light of Classical Rhetoric," Patrick Mahony wrote that "McLuhan's rhetorical orientation reveals a vital alliance between memory and pronunciation. In terms of videotapes, phonograph records, and indexed books, to go no further, memory or information storage has been exteriorized into new media or forms of pronunciation" (14). Mahony doesn't dwell on this notion, but there's a strong connection between McLuhan's reading of mass media and memory's relation to both print and new media. Similarly, Jay David Bolter writes that "the ancient art of memory was in fact another way of addressing the gap between writing and memory. It was an attempt to turn human memory into a technology like external writing" (109). The specific terms used by Mahony and Bolter

—"exteriorized" and "external"—are telling, rethinking memory as a movement beyond the internal. Considered in light of a classical reading (like Corbett's), this move makes sense. If the core of memory is indeed the memorization of speeches, and if that sort of memorization bears little connection to the contemporary study of textual rhetoric and literacy, then the externalization of memory presents a means for theoretical consideration. There is, however, a flaw in this assumption: That memory is solely an "internal" canon, that it is simply an isolated tool built of mnemonic devices and practice.

It is against this inert notion of memory that Carruthers, in *The Book of Memory*, seems to write. Asserting that medieval writers "would not, however, have understood our separation of 'memory' from 'learning'" and that, for them, memory "made knowledge into useful experience," (1), she presents the medieval conception of memory as much more than a tool or a set of exercises, and she notes that historians of rhetoric have sometimes separated memory and delivery from the other canons because of their appearance as "technical" parts of the subject: "This classification may well have contributed to the impression that *memoria*, being merely technical, was limited in its applicability to the conditions of oral debate, as was delivery" (13). This observation underscores Connors' perception of memory as an internal capacity of the rhetor or as a tool to be applied in service of other, more pressing, concerns.

But Carruthers also mentions memory as a cultural process, as something that extends well beyond the standard rhetorical consideration of the term, arguing that "*Memoria* also signifies the process by which a work of literature becomes institutionalized—internalized within the language and pedagogy of a group" (9), and it is here that I find one of the richest sites for the reconsideration of memory. In this sense we might think about types of "cultural memory," or perhaps the ways in which we sanction and organize knowledge. These technologies of

information organization and acquisition are themselves tools of memory, but they're generative tools: means of organizing, of comparing, of associating. This is memory beyond mnemonics.

Memory and New Media

It is in this sense of memory that Winifred Horner addresses the externalization of memory, but also fully pushes the external into a consideration of new media:

> But Plato could not have envisioned that human memories would be replaced by powerful external memories in books, libraries, and finally in the huge computer databases that can store the memory of a culture. With the first technology, history —the cultural memory—began, and memory in the limited internal sense was permanently altered. (180)

Although digital databases represent one way to rethink *memoria*, it is important to remember that this sort of collecting is not exclusive to computerized culture. Similar to digital databases, libraries (public, university, individual) are also representations of memory, both personal and cultural. As alluded to by Carruthers, *memoria* had a significant cultural function: it facilitated the acquisition and sanctioning of knowledge. When work was committed to memory, it acquired a degree of worth and influence on future work. It became part of the cultural and textual lattice that, after Bartholomae, we consider so crucial to the teaching of writing. Text archives, like libraries, function in a similar manner.

Likewise, a textual consideration of memory also affords a more recursive consideration of the canons, one that better reflects our contemporary understanding of writing processes. For example, as they're listed—invention, arrangement, style, memory, delivery—the rhetorical canons can reductively depict a highly linear process of composition. We know, however, that

writing doesn't necessarily function in this way, and that one canon often folds back upon another. So memory, when considered as a means of cultural/textual organization, has a profound influence on invention. The literature review, a touchstone of academic writing, is in this way a means of constructing memory, a genre convention that drives invention and frames an argument. And that literature review is built from other sites of memory: Academic journals, library shelves, and databases. Similar to the mnemonics of classical rhetoric, contemporary memory uses technologies—from library call numbers to saved database searches—in order to facilitate the ease of textual memorization and recall.

But if memory, in the era of new media, is more external, then a number of considerations follow. Horner writes:

> Today memory has become more external as we rely on the cultural memory outside of our own minds stored in books and more and more commonly on the internet. We refer to these electronic places as 'sites,' and they are often marked with images or icons. Rather than storing memories in our minds, we store them on internet sites enhanced with visual, auditory, and written images. Today we do not train our minds to remember but instead enhance our skills in retrieving and evaluating the huge storehouse of electronic memory. So the fourth office of rhetoric is revived today through the modern technology that is increasingly available to us. (179-180)

This contemporary "storehouse of electronic media" includes many types of digital archives, from formal paper-based databases like JSTOR and ERIC to social networking sites like Facebook and Twitter. Although these two types of sites represent different methods and motivations for archiving, they both reveal a specific kind of privatization and ownership of

memory that, if not unique to this moment, surely finds several types of *memoria* moving in a more commodified direction. In terms of academic databases, the argument is simple: Scholarship is often housed on private servers, behind paywalls and often with access limitations. The memory of an academic field, in these spaces, is privately owned, and access is institutionally limited—a process that then affects (or, perhaps, effects) the growth of a field and its ideas. In terms of social networking sites, however, the process is more complex and more fraught. Users are encouraged to archive a more common connotation of memory: photos, notes, and casual observations on day-to-day events. These individual "memories" are then tethered to a social system of memory, an archive that houses and weaves the personal memory into a larger network. And these spaces aren't necessarily new or unique: Users have been generating and storing their thoughts in digital spaces since the advent of the network. With the advancement of the Web, however, the memory-as-digital-artifact has become increasingly owned—and that ownership has been separated from the author. In the case of current social networking, content generated by the individual becomes the property of a corporate host, and the act of archiving isn't a move toward a cultural index but rather a means of keyword harvesting, of furthering an archival engine built to generate advertising revenue. This system, viewed from a hacker perspective, is one built on secrecy and one that relies on ignorance—a system that offers services to the end user but cloaks the technical and commercial underpinnings of that system.

Although I see the frame of internal memory shifting to external memory as a way to situate technology within the rhetorical canons, it is important to note that this movement does not imply that technology simply stands in for the cognitive practices or capacities implied by classical *memoria*. If anything, memory was never an isolated tool or set of exercises, but was always a component in a complex framework of rhetorical and cultural activity.

This is a point reinforced by Collin Brooke, who, in *Lingua Fracta*, notes that a view like Corbett's can "reduce memory instead to a question of storage, as if memory simply signified the retention or location of quantifiable amounts of information. It is in this sense that we speak of a computer's memory—its capacity for storing a finite number of kilo-, mega-, and gigabytes worth of information" (144). Brooke argues for a *practice* of memory rather than an understanding of memory based simply on retention. Again, memory extends beyond mere storage, functioning as a part of and within systems. But it is important to recognize the value of retention and how it functions in digital and cultural spaces.

Technologies of Retention

As many scholars have noted, Rhetoric and Writing, as a field of study, has traditionally focused on the generation of alphabetic texts and has only within the past twenty years made significant moves toward visual and multimodal composition. These practices, however, still privilege a view of technology that focuses on the products of graphical user interfaces. This is what Matthew Kirschenbaum calls (borrowing a term from Nick Montfort) *screen essentialism*, "the prevailing bias in new media studies toward display technologies that would have been unknown to most computer users before the mid—1970s" (31). Kirschenabaum sees a problem with "the current state of new media studies in which the graphical user interface is often uncritically accepted as the ground zero of the user's experience" (34), a bias which can be seen in the courses we teach and the topics on which we present at professional conferences. In short, our discipline is one built on a very specific and screen-centric type of digital output.

For Kirschenbaum, storage—not the screen—is the defining characteristic of new media. Kirschenbaum recalls the era of 5 1/4" floppy disks, media that had to be stored and inserted into

machines. For older machines, without significant internal storage, programs had to run from the disks. And in dealing with the disks, the user had a very real understanding of space and memory, of the very tangible constraints of limited storage capacities. However, as contemporary computing has moved away from removable media and more toward significant internal storage capacity and, more recently, cloud-based extensions of that storage, memory isn't something the average user has a regular experience with. "Since even routine chores like disk defragmentation are performed far less frequently on the current generation of hard drives," Kirschenbaum writes, "storage has become ever more of an abstraction, defined only by a volume letter (on most Windows machines, "C"), a graphic hard drive icon, or a pie chart visualization of space remaining. Greater and greater storage capacity will only serve to further dematerialize the media as their finite physical boundaries slip past the point of any practical concern" (34). In short, digital memory, while connected to more and more issues of data transfer/ownership and information privacy, is becoming increasingly transparent and of seeming inconsequence to the end user.

Thinking again about Brooke's argument of memory as a practice rather than simply retention, there is a compelling connection between the technological abstraction of memory and our use of that technology in the production of texts. If the deprivileging of memory begins with the move from orality to text, then the technologies of textual production have provided a means of privatizing and sanctioning specific methods of memory. By working through the impact of these technologies, we can gain a fuller understanding of their cultural influence—and how the abstraction of that influence creates an opportunity for (or a *kairos* of) subversion. Likewise, we can begin to create threads that link the technologies of retention to the practices of composition.

Privatized Memory and Responsive Publics

With the shift from orality to literacy and the ensuing deemphasis of memory and delivery, the burden of managing retention and distribution processes moved to private/commercial interests. Though this movement could be initially connected to technological scarcity (low rates of literacy or the rarity of printing presses), such technologies grew in prevalence throughout the twentieth century while the private ownership of retention and distribution strengthened. In many ways, the dismissal of memory and delivery reveals a modernist sentiment, one in which the author is responsible for the generative process of finding, styling, and arranging a message, while the transmission and retention of that text—seemingly inert and mechanical processes, lacking the creative weight of *generating* text—is outsourced to private, or at least non-author, interests.

But the transmission and retention of texts is a highly rhetorical process, one which bears significant influence on the final artifact. In terms of memory, the types of books published by a press—and the lineage of publication—affects the reception of a new text. Nuances in binding or page weight have a fundamental influence on memory (how durable is this artifact?)—on storage and retention. And if we consider the book (in its codex form) as a basic technology of retention, we should also consider core issues like cover design: How many authors select their own cover designs? In a world where memory and delivery are deemphasized, cover design is relegated to marketing concerns, an external billboard promoting the "real" content—the text inside.

And within this process, we see a gradual trend (from the twentieth century forward)—where the author faces a disconnection from the process of distributing and storing work—that extends into digital spaces, where nearly the entirety of the composition process hinges on hardware platforms and software applications that obscure the mechanisms operating beneath.

Perhaps the most obscured facet, however, is that of storage. And in the current moment of cloud computing, storage continues to be a growth industry—but an industry that obscures its mechanisms and implications, reducing file transfers and server space to sortable icons.

It is the opaqueness of this process that creates openings for hackers—and against which some hackers work. And it is here that I want to position hackers as a *responsive public*. I adapt this phrase from Christopher Kelty who, in *Two Bits: The Cultural Significance of Free Software*, introduces the concept of the recursive public:

> A recursive public is a public that is vitally concerned with the material and practical maintenance and modification of the technical, legal, practical, and conceptual means of its constituted power and is capable of speaking to existing forms of power through the production of actually existing free alternatives. (3)

Though hackers might qualify as a recursive public, I think that the term needs to be shifted. Although free software proponents, as Kelty writes, "focus on the radical technological modifiability of their own terms of existence" (3), hackers are constantly working *in response* to someone else's existence (or, more specifically, their technologies). Likewise, hackers don't necessarily qualify as a counterpublic, as they're not necessarily operating in opposition to a public (white hat hackers, for example, are often working with the producers of the technologies they're hacking). Hackers, however, are always working in response. The energies of early hackers—and their phreaking[8] counterparts—were focused on the nuances of early computers and the telephone system. Today, those energies have extended into a range of spaces: Networks,

---

[8] Phreaking is the act of hacking phone lines and systems. Phreakers found notoriety in the 1970s when "blue boxes," tools which allowed the user to make free pay phone calls, became popular in hobbyist, anarchist, and student communities.

databases, communication systems, and international correspondence. But hacking remains a responsive enterprise: The hacker requires an object to hack.

Similarly, a publication like *2600*—the product of a responsive public—also operates in response to technology. And *2600*, as I read it, is an enterprise of memory *as well as* an attempt to work against the privatization of memory. In particular, I see a practice of memory represented in three important activities across the history of *2600* (and its predecessors):

- *Aggregating*: At its core, *2600* seems an attempt to build a print database of knowledge—from bits of discarded manuals to schematics for telephone systems to relevant news stories. This isn't original knowledge (as engineers, programmers, or technicians might already have easy access to this material), but it is knowledge that is often hidden from the end-user. The process of aggregation is one that collects and redistributes this information.
- *Fingerprinting*: Well before "crowdsourcing" was a buzzword, *2600* asked its readers to explore something—their local phone exchange or university network—and submit that information. In collecting this data, *2600* offered maps of early networks. Again, this wasn't "unique" information; it is likely that this information existed elsewhere. However, *2600* worked to collect and then widely distribute this information, challenging those who might hide or obscure it (regardless of reason).
- *Narrating/Teaching*: Finally, a core component of *2600* is the explication of technical documents and details. This might include something like a line-by-line narration of virus code. Although this moves beyond simple archiving and into a more hermeneutic space, it also extends into the *practice* of memory—of not just storing technical

> documents or details, but also of situating, explaining, and interrogating the artifact, of making the work of storage meaningful.

Again, the work of hacking is *responsive*, and each of these practices finds hackers responding to a particular technology. Beyond that, however, they are also responding to cultural practices of storage—especially those that obscure the mechanisms of retention from the end user.

In the following section, I will situate each of these three practices—aggregation, fingerprinting, and narration—within the archives of hacker publications. Through this demonstration, I hope to display how hacking hinges on our cultural practices of memory—how the work of the hacker highlights (and often exploits) the fissures within those practices.

Aggregating: Data Collection and Discourse

The first issue of *2600*, dated January 1984, opens with the publication's exigence:

> The idea for *2600* was born early in 1983. We saw a tremendous need for some form of communication between those who truly appreciate the concept of communication: technological enthusiasts. Of course, others have different ways of describing such people—these range from words like hacker or phreaker to stronger terms such as criminal or anarchist. Our purpose is not to pass judgment. *2600* exists to provide information and ideas to individuals who live for both. **All of the items contained on these pages are provided for informational purposes only. *2600* assumes no responsibility for any uses which this information may be put to.** (emphasis theirs) ("Ahoy")

The central focus—to provide information and ideas—is one that remains with the publication today. The way in which that information is provided, however, seems somewhat unique to *2600*

(and to the work of hackers in general). For example, FLASH, a column which ran through the publication's early years, collected and reprinted news stories that focused on technology or communication issues: reprints of stories like "Wiretap City" (*New York Times*), "Teller Machine Crime Coming" (*The Los Angeles Times*), and "Long Distance Option Timetable" (*USA Today*) all appeared in *2600*'s initial issues. Likewise, a wealth of paper material was collected and redistributed in *2600*'s early issues: The phone extensions of government officials, correspondence from phone companies, diagrams of early networks (reprinted from places like Harvard's *Information Technology Newsletter*) and much, much more. From the publication's first issues, it is clear that *2600* viewed the aggregation and (re)distribution of technology-related documents as a central concern. It is also clear that *2600* was initially viewed as publication to be archived, much like a collection of print technical documents: "The three holes on each page serve a purpose," the first issue's editorial note also states, "We suggest that you obtain a loose-leaf book so that you can neatly file every issue of *2600* you receive" ("Ahoy") (When the publication changed formats in 1987 it also did away with the three hole motif, which caused many concerns, as voiced by readers in the letters section.) Although many print publications, especially magazines, seem ephemeral, it is clear that *2600* was meant to be archived, much like the technical documents on which it focused.

Many of the materials published by *2600* were reprinted from notable electronic bulletin board systems (BBSs). In the mid-to-late eighties, however, as many of those BBSs (including *2600*'s own) were seized by the FBI under suspicion of credit card number theft, the impetus to archive technical details and data in print form grew. For example, in the June 1984 issue, under a FLASH article (from "2600 News Service") titled "2600 Writer Indicted," the magazine notes that one of their writers "has been charged with wire fraud in connection with the GTE Telemail

investigation," After stating that *2600* is not the product of an individual, but rather of many people, they write: "We are not an 'underground' magazine; we don't break laws or publish items that are illegal to publish. We simply discuss interesting things that can be done with today's technology. There is certainly no reason for us to go underground." Though *2600* has since been sued (in some notable cases) over materials published, this is a stance it continues to maintain. I will more specifically address this concern in Chapter Five, but this act of publishing documents —and the insistence that it is legal, ethical, and protected by free speech—is a position and lineage that extends to sites like Wikileaks today.

2600's early issues, in the process of aggregating and archiving, also brought the work of "trashing" to the hacker/phreaker forefront. In "Some Thoughts on 'Garbage Picking,'" a hacker documents the kinds of garbage that yield information: "Many a tale has been told on the local bulletin boards about the enterprising phone phreaks who snuck around to their local phone company's central office early one morning and snooped through the dumpsters," finding "wires, relays, and other bits and pieces that an electronics hobbyist would enjoy." The author explains:

> Hackers on time-sharing systems are long familiar with the technique of asking the operating system for some memory or mass storage space that has not been zeroed out, and then dumping whatever was in there to the screen or printer. Things like password files and system programs are always updated or backed up from time to time, and that's when a "garbage copy" will be created. The alert hacker will find this if he or she looks hard enough. ("Some Thoughts on Garbage Picking")

Within this article, the blurring of electronic and physical space stands out. There are numerous instances of the garbage metaphor in computing, and it is in this garbage that the hacker finds

valuable system information—challenging a system (and perhaps cultural) assumption that an item disposed of is, well, actually disposed.

The process of exploring actual dumpsters for technical documents—called "trashing"—becomes a topic of note, especially in *2600*'s early issues. For example, in September 1984, *2600* published "More on Trashing: What to look for, how to act, where to go," an overview of the subject and how best to go about it:

> An inspection of your local Telco office trash receptacles can reveal a wealth of documents of great interest to a telecommunications hobbyist. The fone company doesn't expect anyone except maybe bums to paw through their refuse, and therefore often disposes some interesting materials. In all the installations we have investigated, the Company doesn't shred or incinerate anything. Most sites have their garbage in trash bags convenient for removal and leisurely inspection at home. ("More on Trashing")

The article proceeds to describe best trashing practices, including how to act (posing as boy scouts so that, in the event of a run-in with phone company security, a young hacker could say that they are trying to clean up a public area in hopes of getting a merit badge) and what to look for ("maintenance reports, trunk outage reports, line reports"). Additional trashing articles emerged at this point, each with a focus on finding manuals, binders, or other documents related to the phone company. These documents were then scoured for helpful information, xeroxed, and distributed via bulletin boards and publications like *2600*. In "Trashing: America's Source for Information," (October 1986) a hacker writes:

> I very quickly figured out where some local phone phreaks were getting their material. They crawl into the garbage bins and remove selected items that are of

> particular interest to them and their fellow phreaks. One phone phreak in the Los Angeles area has salvaged the complete 1972 edition of "Bell System Practices." It is so large and was out of order (the binders had been removed) that it took him over a year to sort it out and create enough shelving for it in his garage.
>
> Much of this "Top Secret" information is so secret that most phone companies have no idea what is in their files. They have their hands full simply replacing everything each time a change in wording requires a new revision. It seems they waste more paper than they can read! ("Trashing: America's Source")

This search for "top secret" information continued through the late 1980s and early 1990s, where trashing was a significant theme (and source of information) in *2600*.

Trashing and Social Engineering

In *Hacker Culture* (2002) Douglas Thomas directly connects trashing to the process of social engineering: "Social engineering is nothing more than using social skills to get people to tell the hacker things about system security. It is part research, part conversation, and part hunting through garbage" (61-62). Indeed, many of the letters and personal narratives published in *2600* speak specifically to social engineering: stories of befriending phone operators, of posing as a student or hobbyist group in order to get a tour of phone company facilities, and of acting as an engineer in order to get access to technical information or service/troubleshooting systems. In *Hacker Culture*, however, Thomas posits a few problematic assertions about social engineering, writing that "the process of social engineering is solely about exploiting the mistrust or uncertainty that many people have about technology," that "The premise of social engineering is based completely on the notion of authority," and that "social engineering exploits the fact that

the weakest point in any system's security is the people who use it" (62). When Thomas adopts the computer security mantra that users are the weakest point of any system (a sort of contemporary computing truism that many system/network administrators will agree with), this kind of assertion paints the computer "system" as a self-sufficient entity, a solid and predictable mechanical construct divorced from the assumptions and biases of its programmers. Likewise, it removes the programmer—and the commercial entity that employs the programmer—from the equation, rendering the programmer's view of technology only as a prescribed relationship between the machine and the end user. In this view, the hacker uses social engineering to exploit the weak parts of that relationship, conning support technicians into thinking that the hacker is a hapless newbie (who, in the process of a support call, might then get access to privileged information) or an experienced engineer in the field (who needs immediate access to a privileged piece of information). "What [this technique] demonstrates," Thomas writes, "is the manner in which technology is about the ways in which human relationships are mediated" (62).

Thomas's definition of technology as mediating relationships is a core premise of his book and central to his understanding of hacker culture. I would, however, extend that definition into the space of cultural assumptions about—and the privatization of—technology. If anything, a reading of *2600*'s early issues reveals that hacker social engineering goes well beyond the relationship between the end user and technology—also exploiting the assumptions of the individuals and organizations developing that technology. When hackers and phreakers jump into a dumpster and retrieve (and then reprint) documents, they are exploiting a corporate misunderstanding of memory: That trashed documents are no longer part of a technological system of knowledge. Yes, from the perspective of the person disposing of these documents, they

are indeed inert and no longer part of that knowledge system. The hacker, however, in response, works against (and through) those assumptions about inert material and perceived "waste."

And it is in this sense that the connection first made in *2600*'s "Some Thoughts on 'Garbage Picking'" seems especially profound. These cultural assumptions and perceptions of memory—that discarded materials are no longer indexed and no longer part of the knowledge system—extend well into computing metaphors. When a computer application trashes information, it assumes that said information is no longer relevant, that it is no longer indexed, and thus no longer part of the memory system. In reality, however, that information often remains part of the computing system, just not indexed and easily accessible to the user. (It should be no surprise that modern operating systems employ the metaphor of the waste can or recycle bin: Information is moved there for final contemplation before the user "empties" the device and assumes that its contents are destroyed—just like physical dumpsters.) The hacker, however, works through and against this assumption—knowing that digital data often remains in the system and isn't truly destroyed—reclaiming it, indexing it, and, in the case of *2600*, adding it to a new system of memory. Although this isn't social engineering in the traditional sense, I would argue that it functions in the same manner: Hackers learn about and manipulate systems by exploiting the assumptions of those who program the systems.

Fingerprinting: Collective Experimentation

In *Wikinomics: How Mass Collaboration Changes Everything*, Don Tapscott and Anthony Williams extoll the virtues of the new "Age of Participation":

> Call them the "weapons of mass collaboration." New low-cost collaborative infrastructures —from free Internet telephony to open source software to global

> outsourcing platforms—allow thousands upon thousands of individuals and small producers to cocreate products, access markets, and delight customers in ways that only large corporations could manage in the past. (11)

Though the "Age of Participation" could very well be an apt moniker for the current moment, it is important to note that this type of collaborative knowledge work and data collection occurred well before the widespread adoption of the Internet. In *Hackers*, amidst his discussion of the Tech Model Railroad Club (TMRC), MIT's first hacker collective, Steven Levy, in something of an aside, mentions how the group had a brief interest in the MIT phone system. "The Model Railroad Club," he writes, "would often go on tours of phone company exchanges, much in the way that people with an interest in painting might tour a museum. Kotok [a student in the club] found it interesting that at the phone company, which had gotten so big in its decades of development, only a few of the engineers had a broad knowledge of the interrelations within that system" (40). Levy is writing of the summer of 1961, well before the organization of formal "phreaking" communities, but the observation is an important one. In the 60s and 70s, the phone system was something of a marvel—but also a significant mystery—and thus presented numerous opportunities for technological exploration. Likewise, the phone system, more than the communication networks before it, seemed like a highly personal network, connecting a piece of household technology to other household units via a system of wires and mysterious exchanges. Levy writes that the TMRC spent the winter of 1960-61 trying to fingerprint the closed MIT phone system, attempting to make a map and track the variations in access codes. And as Levy asserts, the group wasn't trying to exploit the system or find a way to make free calls; the MIT exploration was fueled only by curiosity and the hacker ethic of free information.

This act of "fingerprinting" is a practice that occurs in hacker/phreaker communities from the 1960s forward, most specifically in relation to early computer networks and to phone systems. By the time that *2600* arrived (1984), there was a significant amount of phreaker information available—schematics, phone number trees, service extensions—but *2600* soon began to make explicit calls for this information by offering readers a group of phone numbers, for example, and then asking readers to explore those numbers and report their findings. This act of fingerprinting quickly showed up in feature articles like "A Trip to England" (August 1986) which began with an editorial notice: "The following article comes to us from a writer who is spending some time in the United Kingdom. We welcome future contributions from other writers in other countries. Please contact us if you have something to offer." The content of the article (and those like it) is especially interesting, listing phone numbers that range from the obvious and easily accessible ("999 Emergencies-fire, police, ambulance, cave rescue, coast guard, and mountain rescue") to very specific and likely unknown extensions and features ("175 Line fault test-Dial 175 then your last four digits, let it ring, you will hear something, hang up. Your phone will ring, answer it, and then dial 9. A list of diagnostics will be read off to you by a computer."). Similarly, as the *2600* letters section began to grow, so did the number and range of reader contributions, many of which would offer a small piece of information and encourage others to explore. An example (from a letter by Mr. Upsetter, Summer 1990):

> An often overlooked place for telephone experimenters to poke around is the 811 prefix (in California). This prefix, which is used by the BOCs, holds more than the local billing office number. From my Pacific Bell location in California I have found telco office numbers, test numbers, computers, and other things I haven't figured out yet. Here's a sampling: 811-0317: "Testing 1234" recording;

> 811-0428: Pac bell retiree services; [author goes on to include many other numbers and their functions]. If you have the patience, scan all numbers in the prefix. You may want to scan during non-business hours because lots of the numbers use answering machines. These machines often identify what the number is used for. All calls to the 811 prefix are free, and many numbers are dialable from throughout the state. Happy hunting. ("Free Phone Calls")

The prevalence of these letters is staggering, and a chronological reading of them renders a history of consumer technology from the rotary phone to the fax machine, from the first cellular devices to Web-based social networking. In turn, these articles and letters show a resistance to sanctioned uses of technologies and corporate perceptions of consumer information. Consider, for example, the materials that might be offered to a typical phone customer in the early 1990s: The phone itself, a manual for using that phone, and a phone book with local numbers. Within these documents is a prescribed use for that technology (to place voice calls) and the geographic constraints of that prescription (mostly, a local area). By fingerprinting the network, hackers extend that prescribed knowledge and, in turn, challenge the boundaries of appropriate usage. They also build a new *memoria* artifact, a collection of print pages that documents many now-extinct service lines and extensions, building a history of service extensions, voice mail providers, and technical frequencies.

And much like Wikipedia challenged the concept of the encyclopedia as a source of sanctioned memory, hackers collected and published information that challenged the constraints of typical consumer knowledge. They weren't necessarily generating "new" knowledge, but were rather unearthing hidden information, stealing snapshots of the gears driving consumer devices

and their networks.

Narrating: Writing New Technologies

Though narration seemed to be a more visible component of *2600* in the late '90s and 2000s (as the publication turned its focus more toward computer networks than to phone systems), we can still see narrated articles in some of the earliest issues. This act of narration frequently occurs in the form of a walkthrough—most notably of computer code that is explained and annotated. For example, with the rise of the first major computer worms/viruses in the late '80s, *2600* ran a series of features in which code would be printed and explained—both that of the virus and of virus scanning software. And the growth of the Internet found *2600* publishing walkthroughs on topics like the use of UNIX and the process of tracking network activity. Recent articles have focused on topics like email spam, wifi networking scanning, and dedicated videoconferencing units, presenting readers with relevant snippets of computer code and then explaining that use of code to the reader.

And it is within these walkthroughs that I see one of the major enterprises of contemporary hacking. If aggregation and fingerprinting are two means of acquiring information, then narration is the tool that clarifies the information and situates it in actionable terms for the reader. There's a practice of memory for those who initially retrieve and distribute the documents, but there's also a practice in reading them—of working through both the text and its annotations.

This distribution and annotation of code also speaks back to the MIT Model Railroad Club and their system of circulating computer code. As Levy describes them in *Hackers*, the Tech Model Railroad Club was working with early card-driven computers, and the act of

programming was a fundamentally social enterprise. The group kept their active projects in a communal drawer, and there was a standing challenge to improve (or to "hack") an active project. In fact, the subtle changes in code, which in turn led to the further understanding of new machines, was the central value of the hacker ethic. This represents two kinds of memory: First, because the cards were the means of storing the programs (something of an equivalent to today's internal memory), they acted as the simplest sort of memory—the technology of retention. But that technology was also the foundation of a programming process, a piece of knowledge that passed from person to person. Likewise, with each variation in the programs, the club began to understand a bit more about the machines: creating games, manipulating the sensor lights, etc. These earliest moments of collaborative computer programming were centered on memory as a technology of retention and exploration.

Although we might not think of those early programs as rhetorical artifacts or parts of a rhetorical process, we can see shifts in that direction across the growth of the computer industry. Levy documents how the hacker ethic spread to the 1970's west coast homebrew computing culture, generating energy in hobbyists. In 1975, however, a young Bill Gates would write a version of the BASIC programming language for the Altair home computer—a piece of software that he and Paul Allen planned to charge money for. Borrowing from the hacker ethic, however, another hobbyist found an early copy of the software and duplicated it. "Why should there be a barrier of ownership," Levy writes from that user's perspective, "standing between a hacker and a tool to explore, improve, and build systems?" (232). The free distribution of the software drew Gates' ire, and he quickly condemned the hobbyist community, claiming that this sort of distribution would hinder, among other things, the ability to generate jobs in computing. Within this moment in Levy's narrative, a split begins to build: One that pits the rise of commercial

computing against its community-driven roots. A familiar tale. But this is also the point from which compelling trends arise: From the perspective of commercial software, code—the underpinnings of digital text—is a trade secret. The Microsoft Windows kernel, Google's search algorithm, Apple's phone interface—these are all proprietary properties driving many of our daily interactions with technology. The protection of these technologies is mired within massive cultural structures (not the least of which include the free enterprise system and copyright/patent laws), but it also reflects the worst parts of screen essentialism: the features with which the user visibly interacts are paramount, and the mechanisms behind that interaction aren't to be manipulated or distributed. If we consider these technologies for productive communication, they freeze the user at the level of style. The Microsoft Word document is a key example of this: The user becomes locked into a specific file format whose core structure (the technology fueling the screen artifact) remains hidden.

So by both distributing and narrating computer code, hackers are challenging the assumption that code (or other technologies) is simply a proprietary formula fueling the workings of the screen, something of little use to the end user. Instead, they're exploiting the holes in that assumption to gain access to the code and to then explain that system to the reader. These assumptions are far reaching; they're the reason, for example, that so many early *2600* articles focused on exploits enabled by simple default passwords (like "password") that were built into the system. Though these exploits offered easy access to the entire system, they were (due to the hidden code) often unknown to the end user whose data was at risk. A cultural turn away from memory and delivery—a turn that in effect says *how the system works isn't important or of use to you, what matters to you is that it works*—abstracted these concepts and argued that an artifact like proprietary code isn't something to be stored, archived, or distributed. The hacker

disagrees and asserts that the assumptions within this code compromise the end user's experience and data. And a primary means of challenging these assumptions lies within the canons they ignore: storing, reproducing, and distributing the texts.

It is difficult, however, to speak of memory without also considering the importance of delivery. In the next chapter, I will examine the role of delivery within hacking, specifically turning my analysis to the importance of a print publication that is a product of a decidedly electronic (and technically savvy) public.

Chapter Four: Hacking and Delivery

> "In fact, I would dare say that most of the research published in the journals *Kairos* and *Computers and Composition* is related moreso to the canon of delivery than to any of the other canons—although scholars in that field seldom label their work as 'delivery.'" (211)
>
> —Jim Porter, from "Recovering Delivery for Digital Rhetoric"

> *"*...the fifth canon, it can be maintained, is now the most powerful canon of the five." (n.p.)
>
> —Kathleen Welch, from "Electrifying Classical Rhetoric"

I think it is fair to assert that, until the early 1990s, delivery was, as Kathleen Welch (1990) wrote, "the function of rhetoric most frequently (one could say most avidly) ignored by writing instructors and their institutions." At that time, a conventional view of delivery, like that of memory, tethered the canon to orality, to the nuances of transmitting a message. With the advent of print, it seemed, delivery was immaterial.

We now, of course, know better. Delivery is wound into much of our communication, from text messages to emails, from downloaded PDFs to streaming video. And our software constantly reminds of us this, making a *whooosh* sound when an email is sent or blinking the word "buffering" while a video loads. If we lost delivery with print, the digital certainly seems set on reminding us that delivery is a fundamental concern of composition.

In this chapter, I argue that the increasing commercialization of delivery has obscured the mechanisms of distribution from the end user. In turn, many hacker activities are an attempt to expose those mechanisms—to show how the technologies of delivery function. This hacker activity often falls under government scrutiny or the threat of litigation, but I think it carries profound implications for the ways we think through and talk about the work of delivery.

For example, we would consider it outrageous to use a piece of software that would take a group of sentences and arrange them in a proprietary, algorithmically-determined optimal order. We would reject this sort of tool because because we know that the work of arranging and organizing a text is a crucial part of composing. And yet we outsource delivery in just this way, passing our texts to companies and technologies whose ins and outs are frequently obscured. From the first throes of rhetorical thought, rhetoricians have acknowledged that audience awareness is of paramount importance, and the first rhetors were thus concerned with the (then embodied) transmission of language to an audience. The commercialization of delivery, however, has limited the rhetor's/author's control of that transmission, selling the perceived simplification of delivery as a benefit. The emergence and growth of hacking, then, is a response to and a dismantling of this habit—exposing the technologies and assumptions that drive our systems of delivery and reminding us that delivery isn't automatic or automated.

In what follows, I attempt to situate hacking in relation to (and, perhaps, in opposition to) the growth and commercialization of delivery. I begin with a brief look at the role of delivery in Composition and Rhetoric scholarship, contextualizing my argument within the reclamation of rhetorical delivery and its relationship to the production of text. Next, I place hacking within Jim Porter's *techne* of digital delivery, using Porter's *koinoi topoi* of digital delivery as a frame for working through the relationship between hacking and the transmission of texts. Porter's *techne*,

I argue, offers a way to read contemporary hacking as a specific response to the commercialization of delivery rather than a response to commercialized technology. I then offer three specific narratives from the pages of *2600: The Hacker Quarterly* as a means of working through this heuristic. Each of these three narratives tells us something about the relationships between the commercial entities delivering text and data, the government that regulates that transmission, and the hackers that operate somewhere in the spaces between.

Linked together and historicized, however, these narratives offer a picture of the shifting landscape of delivery and the increasing ways in which that space is regulated and owned. This regulation and ownership connects to many of the major discussions about digital spaces: concerns of possession and piracy, of the economic viability of art, and the role of communication industries in digital spaces. More importantly, however, these tensions connect to a deeper concern—that of textual transmission and its relationship to a functioning democracy. And the current moment of hacking and hacktivism seems centered on the shrinking public sphere and the encroachment of private, commercial interests on both the mainstream news apparatus and on the larger political sphere. This chapter works toward a consideration of hackers and the technologies of delivery to facilitate, in the final chapter, an analysis of the implications of privatized delivery systems on democracy and the digital commons.

Delivering Text

During the past two decades of Composition and Rhetoric scholarship, there has been an increase in the considerations of delivery—the arc of which says much about how new technologies have shifted our thoughts on composing. Bob Connors, for example, in 1993 wrote that "The canon of delivery has to do simply with the manner in which the material is delivered.

In written discourse, this means only one thing: the format and conventions of the final written product as it reaches the hands of the reader" (65). Connors, writing in a pre-Web space, reminds us of the once-dominant understanding of textual transmission, situating delivery firmly within the constraints of the printed page. "Like speakers," Connors writes, "who are scrutinized as soon as they walk out on the platform, writers are being sized up as soon as their manuscripts fall from a manila envelope or are pulled from a pile" (76). Although Connors is correct in asserting that formatting concerns have an impact on the reception of a text, his assessment speaks to a time (his essay was first published in 1983) when delivery was simply seen as the form in which a text arrived.

By the late 1990s, however, this form-centric understanding of delivery was in question. For example, Kathleen Welch, in *Electric Rhetoric* (1999), argued that the deprivileging of memory and delivery connected to current-traditional writing instruction and to formalist/ traditionalist literary paradigms—both of which treat language as an object outside of ideology (145). In this manner, language and the technologies of textual distribution become simple tools, a metaphor that Welch says we need to discard. Welch also notes that the loss of memory and delivery was no accident—what she calls "ideological suppression" (143)—and sees an ideologically-centered understanding of text and the canons as operating in opposition to expressivist and cognitivist modes of writing instruction. "Digital literacy for any group does and will include reconfigurations of the canons of memory and delivery," she writes, adding that "perhaps the recognition of all five canons and the definitive twentieth-century erasure of memory and delivery will lead to the obliteration of the current-traditional paradigm and its twin the false binary opposition of content and form" (147).

John Trimbur (2000) connects the deprivileging of delivery to the relationship between teachers and texts, arguing that "neglecting delivery has led writing teachers to equate the activity of composing with writing itself and to miss altogether the complex delivery systems through which writing circulates" (189-190). Trimbur's article begins with an observation about the closure of a campus computer lab and its impact on a deadline for his class. Although that technological problem initially seems like a traditional excuse for late work, it is actually a reminder of the complex systems of delivery at work in writing. "To say," Trimbur writes, "as I have, 'I just want the paper,' suggests that the student's words alone are what count and to identify writing with the creative moment of composing, thereby isolating an education in writing from the means of production and delivery" (189). As Trimbur sees it, writing instruction has typically privileged the closed system of exchange between instructor and student, creating an understanding of writing that begins and ends with the production of text. In challenging this pattern, Trimbur pushes toward a more socially situated concept of delivery, one that "*must* be seen as inseparable from the circulation of writing and the widening diffusion of socially useful knowledge" (191).

Both Trimbur and Welch respond to limited notions of current traditional pedagogies that isolate the writer and place her outside of textual networks and cultures. In the eleven years since the publication of Trimbur's and Welch's work, digital delivery has reinforced the importance of the canon both in writing studies *and* in the cultural distribution of digital artifacts. In many ways, the highly political structures of delivery seem today more visible—or at least easier to highlight. DeVoss and Porter (2006) illustrate this connection by relating writing to peer-to-peer software, using filesharing as an example of "a crisis in *delivery*" that "has fundamentally changed the national landscape regarding the digital distribution—and thus the delivery—of

documents" (179). By arguing for a focus on delivery in the study of writing—what they call the "economies of writing" (184)—DeVoss and Porter are able to consider digital distribution and the politics thereof.

We can consider their argument by moving beyond alphabetic text and toward the exchange of digital artifacts. Although digital filesharing is often discussed in terms of ethics or legality, the practice actually represents the moment at which consumers left the culturally sanctioned spaces of exchange. Before Napster[9], recorded music was typically transmitted through broadcast or artifacts (8-tracks, LPs, CDs), and to be a sanctioned distributor of music one needed access to a supply chain and a means of distributing that supply (a storefront or radio tower). While there have always been transactions occurring outside of that chain, the duplicates and bootlegs of an analog era carried production markers (photocopied inserts, hand-written track lists) which announced them as duplicates. In a digital space, as we now know and regularly see, the simple means of exact duplication has shifted the relationship between producer, consumer, and artifact. And although digital delivery offers opportunities to rethink and challenge these relationships, the tensions involved—between producer, consumer, and artifact—have been a staple of hacker culture since the first phone phreakers in the 1960s and 70s. To think through this history and these relationships, however, it is helpful to develop a delivery heuristic. In the next sections, I turn to Jim Porter's *techne* of digital delivery, situating it in terms of hacker activity, and then using it to think through three key narratives in the archives of *2600*.

---

[9] Napster is now recognized as the first major widely-used instance of peer-to-peer filesharing. Napster offered an easy-to-use interface for the exchange of mp3 files, and the service was quickly sued and shut down by the recording industry. It is now seen as a sort of watershed moment for filesharing and digital distribution. I discuss this in more detail in the next chapter.

Hacking and the Techne of Digital Delivery

In response to the shifting relationship between producers, consumers, and artifacts, Jim Porter (2009) sees "copyright—and the related issues of ownership, licensing, and control of digital material—as a key subtopic of digital delivery." (22) Porter writes that a *techne* of digital delivery must focus on two concerns: productive knowledge and practical judgment (23). In short, such a *techne* must focus on both how a technology works and on the critical consideration of authorial choices. "One cannot be an effective digital writer without knowing both technical procedures and how to deploy them to achieve the desired end," he writes, insisting that "the *techne* for digital rhetoric includes both technical/procedural knowledge and knowledge of audience and effect" (6). Porter is working toward an understanding of digital delivery as an art, and he's attempting to move past the notion that technologies are more than a set of skills to be acquired. One must also understand how delivery speaks to the core rhetorical concerns of audience and message. Porter ultimately arrives a set of *topoi* for digital delivery, a five-part framework for considering digital rhetorical decisions:

- *Body/Identity* — concerning online representations of the body, gestures, voice, dress, and image, and questions of identity and performance and online representations of race, class, gender, sexual orientation, and ethnicity
- *Distribution/Circulation* — concerning the technological publishing options for reproducing, distributing, and circulating digital information
- *Access/Accessibility* — concerning questions about audience connectedness to Internet-based information

- *Interaction* — concerning the range and types of engagement (between people, between people and information) encouraged or allowed by digital designs
- *Economics* — concerning copyright, ownership and control of information, fair use, authorship, and the politics of information policy. (208)

I reprint his heuristic here because I'm struck by its connection to current hacking practices. I also think that Porter's frame offers a way to read hacking in relation to the *techne* of digital delivery. In the following subsections I briefly address each of Porter's considerations, connecting them to current hacking practices.

Body/Identity

In classical thought, body and identity are major facets of the canon of delivery. In her keynote address to the 2005 Computers and Writing conference, Andrea Lunsford echoed the importance of action and delivery in contemporary considerations, viewing writing "as an active performance, that is an act always involving the body and performance" (170). Lunsford firmly places her definition of *delivery* within *performance*, and Porter's body/identity *topoi* echoes this connection. Differentiating two types of ethos—that of writing a newspaper editorial and that of attending a protest—Porter writes that "public performance is also rhetoric: using the body itself as a 'text,' a delivery mechanism for a persuasive point" (212).

Prior to the past two years, it might be difficult to see hacking as an embodied activity. The 1960s hacker, as described by Levy, was a code-focused student who never left the computer lab. The typical mid-90s depiction of a hacker focused on a suburban, white, nondescript male, usually hidden away in a poorly lit basement. In these views of hacking, the hacker is a vehicle, a digital presence, a means through which the hacker ethic is employed. Recent shifts toward

"hacktivism," however, remind us that hacking has always been a performed and, to some degree, embodied activity.

For example, Anonymous, the most visible hacking group today, has adopted the Guy Fawkes mask (Figure 3) as its trademark. Members of the group often wear the mask when participating in public protest, drawing on the cultural symbolism of the Gunpowder Plot and narratives such as Alan Moore's *V for Vendetta*. It is helpful to compare the mask to the Anonymous "flag," which represents a more conventional understanding of hacking. The flag (Figure 4) shows an individual, donned in business wear, with a question mark rather than a depiction of a face, inferring that Anonymous are not knowable, that they lack personal distinctions, that they are a public without traditional embodied representations of self. When comparing the flag to the mask, however, we're reminded that this sort of anonymity is a rhetorical move—one reinforced by the Guy Fawkes mask. Both of these icons draw on understandings of anonymity and traditional hacker narratives. In the standard Hollywood tale, the hacker is dangerous, an anonymous threat to your banking account. By appropriating the images of that anonymity, however, Anonymous can *perform* that anonymity. Hacking, they remind us, was always embodied. Additionally, as Anonymous have moved from computer-based attacks to physical protests, they have added many non-hackers to their rank. As Gabriella

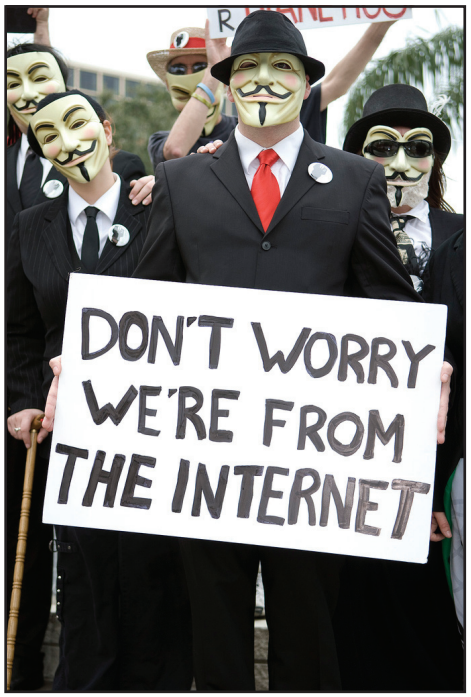

Figure 3 [Creative Commons Licensed]
Members of Anonymous at a public protest
from Anonymous 9000; "2nd Anoiversary 13" *Flickr;* Yahoo!; 16 January 2010; Web; 16 December 2011.

Figure 4 [Public Domain]
The de facto Anonymous flag
from AnonymousLegion; "Anonymous Flag" *Wikipedia;* Wikimedia Foundation; 25 January 2009; Web; 16 December 2011.

Coleman and Michael Ralph note ("Is It A Crime?"), participation in Anonymous is no longer limited to some hacker elite; instead, a knowledge and digital literacy of specific communication tools (Internet Relay Chat, for example) is the only participatory threshold. The Guy Fawkes mask and the performance of anonymity also represents a move toward inclusive practice and protest.

It is also worth noting that Anonymous does not represent all hackers and that hacking is performed in other ways. For example, Lulz Security, a hacker group that splintered from Anonymous and, to some degree, was successful in mocking the seriousness implied by the Guy Fawkes mask, represented itself much differently. The Lulz Security logo (Figure 5) depicts a figure with a top hat, monocle, handlebar mustache, and glass of wine, drawing on cultural signals of class and taste. If the Anonymous flag is based on a conception of the hacker as unknowable, the Lulz Security logo shows hacking as an irreverent practice—as a performance both beyond and wholly embracing the over-the-top symbols often associated with hacking. Here, the hacker is cultured and disdainful, mocking the social message of Anonymous by adopting signifiers attached to an archaic cultural elitism. And the Lulz Security logo, like the Anonymous flag and the Guy Fawkes mask, reminds us that the *techne* of contemporary hacking is firmly situated in the ethos of an embodied performance.

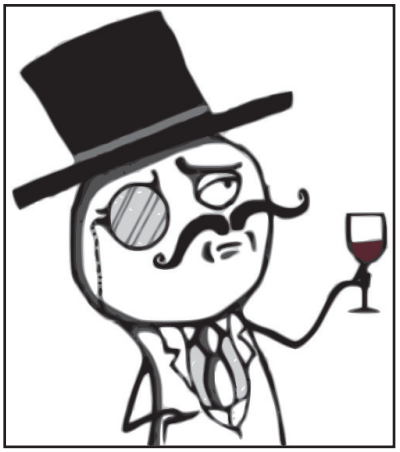

Figure 5 [Fair Use]
The Lulz Security logo
from Lulz Security; "Lulz Security" *Wikipedia;* Wikimedia Foundation; 4 July 2011; Web; 16 December 2011.

Distribution/Circulation

Although the narratives below will consider the relevance of print distribution and circulation to a hacker public like that of *2600*, it is also important to note that the Distributed Denial of Service attack (DDoS), the tool most frequently used in digital protests, is firmly rooted in concerns of distribution and circulation. In a DDoS attack, a website is overloaded with data—the equivalent of hundreds of thousands of users simultaneously pushing refresh on their browser. Most servers aren't capable of simultaneously pushing this amount of data, so the DDoS attack effectively crashes the server, making it appear as if the attacked website is offline. DDoS advocates equate it to a virtual-sit in, crowding the "lobby" of a website so that business-as-usual can't be conducted. DDoS opponents argue that such an analogy doesn't work, as attackers often use thousands of hijacked computers in a DDoS attack. Likewise, they say, a sit-in requires risking the body and carries an imminent threat of arrest. A DDoS attack, however, is disconnected, with a potentially anonymous protester sitting safe at home. The US government has since ruled that DDoS attacks are illegal.

Even in tech-savvy circles, the DDoS attack is a contested subject. Although some see the DDoS attack as a valuable tool for disrupting digital communication, others (including many in the *2600* readership) see the DDoS attack as something petty and outside "true" hacker activity, claiming that it requires no skill or creative thought. The DDoS attack does, however, rely on an understanding of digital delivery and the ways that delivery can be disrupted. Porter writes that "digital distribution refers to rhetorical decisions about the mode of presenting discourse in online situations" (214), and the DDoS attack, regardless of technical complexity, is a rhetorical tool for disrupting that distribution—a kind of anti-discourse. Still, that anti-discourse is a fundamentally discursive act, and it exists within a constellation of traditional discursive moves, such as announcing a DDoS attack via a Web manifesto or rallying DDoS participants through a

platform like Twitter. Likewise, the DDoS conveys a message to both the company being disrupted and to users attempting to access that company's website. In short, it uses an awareness of delivery to purposefully disrupt delivery.

Access/Accessibility

Porter writes that "Approaching the problem [of a task to be communicated] from the perspective of audience access/accessibility means starting with audience need—and with the diversity of audiences—and then developing a rhetorical approach (or, more likely, a variety of approaches) to address that need" (216). Hacker groups like Anonymous have used a number of spaces—Twitter messages, YouTube videos, and even public protests—to communicate their messages. And though Anonymous began in a specific corner of the Internet (the website *4Chan*[10]) with a specific goal (in a sense, digital pranks), the group has since grown and splintered, extending the scope of their actions and their participants through a number of accessible channels. Likewise, *2600* has, for nearly fifteen years, sponsored public meetings for the discussion of technology and hacker concerns. To be recognized by and listed in the publication, *2600* requires that these meetings be held in public spaces and open to anyone. In addition, because *2600* is a print publication, a *2600* reader requires no direct access to computers. Although hacking is often associated with cryptic computer knowledge and acronym-heavy jargon, a *techne* of delivery—as demonstrated by Anonymous and *2600*—requires an awareness of access and its impact on the reception of a message.

Interaction

[10] 4chan is a popular message board best known for its anonymous spaces (there are no logs or archives) and the many cultural memes and in-jokes produced by users of the site.

Porter sees interaction as "a rhetorical topic pertaining (a) to how humans engage computer interfaces in order to perform various actions (e.g., withdraw cash from an ATM, post an entry to a blog), and (b) to how humans engage other humans through computer-mediated spaces" (217). Additionally (and interestingly), Porter writes that:

> The true revolution of the Internet lies at the right end of the interactivity spectrum—when users can critically engage what they read (e.g., by commenting on a published editorial posted on a blog) or further to the right, when they co-produce and become writers, when the distinction between audience and writer blurs. At this level, a site actively invites the audience to become a co-producer of content. (217)

This observation, though centered on Web 2.0 technologies, bears a strong connection to *2600* and similar hacker e-zines (like *Phrack*). *2600* is, in many ways, an interactive *print* technology: its articles are written by readers, and it has, since 1984, featured a letters section that often seems more like the comments section of a blog (in which readers contribute knowledge or address other readers) than a typical magazine's letters section (in which readers address the editors or the publication in general). Likewise, the interaction in a publication like *2600* has, since its inception, spanned both digital and analog mediums. Though *2600* is mailed, it has always accepted submissions via email (or in its early days, via GTE telemail). In addition, *2600* has had a strong connection to the electronic bulletin board community (in the 80s/early-90s) and to the Internet. It is clear that hackers have a huge interest in (what Porter describes as) "how humans engage computer interfaces in order to perform various actions," but the distribution of hacker knowledge has, for quite some time, considered "how humans engage other humans through computer-mediated spaces" (217).

Economics

Of course, the primary relationship between hacking and delivery, I would argue, is that of economics. If, as Porter asserts, all writing "resides in economic systems of value, exchange, and capital" (218), hacking is a challenge to those systems—or at least the way they are currently constructed. Open-source software aside, the majority of technologies rely on obscuring the mechanisms of delivery from the user. These cloaked mechanisms then dictate the roles and abilities of the consumer, generating sanctioned spaces for and uses of products. Hacking is a challenge to these practices and to the economic systems that they promote and reinscribe. In Steven Levy's *Hackers*, for example, the first student hackers found interest in the arrival of early computers at MIT. The students, lacking formal instruction on how to use the machines, began to discover tricks—hacks—that improved their use of the machines. But in other narratives, such as those of phone phreakers, experimentation occurred in response to a closed and mysterious system of delivery. Likewise, the corporate entity in charge of that system (then, the Bell System) issued dictates regarding appropriate and inappropriate use of the system (which was strung through public space and wired into homes), obscuring the technologies of delivery. The phone phreaking (or experimentation) popularized by hobbyists in the 1960s and 70s responded to these closed systems. And from the economies enabled by closed systems of delivery we can arrive at a number of concerns including ownership, transparency, copyright, and the public domain—areas of great interest to hacker publics like that of *2600*.

Through Porter's heuristic, I've tried to situate the practice of hacking as one that both uses and responds to a rhetorical *techne* of digital delivery. In what follows, I employ and extend the concerns of that heuristic (specifically, issues of distribution, access, and economics) within

three narratives from the archives of *2600*. In these narratives, hackers operate in opposition to common (or legally/commercially acceptable) understandings of delivery. Through each, however, *2600* leverages the status of its print artifact as a culturally sanctioned space for discussion, invoking the First Amendment and finding tension between the material deemed appropriate for digital discussion and that deemed acceptable for print. More importantly, however, each of these moments reminds us of the importance of delivery, and how a hacker culture has rallied around and responded to the problems with the privatization and commercialization of the canon.

Narrative 1: Moving Satellites in the Sky

The August 1985 issue of *2600* opens with an all-caps headline of SEIZED!, announcing that the "2600 *Bulletin Board is Implicated in Raid on Jersey Hackers*." First described in the February 1985 issue, *2600* promoted its bulletin board[11], named The Private Sector, as a discussion forum and communications hub—"Hobbyists from all over the country use the system to converse on telecommunications topics," the publication boasts—and as point of faster correspondence between readers and writers: "Now, subscribers will be able to send articles, letters, or questions to *2600* instantly" ("2600 Bulletin Board Online"). Bulletin Board Systems (BBSs) were an important part of the hacker/phreaker infrastructure at this time, and much of *2600*'s early print content was drawn from material that had been first posted to prominent BBSs. Likewise, the 1984/85 issues of *2600* include stories of other bulletin boards falling into the hands of government agents. The June 1985 issue, for example, includes the story "Sherwood

[11] Bulletin Board Systems were modem-driven electronic message boards. In the 80s and early 90s (before mass adoption of the web), they were widely used for the exchange of electronic messages files. The "bulletin board" metaphor was apt, as one user would post a message or file and then log off—and then another user would log onto the site and view the materials.

Forest Shut Down by Secret Service: An All Too Familiar Story," noting that "two of the most prestigious hacker bulletin boards" had been shut down by the Secret Service under allegations of wire fraud and credit card fraud. (In response, *2600* vowed to reprint Sherwood Forest articles in future issues.) Although "The Private Sector" name carried the same tongue-in-cheek connotation as "Sherwood Forest," it is worth noting, based on a repeating ad in the 1985 issues, how specifically *2600* positioned The Private Sector. First, the advertisement speaks of the board's discussion forums—Telcom Digest, BBS Advertising, Telcom, Trashing, Media/News Articles, Telcom Questions, Electronics, Security, Computers & Networking—most of which seem distanced from traditional hacker (or at least typically illegal) jargon. Second, the ad text encourages readers to "Call The Private Sector for the most interesting and intelligent talk on telecommunications and computers that your modem will ever find." By declaring that The Private Sector was a space for *intelligent talk* about *computers* and *telecommunications*, *2600* positioned the board as a hobbyist space rather than—as other boards seemed to be—a hub for the transmission of stolen/illicit documents[12]. Still, that positioning did little to save the board, as the entirety of the August 1985 issue focuses on the government seizure of The Private Sector, beginning with a news-like breakdown of the events:

> On July 12, 1985, law enforcement officials seized The Private Sector BBS, the official computer bulletin board of *2600* magazine, for "complicity in computer theft," under the newly passed, and yet untested, New Jersey Statute 2C:20-25. Police had uncovered in April a credit carding ring operated around a Middlesex County electronic bulletin board, and from there investigated other North Jersey

---

[12] *2600* would maintain that the material kept on its BBS was entirely legal (similar to the materials it printed), though it is now difficult to verify that claim.

> bulletin boards. Not understanding subject matter of the Private Sector BBS, police assumed that the sysop[13] was involved in illegal activities. ("Seized!")

The story proceeds to document the narrative of the seizure (and the arrests of the BBS sysops) and its aftermath. *2600* quickly mobilized, petitioning the prosecutor's office but receiving no news until the next day's press conference, in which "…paranoia about hackers ran rampant. Headlines got as ridiculous as hackers ordering tank parts by telephone from TRW and moving satellites with their home computers in order to make free phone calls." ("Seized!"). For example, a story (from the July 29, 1985 issue of *U.S. News & World Report*) about the arrests of the BBS owners says that

> Prosecutor Alan Rockoff, announcing the arrests on July 17, said the seven had also penetrated "direct lines into sensitive sections of the armed forces." When investigators tried one computer listing, they reached an angry general who demanded to know how they had learned the secret access code. ("'Hackers' Score a New Pentagon Hit")

A similar story from the Associated Press, dated July 16, notes that

> Authorities found on the youths' software telephone numbers of private work lines of generals in the Department of Defense, computer companies that handle medical and financial records, and a computer system of TRW, Inc., a Cleveland based defense contractor ("Prosecutor Says Juveniles Used Computers to Access Defense Information")

and, as reported in a July 17 AP story

---

[13] Sysop is short for System Operator, the individual that owned the computer equipment and maintained the bulletin board.

> "They were changing the positions of satellites up in the blue heavens" to make overseas calls, [the Prosecutor] said, adding that in one instance they disrupted telephone communications on two continents by reprogramming a satellite. Richard A. Brayall, a spokesman for the American Telephone & Telegraph Co., said he didn't believe the youths had information that could move satellites. He said no satellites had changed positions and that there had been no reported attempts to shift satellites. ("Teen-Agers Accused Of Breaking Into Pentagon Computer Program")

The satellite allegation, *2600* writes, stems from a telecommunication forum on The Private Sector, in which users were discussing "TASI (Time Assignment Speech Interpolation), a method of transmitting satellite conversations" ("Moving Satellites"). They also clarify that

> as far as we know there is *no* way to use TASI and similar information fraudulently, and certainly one cannot move satellites using this. Evidently Middlesex County law enforcement saw posted messages on the routing of calls *through* a satellite and jumped, due to paranoia, to the conclusion that it was for the *moving* of the satellites. ("Moving Satellites")

In reports about the seizure, the stories of government infiltration and satellite movement are the most compelling. But those two allegations also speak to cultural perceptions of hacking and misconceptions of delivery. In 1985, perceptions of hacking were still strongly shaped by the film *WarGames*. Douglas Thomas notes that "With the release of *WarGames*, hacker culture had a national audience" and "undoubtedly, the film had a greater impact on hacker culture than any other single media representation" (26). There was also mention of the film in the BBS seizure press conference: "'It's like 'War Games,' only it's real life. It's happening today,' Rockoff said,

referring to the popular movie about a youth who breaks into computers that affect national security operations" ("Teen-Agers Accused Of Breaking Into Pentagon Computer Program"). Writing about *WarGames*, Douglas Thomas also argues that

> In the film, the hacker is positioned as dangerous because he is exploring things about which he has little or no understanding. It is easy in a world of such great technological sophistication, the film argues, to set unintended and potentially disastrous effects into motion even accidentally. […] The hacker stands at the nexus between the danger and the promise of the future of technology. (25-26)

In this instance, the media representation of the hacker is built largely on a suspicion of the unknown, and the *2600* seizure was predicated on that same assumption—mostly a misreading of a discussion thread about transmitting data through satellites. Although there was fear about the hacker's access to protected information, that fear also connected to an unfamiliarity with the BBS technology (BBSs were, in the mid-80s, still toward the cutting edge of communication technologies). The Prosecutor would soon redact his statements, and—months later—The Private Sector would be returned to its owner and all but a minor charge would be dropped ("Private Sector Returning"). The seizure, however, now seems a galvanizing moment in *2600*'s early history, an incident where the publication became especially vocal about the misconceptions of technology. In the August 1985 issue, they connect the seizure to the need for technological literacy:

> The concept of a bulletin board must be understood. The value of The Private Sector must be known. The connection to publications and freedom of speech has to be established so that people understand the threat to *them* whenever a bulletin board is shut down. When we do this, we'll be that much closer to getting The

> Private Sector back on line and making a positive precedent. ("Commentary: The Treat To Us All")

Extending that pedagogical imperative, they also note how the government seizure was initially centered on credit card fraud, explaining how credit card theft is a low tech crime, and how that theft lies in the ease of finding credit card carbons:

> With regards to credit card fraud, computers are only used as a means for communication. Credit card carbons are so easily found and the process of performing the actual illegal charge has been made so easy that it is not even necessary to discuss the topic with others to be able to commit the crime. ("Moving Satellites")

As presented, the true threat isn't the technology, but rather an unchecked business practice that disregards security. And although this could be read as an excuse or a justification for credit card theft, it seems more like a rallying call for a kind of hacker advocacy—a theme that echoes through the issue:

> When all these exotic charges are revealed to be mere flights of fancy, a great lack of knowledge about computers and telephony is uncovered on the part of law enforcement. We feel that law enforcement officials, along with telecommunications hobbyists, should start to research the field by looking in their public library, or even better a local college library. ("Moving Satellites")

This is one of the major themes that runs throughout *2600*'s archives: Government understands too little about technology, and it in turn legislates (or prosecutes) based either on reactionary motives or, more likely, industry pressure. This then creates a system in which the

producers of technology are the driving force in the legislation of that technology. *2600*'s call for education is the primary hacker response to this assertion.

This is also a moment embedded in delivery: data moving through satellites, the alleged transmission of credit card numbers, and the infiltration of TRW (a government contractor) computers. These are all private systems of data transmission, and the core complaint rests *both* on the unlawful entrance into those systems *and* on a bulletin board discussion of those events. But entangled in this is the problem of (and assumptions about) electronic communication. Although there isn't data available for comparison, I think it is fair to assume that the amount of *electronic* participation on the Private Sector BBS had some degree of correlation to the size of *2600*'s *print* readership. Likewise, as stated in an above-quoted AP story:

> Authorities found on the youths' software telephone numbers of private work lines of generals in the Department of Defense, computer companies that handle medical and financial records, and a computer system of TRW, Inc., a Cleveland based defense contractor ("Prosecutor Says Juveniles Used Computers to Access Defense Information")

These alleged transgressions were the exact same concerns that *2600* had already covered in its print publication. The first issue of *2600*, for example, had a listing of White House phone number extensions. And TRW, Inc. had been a major focus in *2600* as it was not just a government contractor but also a credit rating agency—and, in *2600*'s opinion, did a poor job of protecting that credit data. So although *2600*, the print publication, had a degree of autonomy and credibility in discussing and publishing these concerns, The Private Sector, an electronic discussion space, was—at least in 1985—much more vulnerable. The concern, as presented, wasn't *what* was being discussed, but rather *in what space* it was being discussed. And although

the charges against The Private Sector were soon dropped, this issue would again arise in a different form.

Narrative 2: *Phrack* and E911

The first issue of *Phrack*[14], a popular hacker e-zine, was posted to the "Metal Shop BBS" on November 17, 1985. Whereas *2600* positions itself as a mainstream hobbyist publication, *Phrack*'s "Introduction" reads like an address to a BBS-saavy in-group:

> Welcome to the Phrack Inc. Philes. Basically, we are a group of phile writers who have combined our philes and are distributing them in a group. This newsletter-type project is home-based at Metal Shop. If you or your group are interested in writing philes for Phrack Inc. you, your group, your BBS, or any other credits will be included. These philes may include articles on telcom (phreaking/hacking), anarchy (guns and death & destruction) or kracking. Other topics will be allowed also to an certain extent. If you feel you have some material that's original, please call and we'll include it in the next issue possible. Also, you are welcomed to put up these philes on your BBS/AE/Catfur/ Etc. The philes will be regularly available on Metal Shop. If you wish to say in the philes that your BBS will also be sponsoring Phrack Inc., please leave feedback to me, Taran King stating you'd like your BBS in the credits. Later on. ("Introduction")

---

[14] It is worth noting that "Phrack" is a combination of two terms: Phreak and Hack. At the time, like *2600*, it spoke to both phreakers and hackers. Similarly, the use of words like "philes," rather than just "files," reinforces the importance of telephone phreaking to this public in the mid-1980s.

In *Hacker Culture*, Douglas Thomas differentiates *Phrack* from *2600* by pointing to the difference in medium (print vs digital) and audience: *Phrack* directly addressed and monitored the hacker underground. *Phrack*, he says, "tells the members of the underground what is going on, who has been arrested, who is angry with whom, and so on" (121). Although *2600* seems to privilege literacy and advocacy, *Phrack* was more likely to report on files and gossip. *Phrack* was first mentioned in the Summer 1989 issue of *2600*, in a column that stated:

> There's plenty of room in the hacker community for innovative newsletters and magazines. An electronic newsletter called Phrack is one that built a strong following by doing something different: collecting hacker files and articles and distributing them in a "package" to bulletin boards all over the world. One of their regular articles, Phrack World News, is a must-read for many hackers. ("The New TAP")

These "packages," however, soon put *Phrack* on the government radar.

In 1989, *Phrack* distributed a text file titled "Control Office Administration Of Enhanced 911 Services For Special Services And Major Account Centers." The file had been acquired by a hacker, known as Prophet, who found it while snooping through a BellSouth computer that housed emails, calendars, and memos. BellSouth considered that computer invisible and left it wholly unsecured; it required no passwords (Sterling). Prophet copied the file and left.

Though several other people would also receive copies of the file, it ultimately landed in the hands of Craig Neidorf, aka Knight Lightning, the then-publisher of *Phrack*. Neidorf was a political-science major at the University of Missouri, and he was especially interested in freedom of information issues. He saw the potential publication of the E911 document as a hacker badge-of-honor, one that could document the prowess of the underground while also embarrassing

BellSouth. Concerned about liability, however, Neidorf and Prophet cut the document in half, removing phone numbers and non-disclosure warnings. The file was then distributed as part of the February 25, 1989 issue of *Phrack* (Sterling 116). Initially, there was little response to the document. *Phrack*, in turn, maintained business-as-usual, publishing six more issues.

Then, in January of 1990, the phone system crashed. For a full day, *The Washington Post* reported, only 50% of the dialed calls in the US were connected—something the *Post* called "an unprecedented breakdown" (Burgess).

Reporting on the crash, *2600* attributed the phone system failure to a lack of redundancy in the telephone network and to poorly designed AT&T software: "Sounds like a worm[15] to us. Not the kind that gets spread deliberately. There are plenty of programming errors that cause worms. It could happen to any computer system" ("The Day The Phone System Really Died"). The *Washington Post* pointed blame toward the computer network behind the phone system, writing that "suspicions focused on the highly complex computer software that manages the network" and "AT&T's working assumption last night was that its problem was accidental and it played down suggestions that it was caused by a computer 'virus,' a type of program designed to spread and replicate itself and which saboteurs have used to immobilize other computer network." The *Post* also quotes an AT&T spokesman as saying that "All indications so far are that a ... virus is not involved" (Burgess).

Despite AT&T's assertions that the crash was accidental, a secret service agent arrived at Craig Neidorf's door two days after the crash, asking questions about a stolen E911 document.

---

[15] The Jargon File (a hacker dictionary of sorts) defines worm as "a program that propagates itself over a network, reproducing itself as it goes"—a term which comes, via tapeworm, from John Brunner's 1975 sci-fi novel *The Shockwave Rider*. The Jargon File also notes that though "worm" now has a negative connotation, this wasn't always the case. Many early worms were caused by programming errors and code gone awry. *2600* is referring to this kind of worm.

The following day, secret service agents returned with campus police and a search warrant. On February 1st, 1990, Neidorf was indicted on counts of "wire fraud, computer fraud, and interstate transportation of stolen property valued at $5,000 or more" (Denning 26). News reports from the time are telling: A February 1990 story from *The Washington Times* opens with:

> A 19-year-old Missouri man has pleaded not guilty to federal charges that he broke into the 911 emergency telephone network for nine states, then published information on its access to other computer buffs. Prosecutors said that the two used computers to enter the 911 system of Atlanta-based Bell South, then copied the program that controls and maintains the system. ("Alleged 911 Hacker Pleads Not Guilty")

In this account, rather than distributing a redacted E911 document, Neidorf has instead infiltrated, accessed, and copied the program that controls the 911 system for nine states. And the differences—between what was reported and what the *Phrack*/*2600* communities saw as the reality of the situation—speak back to core concerns voiced by *2600* regarding ignorance and misinformation in popular depictions of hacking and technology.

Neidorf's case was ultimately rolled into "Operation Sundevil," a national crackdown on hacking in the summer of 1990, in which at least 150 secret service agents seized at least 42 computers and 23,000 floppy disks. Bruce Sterling, in the *Hacker Crackdown* (1992), documents the process of these hacker raids, describing how suspects were kept under guard while the agents worked through the house. Two agents, typically a "finder" and a "recorder," would look for hot spots such as a teenager's bedroom. Sterling writes:

> Even Secret Service agents were not, and are not, expert computer users. They have not made, and do not make, judgments on the fly about potential threats

> posed by various forms of equipment. They may exercise discretion; they may leave Dad his computer, for instance, but they don't HAVE to. Standard computer-crime search warrants, which date back to the early 80s, use a sweeping language that targets computers, most anything attached to a computer, most anything used to operate a computer—most anything that remotely resembles a computer—plus most any and all written documents surrounding it. Computer-crime investigators have strongly urged agents to seize the works. (Sterling 161)

These raids are an embodiment of the early-1990s government response to hacking, an attempt to push hacking out of the intangible world of digital communication and into the traditional communication channels of print and televised media coverage.

During the ensuing trials, it was revealed that the government had been monitoring *Phrack* for some time. *2600* noted that, for example, the government had monitored every piece of email going into and out of Neidorf's University of Missouri email account ("For Your Own Good"). Shortly before the trial, Neidorf learned that, two years earlier, a team of government agents had, through spyholes and one-way mirrors, filmed "Summercon"—*Phrack*'s one-day convention for hackers. As Sterling describes it, "nothing illegal had occurred on the videotape, other than the guzzling of beer by a couple of minors. Summercons were social events, not sinister cabals. The tapes showed fifteen hours of raucous laughter, pizza-gobbling, in-jokes, and back-slapping" (Sterling 257).

In many ways, the E911 file had as little to do with "Operation Sundevil" (and all the related surveillance) as it did with the phone system crash. The government, however, saw Neidorf and *Phrack* at the center of the hacker underground. This perception and vulnerability, *2600* argued, was due to *Phrack*'s digital distribution: "In many ways *Phrack* resembled *2600*,

with the exception of being sent via electronic mail instead of U.S. Mail. That distinction would prove to be *Phrack*'s undoing" and that there would have been a bigger response if the same thing had happened to a print publication: "Had a printed magazine been shut down in this fashion after having all of their mail opened and read, even the most thick-headed sensationalist media types would have caught on: hey, isn't that a violation of the First Amendment?" ("For Your Own Good").

2600 continued to narrate and critique the Neidorf case, offering (in Summer 1990) a day-by-day account of the trial. The publication was particularly outraged by AT&T's claims regarding the document's worth—$79,449 initially, a figured which was revised down to $24,639.05 (based on AT&T's alleged R&D costs) for the actual trial. However, a turning point occurred when Neidorf's defense attorney pointed out that the E911 document was already publicly available:

> The proprietary claims were further damaged when it was demonstrated that not only was the content of E911 files available in other public documents, but that the public can call an 800 number and obtain the same information in a variety of documents, including information dramatically more detailed than any found in *Phrack*. After considerable waffling by the witness, [the prosecuting attorney] finally received her acknowledgment that the information found in [*Phrack*] could be obtained for a mere $13, the price of a single document, by simply calling a public 800 number to Bellcore, which provided thousands of documents, "including many from Bell South." ("The Neidorf/Phrack Trial")

Two days later, the judge declared a mistrial.

The outrageous document pricing (and the truth of its availability) is perhaps the biggest legacy of this trial, and there are several readings of it. Sterling, in *Hacker Crackdown*, argues that the pricing was simply a maneuver to render the document as dangerous—and, in turn, display how hackers were endangering the public:

> It was not [U.S. Attorney] Cook's strategy to convince the jury that the E911 Document was a major act of theft and should be punished for that reason alone. His strategy was to argue that the E911 Document was DANGEROUS. It was his intention to establish that the E911 Document was "a road-map" to the Enhanced 911 System. Neidorf had deliberately and recklessly distributed a dangerous weapon. Neidorf and the Prophet did not care (or perhaps even gloated at the sinister idea) that the E911 Document could be used by hackers to disrupt 911 service, "a life line for every person certainly in the Southern Bell region of the United States, and indeed, in many communities throughout the United States," in Cook's own words. Neidorf had put people's lives in danger. (259-260)

Sterling also notes how the U.S. Attorney prevented the document from appearing in the public proceedings and would not allow jurors to see the E911 text (260). Each move by the prosecution, it would seem, worked to build an air of danger around the case and its implications.

Douglas Thomas, however, situates the document's value in the "culture of secrecy that surrounds technology." Though, in court, AT&T connected these costs to the economics of production, Thomas argues that the costs actually infer the value of secrecy. "Bellsouth," he writes, "having its document copied and distributed, was itself exposed as not able to maintain secrecy, which is the real source of the damage." Thomas ultimately connects this to ownership

issues, asserting that "the secret is not about withholding information; quite the contrary, the culture of secrecy is about limiting access and to whom information is given" (126).

We can synthesize and extend these arguments into a space of delivery. Although hackers had been previously prosecuted for issues relating to secrecy, the *Phrack* case is a specific and important moment, as this was not simply a file that was stolen and then stored or emailed to a group of associates. This was a file redistributed through a digital publication. And though hackers are often associated with the act of *infiltration*, the *Phrack* trial was firmly grounded in concerns of *circulation*.

As an example: In its Winter 1989-90 Statement of Ownership, Management, and Circulation for the USPS, *2600* claimed a readership of 2,020 individuals. The *Phrack* Hacking directory, as introduced in the case, included 1,300 individuals ("The Neidorf/Phrack Trial"). *2600* had, at this point, published many similar documents and boasted a bigger documented readership. As *2600* had noted, however, they also had the benefit of print, and an attack on a print publication would be read as an attack on the First Amendment. *Phrack*, however, proved to be an easier target, as it was simply a bundle of electronic files distributed via electronic bulletin boards. Although *2600* published much of the same material, it benefited from the legal protection and cultural endorsement offered to a print distribution system.

The digital distribution of the E911 file also says much about the perceived ownership of information. AT&T's network was a public one, with telephone lines reaching across public spaces and into homes, but the specifics of that network were trade secrets. And although the E911 document actually contained little usable information, the document's danger was contextualized in terms of the potential damages of exposure. Within the trial, however, the concern wasn't the loss of AT&T secrets; instead, the whole case centered on the social damage

that could be caused (as connected to the phone system crash) by hacker interference in the 911 system. If non-authorized parties (read: hackers) have access to the inner-workings of this system, the argument infers, the system is jeopardized. So the E911 case presents a tacit argument that the public is better served by a *private* 911 system. If hackers can access the system's documentation—or simply understand how the system works—the system is broken. Publications like *Phrack* and *2600* argue that we are better served by knowing more about how a system functions. The owners of those private systems, however, argue that security and commercial viability require them to keep the systems closed.

Additionally, if we want to conceptualize delivery in terms of performance, there are plenty of examples within this case: hacking as performance, the FBI raid as performance, and court proceedings as performance. But these performances—and the events that incited them—are fundamentally tied to and channeled through the larger cultural systems of delivery, the mediums and machines through which the performance is conveyed to an audience.

Although we see this argument fully realized in the courts of 1990, it is an issue that remains relevant today. Our systems of delivery continue to be obscured.

The *Phrack* trial had several other outcomes worth noting. First, the Electronic Frontier Foundation formed in response to the 1990 hacker raids. Second, following the raids and the trials, *2600* began to document a dramatic increase in annual readership. In 1991, the publication's documented readership was 3,194. In 1992, the number was 5,178. And by 1994, documented circulation was up to 15,332. Although these numbers increase with the growth of the personal computer industry, it is worth noting that they also grow with the post-E911 rise in hacking-related arrests and visibility. Finally, although the letters section is a hallmark of *2600*,

the Summer 1990 issue is the first in which the publication receives and publishes anti-hacker letters. *2600* writes:

> Bringing the *Phrack* story to the attention of the public was no easy task. But it would have been a lot harder were it not for the very thing that the whole case revolved around: the electronic transfer of text. By utilizing this technology, we were able to reach many thousands of people throughout the world. ("Negative Feedback")

So for *2600*, the *Phrack* case was both about the implications of electronic distribution and the opportunities afforded via electronic communication and advocacy. The growth in readership, one might then argue, reflects this understanding of the implications of print and digital communication.

A decade later, however, *2600* would find itself in another legal conflict with echoes of E911.

Narrative 3: DeCSS

The end of the twentieth century marked significant shifts regarding intellectual property rights and the movement toward digital delivery systems, events which were situated within the Digital Millennium Copyright Act (DMCA). The DMCA, signed into law in October 1998, was an extension of the 1976 Copyright Act and had, at least initially, two significant provisions. First, the DMCA created a sort of safe harbor for Internet Service Providers (ISPs)—if they worked with copyright holders to monitor and eliminate violations. So, under the DMCA, an ISP is not liable for a user's infringement if the ISP works with the copyright holder to eliminate that infringement. For example, YouTube is currently a DMCA hotspot. If a YouTube user

uploads infringing content (say, a personal video with a copyrighted song as background music) and YouTube receives a DMCA takedown request from the publisher of that music, YouTube must, under the DMCA, comply or be held liable. The DMCA has thus prompted a digital culture in which many ISPs and websites are not willing to evaluate the use of potentially infringing content; instead, a DMCA takedown notice urges a takedown—regardless of the context of a potential infringement.

Another major provision of the DMCA was the protection of Digital Rights Management software (DRM). DRM, in short, prevents the digital duplication of media. For example, until recently, MP3s purchased at the iTunes Store were protected by Apple's DRM, which dictated the number of computers on which a song could be played, how many times it could be copied to a CD, etc. Today, DRM is most frequently used for the protection of digital video distribution, and DRM is the reason why a video purchased at Amazon's digital video store cannot be played on an Apple device. DRM dictates where and how a file can be used. The DMCA, in turn, clearly states that "no person shall circumvent a technological measure that effectively controls access to a work protected under this title" (1201, 1A) and that "no person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof that is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or portion thereof" (1201, 3b1A).

DRM experienced a boom after the DMCA, especially in regards to the distribution of video. Commercial DVDs, first introduced to market in 1996, included a protection called "Content Scrambling System" (CSS), which prevented some forms of disc duplication and which ensured that a DVD could only be played on an approved device. For computer users, approved

devices included only machines running a Windows or Macintosh operating system. Linux users had no playback options.

In October 1999, a programed named DeCSS was anonymously posted to the LiViD (Linux Video and DVD) mailing list. The poster had seemingly disassembled a DVD player, determined the scrambling algorithm, and then distributed that algorithm via DeCSS. The code quickly spread and was incorporated into software that would allow for video playback on Linux. Lessig (2001) notes the importance of this exigence:

> Let's be clear first about what CSS did. CSS was not like those early software protection systems. It didn't interfere with the ability to copy DVD disks. If you wanted to pirate a DVD disk, all you needed to do was copy the contents from one disk to another. There was no need to decrypt the system in order to copy it. So CSS didn't disable copying. All it did was limit the range of machines that DVD disks could be played on. And that in turn was the limitation that gave rise to the need for a crack. (189)

As Lessig notes, the purpose of DeCSS was not unauthorized duplication; that goal could be achieved by simply duplicating the DVD—encryption and all. Instead, the DeCSS software was built with a goal to facilitate the playback of a DVD on any machine, not just those running the Windows and Mac operating systems. Because Linux, an open-source operating system used by many tech-savvy hobbyists, was outside of the Windows and Mac ecosystem, an application like DeCSS was necessary for DVD playback. From a strictly legal perspective, however, DeCSS—regardless of exigence—violates the DMCA.

Shortly after the initial distribution of DeCSS, the MPAA (Motion Picture Association of America) began issuing DMCA takedown notices to sites hosting the DeCSS code. *2600*, a fierce

critic of the DMCA and a proponent of media mobility, began hosting the code on its website. A November 1999 post on 2600.com reads:

> In the last few days there have been numerous reports of movie industry lawyers shutting down sites offering information about DeCSS. 2600 feels that any such suppression of information is a very dangerous precedent. That is why we feel it's necessary to preserve this information. We do feel sympathy for the DVD industry now that their encryption has been cracked. Perhaps they will learn from this. We hope they apply that knowledge in a constructive way. If they choose to fall back on intimidation, we'll just have to deal with that. ("DVD Encryption Cracked")

Directly below that November 1999 post, 2600.com offered links to the original CSS algorithm, the DeCSS code, and links to other sites hosting the code.

Shortly after, in December of 1999, the DVD Copy Control Association filed a formal complaint (in California) against a number of parties, including *2600*. Three weeks later, the MPAA filed a lawsuit (in New York) against *2600* for distribution of the code. Two months after posting the DeCSS code on their website, *2600* was firmly entrenched in the DeCSS legal battle.

At the trial's onset, there were several notable arguments. First, *2600* (and others) had distributed the code electronically. Though *2600* was a print publication, it had hosted links to the DeCSS code via its website—a digital space. At the time of the trial, *2600* had not distributed the code via its print publication, and, because of its connection to the digital distribution of files, the trial had echoes of the *Phrack*/E911 trial. Second, the distribution of the code was enmeshed in many assumptions about media artifacts and their distribution. In a Spring 2000 editorial, *2600* wrote:

> The MPAA is coming at us using a very scary piece of law that civil libertarians have been wanting to challenge since its inception. It's called the Digital Millennium Copyright Act and it basically makes it illegal to reverse engineer technology. This means you're not allowed to take things apart and figure out how they work if the corporate entities involved don't want you to. With today's technology, you are not actually buying things like DVDs—you are merely buying a license to use them under their conditions. So, under the DMCA, it is illegal to play your DVD on your computer if your computer isn't licensed for it. It's illegal for you to figure out a way to play a European DVD on your TV set. And if you rent a DVD from your local video store, figuring out a way to bypass the commercials in the beginning could land you in court or even prison. ("The Next Chapter")

This argument centers on the notion of licensing media artifacts, a key component of the DeCSS lawsuit and a concept borrowed from the process of distributing software. For example, when a user purchases a copy of Microsoft Office, she is not purchasing a copy of the Microsoft Office code (which is a protected trade secret). Instead, she is licensing the use of that code within the parameters set by the licensor—in this case, Microsoft. In the post DRM-era, many media companies have appropriated the license metaphor. This metaphor, however, often proves problematic for media consumers. Long before digital distribution, art often seemed inseparable from the distributed artifact; this is rendered in the ways people speak of their favorite "album" or "record." The physical object of distribution is, as necessitated by commercial processes, fundamentally connected to the conceptual piece being distributed. This artwork/artifact conflation creates dissonance when media companies appropriate a license metaphor.

From the *2600* perspective, an artifact, once purchased, is fair game for any use scenario. For example, a record should be able to play on any record player, and it should be available for any type of use—to be played backwards or to be remixed for hip hop break beats. From an MPAA perspective, however, the artifact serves only as a neutral medium of transmission for the actual thing, the artwork, which is governed by specific licensing guidelines created by the rights holder. And the core of the DeCSS trial rested in the space between these two perspectives: The MPAA saw DeCSS as a tool that could only serve the purpose of violating licensing terms and agreements (which ultimately enables piracy). 2600 saw DeCSS as a means of device liberation, allowing a user to watch DVDs when and how she wanted[16].

Months later, *2600* would lose the DeCSS case. *2600*'s final argument rested on the First Amendment, insisting that the distribution of computer code was free speech and should be protected as such. The court, however, would support the power of the DMCA and argue that the DeCSS exists only to subvert copyright protections (which, they say, the government has a vested interest in protecting) and not to enable any sort of meaningful speech:

> The restriction the Court here upholds, notwithstanding that computer code is within the area of First Amendment concern, is limited (1) to programs that circumvent access controls to copyrighted works in digital form in circumstances in which (2) there is no other practical means of preventing infringement through use of the programs, and (3) the regulation is motivated by a desire to prevent

---

[16] One interesting side note regarding the licensing/artifact issue: In most current software licensing scenarios, a user can re-download an application if the file is accidentally lost or deleted. This is because the user has purchased a license to use the software, and that license extends beyond a single instance of the program. Recently, Apple and Amazon have pushed the music and movie industries to adopt similar policies (allowing users to re-download purchased content). The music and movie industries have been reluctant to sign on.

> performance of the function for which the programs exist rather than any message they might convey. (Universal City Studios Inc. v. Shawn C. Reimerdes)

Within this trial and decision, there is a complex web of Porter's *topoi* of digital delivery, particularly in regards to the intersections of distribution and economics. Much of this centers on the means of transmitting copyright-protected documents through digital systems. Prior to the growth of digital delivery systems, *mass* distribution was contingent on expensive technologies and distribution chains typically owned by commercial entities. Although there were plenty of opportunities for smaller and localized distribution, and there were independent means of achieving that distribution, mass distribution was largely a function of industry and of the commercial entities producing and distributing artifacts. In many ways, the growth of those technologies further entrenched the relationship between distribution and the commercial economies that drive mass distribution. Through the growth of this distribution apparatus, the business of making and distributing an artifact (like a DVD) had a primary concern in the integrity and protection of that system of mass delivery.

Digital delivery presented a new challenge to these systems, as both independent producers and consumers had easy and affordable access to those systems of mass delivery. The whole of the Napster conflict, for example, centered on the fact that a music consumer could, with only simple software tools, engage in the duplication and mass distribution of audio files—a process that was much quicker and more efficient than the authorized commercial systems of delivery. This threat hangs over the whole of digital delivery, and it drives much of the discussion and legal consideration of digital space. The DMCA's primary purpose is to protect those traditional channels and modes (especially in regards to consumer media), reifying a print-based copyright model in a digital space. And, as Leah Lievrouw notes, "the legal decision

against [2600] allows the 'anticircumvention' provisions of the DMCA to take precedence over the First Amendment rights of speech and press" (116). The impact of that anticircumvention protection extends well beyond the artifacts of entertainment media, and this creep of influence mobilized activist hacker publics like that of *2600*.

Because *2600*'s argument centered on the notion of protected speech, the computer underground took the court decision (and increased legal pressure to eliminate the distribution of DeCSS) as a rallying cry, and new forms of DeCSS emerged. Motivated (and now archived) by Dr. David S. Touretzky of Carnegie Mellon, DeCSS advocates quickly generated new ways of distributing the code. If, as the courts argued, code wasn't protected speech, computer enthusiasts attempted to stretch the boundaries of language and genre, considering how an adaptation or translation of the DeCSS code might push it into protected territory. Notable contributions to this project included distribution by music, by a Star Wars-like video sequence, by representations of the code on T-shirts and ties, and, perhaps most famously, by Seth Schoen's DeCSS 456 haiku, which begins:

> (I abandon my
> exclusive rights to make or
> perform copies of
>
> this work, U. S. Code
> Title Seventeen, section
> One Hundred and Six.)
>
> Muse! When we learned to

count, little did we know all

the things we could do

some day by shuffling

those numbers: Pythagoras

said “All is number”

long before he saw

computers and their effects,

or what they could do

by computation,

naive and mechanical

fast arithmetic. (Schoen)

And which includes the technical details of DeCSS in haiku form:

Use t2 for an

index into Table Two:

find a byte b1.

Use t1 for an

index into Table Three:

find a byte b2.

Take exclusive OR
of b1 with b2 and
store this in t4.

Shift t1 right by
a single bit (like halving);
store this in t2.

Take the low bit of
t1 (so, AND it with one),
shift it left eight bits,

then take exclusive
OR of that with t4; store
this back in t1. (Schoen)

Central to these interpretations of DeCSS, to the arguments about free speech, to the distribution of the code, and to *2600*'s position in the case, is the role of delivery in the transmission of texts. And though the core conflict of DeCSS focused on the delivery of DVDs, the implications of this challenge moves well beyond the transfer and playback of video.

Many of the precedents for digital delivery are being set in the space of consumer entertainment media and by major media conglomerates. These precedents have been set in the

ten years after the DMCA, in a group of laws built to maintain the trends and norms of a print and analog culture of distribution. Multiple editorials in *2600* argue that these laws are the product of corporate influence and lawmakers who understand too little of digital culture—the same lawmakers who alleged that hackers were moving satellites or altering the 911 system. And within this relationship between corporate technology interests and governing bodies, there is a slow movement toward commercial privilege and consumer limitations. Ownership has become the defining characteristic of digital delivery, and consumers, the DMCA argues, can't own a piece of media or a technology platform. They can simply borrow that media or use that platform in an authorized manner.

Returning to the notion of a *responsive public* (discussed in the previous chapter), many current hacker projects are a response to these limitations. "Hacker spaces," club-like workshops in which a hobbyist can rent a bench and participate in any number of community-based hobbyist projects, are a recent example of this—an assertion that technology is not limited to the consumable and disposable, and that electronics be repurposed and redesigned. If the commercial space will not tolerate this sort of experimentation, the responsive public says, we'll create our means of doing so. This response works well for the repurposing of consumer electronics; however, political speech or public activism seems to shift the nature of and space for the response. In the following chapter, I will consider how shifts in public policy—and our responses to them—have a tremendous influence on the future of discourse in digital spaces.

Conclusion

Although the common conception of a hacker public is linked to emerging technologies, I think the three narratives used in this chapter are a reminder that although hacker groups often

form around a shared interest in technology, that interest often finds them in conflict with the producers and legislators of technology. In the same way that Trimbur and Welch argued that texts circulate within networks of individuals and ideologies, hacker publics like that of *2600* argue—either directly or through their actions—that corporate and legal limitations on consumer and telecommunication technologies have an impact that extends well beyond the individual use of a DVD or a fax machine. And just as an academic deprivileging of delivery enabled the rise of, for example, current traditional pedagogies, the slow creep of copyright law and proprietary licenses echo the problems with ownership and a dismissal of the complex channels through which artifacts move. And although the *2600* public rallies around technology, the limitations placed on the usage of technology have in turn shifted the nature and focus of their discussion and work.

And with an increase in access to the technologies of mass collaboration and distribution, these publics have been able to fabricate fissures in the traditional systems of delivery. Still, the situation remains complex: As publics like that of *2600* and Anonymous have moved more toward activism and action, they still face the challenges of organizing within commercial, privatized spaces. Although emerging technologies provide opportunities for mass collaboration and distribution, those technologies—and the spaces they generate—have specific thresholds for dissent and action. In the next chapter, I address that very question: What are the potentials of and problems with a digital public sphere that is privately owned? Embedded within that question are issues of memory and delivery—of the storage and transmission of artifacts, ideas, and texts. By reading the work of hacker publics as responding to concerns of memory and delivery (rather than the technologies themselves), we can begin to conceptualize the challenges to activism and dissent in digital spaces.

Chapter Five: Property, Circulation, Publics

> "In thinking about the relationship between forms of symbolic representation that humanists care about and forms of political representation that activists care about, perhaps we need to break some systems to understand how they are made" (181).
>
> —Elizabeth Losh, from "Hacktivism and the Humanities"

> "But work in computation and digital media is, in fact, a radically heterogeneous and multimodally layered—read, not visible—set of practices, constraints, and codifications that operate below the level of user interaction. In this layered invisibility lies our critical work. So no, our ethics, methods, and theory are *not transparent* in our tools—unless you have the serious know-how to critically make them or to hack them. So let's work in and teach the serious know-how of code and critique, computation and cultural studies, collaboration and multimodal composing as so many literacies, capacities, and expressivities attuned to our moment and to the contexts and conditions in which we find ourselves" (109).
>
> —Jamie "Skye" Bianco, from "The Digital Humanities Which Is Not One"

Introduction

In "Technology and Literacy: A Story about the Perils of Not Paying Attention," an essay drawn from her 1997 Chair's Address to the Conference on College Composition and Communication, Cynthia Selfe makes an important call-to-action: "I believe composition studies faculty have a much larger and more complicated obligation to fulfill—that of trying to understand and make sense of, to *pay attention* to, how technology is now inextricably linked to

literacy and literacy education in this country" (414). Selfe's essay is a response to a document from the Clinton-Gore administration, *Getting America's Children Ready for the Twenty-First Century*, "which announced an official national project to expand *technological literacy*" (416) and which found schools and states making budget cuts to create funding for technology expenditures. Selfe troubles the project's core assertion, "that such an effort will provide all Americans with an education enriched by technology, and, thus, equal opportunity to access high-paying, technology-rich jobs and economic prosperity after graduation" (419), and the social progress narrative that is often attached to similar literacy myths.

But Selfe also connects this late-90s push for digital literacy to the economic concerns of the Clinton-Gore administration, noting how students who learned to communicate in high-tech schools would then want those high-tech tools later in life—driving the consumption of updated technologies and support for public policies that favor market growth in the technology sector (427).

It is important to firmly situate Selfe's argument in a historical context: She was writing at the dawn of the Web, before the burst of the dot-com bubble, before the growth of smartphones, before Google and Facebook. The technological world of Selfe's essay was much different from the one in which I write this chapter—and that is exactly what makes her warning so prescient and so harrowing.

Today, in 2012, we might say that the Clinton and Gore plan was, by their measure, an economic success. Between tablets, smartphones, and notebook computers, technology sales have simply skyrocketed. For example, as of this writing, Apple Computer is the world's most valuable company with a market capitalization of over $500 billion, almost $100 billion more

than Exxon, which is the world's second most valuable company ("Apple market value"). Computer consumption is booming.

Higher education is a notable part of this boom: Frequently refreshed computer labs, classroom technologies, mandatory laptop purchase policies. And yet, I would argue, outside of a dedicated few, we have been very slow to adapt to and critically engage with these new technologies. In too many ways, the study and teaching of literacy looks much like it always has. Technology consumption has surged, but the acquisition of critical digital literacies has been comparably slow. Too often, I worry, we haven't paid attention.

In this final chapter, I historicize and contextualize an approach to technology, property, and authorship. Specifically, I place the previously discussed concerns of hacker exploitation/ experimentation within a context of intellectual property and digital publics. Through such an arc, I hope to better understand and explain the implications of policies such as the recent Stop Online Piracy Act (SOPA), as well as provide a direction for future work.

I begin with an overview of intellectual property policy in the United States, focusing on a period of time that begins with the 1984 *Sony v. Universal* case and ends with the 2001 lawsuit against Napster. This period of time, I argue, placed the growth of consumer technologies within a backdrop of property and ownership, and many of the following (2000-2010) developments in composing and connectivity technologies were situated within a frame of ownership. SOPA, for example, is presented as a means of protecting property, but actually extends well beyond that. This property-centric focus has considerable implications for contemporary authorship and for the future of texts.

I then shift to a brief consideration of Digital Rights Management (DRM) software, the technologies of ownership, and the networks through which texts move. Drawing on work from

scholars like Dan Burk and John Tehranian, I argue that these technologies of protecting ownership are an attempt to reinscribe materiality on digital objects. This reinscription, however, offers a tremendous amount of commercial overreach, granting rights-owners invasive and potentially damaging capabilities that simply weren't possible with non-digital artifacts.

This overreach extends into questions of the public sphere and considerations of digital dissent, prompting a question of how transparent and commercially protected spheres impact digital discourse. In considering that problem, I situate my discussion of the digital sphere within work by Warner, Calhoun, Dean, and Downey and Fenton. With an eye toward digital dissent and disruption, I argue, we need to develop a view of discourse, dissent, and authorship that is informed by the technologies through which texts circulate.

Within this chapter, I make a number of calls and assertions about the directions in which I believe the field must move. It is important to note, however, that many of my colleagues are already engaged in this work. Although I believe that there is still too much hesitation toward non-print authorship and the tools of digital communication, I readily acknowledge that a number of wonderful people are fighting the good fight—and I thank them for the inspiration they've offered me.

Finally, beyond just being the final section of a dissertation, I believe that this chapter marks some of my thinking for future work. In short: It is on thing to argue for change; it is another to engage in the difficult work that ultimately generates change. Though I do much of the former, I'm ready to tackle the latter. This, I hope, is a first utterance toward that.

Copyright Law, Napster, and the Shape of the Conversation

The 1980s and 1990s saw significant shifts in U.S. copyright laws, a period that began with the 1984 Supreme Court decision on *Sony Corp. of Amer v. Universal City Studios, Inc.*—often referred to as the *Sony-Betamax* case. The conflict evolved from Sony's production of the Betamax recorder, one of the first mainstream consumer tools for video recording. Universal Studios saw significant infringement capabilities in the recorder and quickly filed suit against Sony, arguing that Sony was liable for any copyright infringement committed by Betamax owners. In a 5-4 decision, the U.S. Supreme court offered several important rulings, most notably that "time shifting" (recording a program, for personal use, to watch at a later time) is considered "fair use" and that a technological manufacturer can't be held liable for potential infringing uses of that technology if that technology "merely be capable of substantial noninfringing uses" (*Sony v. Universal*).

The *Betamax* decision would shape much of the thinking about reproduction and distribution in the 1980s and 90s, and the decision would be cited in many subsequent discussions about digital copyright infringement. In short, the Betamax case now acts as an important frame for modern considerations of copyright. As John Logie notes in *Peers, Pirates, and Persuasion*, "the holding in *Betamax* has largely been understood as articulating a principle of judicial non-interference with technologies that have both legal and potentially illegal applications" and that "the *Betamax* standard is necessary for the ongoing development of computer technologies because copying data is fundamental to the operation of computer technologies" (134). From backups to email attachments to the mass duplication that happens on a basic processing level, we have countless interactions with the copying of data on a daily basis, and the *Betamax* case has been the fulcrum of much of the professional and legal consideration of digital duplication. Sure, copyright questions were a concern well before the *Betamax* case,

but that specific Supreme Court decision marks the start of an arc in which content producers, technological manufacturers, and consumers have found tension in both the marketplace and the courts.

Although the Digital Millennium Copyright Act (DMCA) was passed fourteen years after the *Betamax* case, it shares some important conceptual links with the Betamax ruling. In *Code*, Lessig traces the DMCA to a 1995 Commerce Department White Paper—*Intellectual Property and the National Information Infrastructure*—that suggested changes to law based on developing technologies and the growth of the Internet. The proposed suggestions included a clarification of copyright law, an increase in copyright education, and legal support for "copyright management schemes" (174). The DMCA's most notable legacy is that final tenet, the ways in which it protects copyright management software. Although the DMCA was born in the context of growing digital tools and Internet usage, the copyright protection provision specifically spoke to the *Betamax* case and the advances in duplication technologies available to consumers. That provision is, in some ways, an adjustment to *Betamax*, a means of allowing for the development of potentially-infringing technologies while also setting specific legal constraints on the uses of those technologies.

Following the DMCA, Congress passed the (1998) Copyright Term Extension Act. In a string of policy rulings concerning intellectual property, the bill extended the Copyright Act of 1976 and created a greater barrier between copyrighted works and the public domain (which, after the bill, instituted a copyrighted period of at least the author's life plus seventy years). As Lessig has noted, the copyright system—which had been fairly stable in early U.S. history—experienced significant revision in a short amount of time, and by the late-1990s was "more effectively protected than at any time since Gutenberg" (*Code* 175).

It is within this context that Napster arrived.

The late 1990s saw tremendous commercial and consumer interest in the potential of streaming music, with companies like RealNetworks and MP3.com developing means of encoding and transmitting audio files. These shifts threatened the decades-long distribution channels owned and managed by major record labels, and the industry, as John Alderman documents in *Sonic Boom*, "took notice and as the incredible ongoing growth in online music raised the prospect of a label-less future, the industry finally began to invest heavily in online ventures—hedging its bets as much as providing real vision" (96).

Meanwhile, in a now well-known moment, Shawn Fanning—a student at Northeastern University—was spending sleepless nights developing a peer-to-peer system of music exchange. "While MP3.com was moving ahead full-throttle with IPO money," Alderman writes, "the Napster trio didn't seem to care at all about the music industry, making friends, or playing by established rules. All Fanning really wanted was to make it easier to find music to trade online" (103). Napster, the system that Fanning developed, was a technological departure from the typical, browser-based Web. Different from the standard architecture of Web usage, in which "clients" (through browsers) accessed "servers," Napster placed clients in communication with each other (a client-client model), moving away from a server-based model and creating a potentially more powerful system of distribution (Reyman 3). In this case, the system facilitated the sharing of music—much of which was copyrighted. And this system of sharing was hugely popular, with over 80 million registered users at the height of Napster's popularity (Logie 5).

The importance of the Napster moment can't be understated. As DeVoss and Porter note, "The Napster controversy surfaced trends and tensions at play in our digital culture and across the diverse and robust networks that emerged and rapidly grew in the late 1990s and into the

2000s" (182). If the *Betamax* decision and the DMCA were passed in moments fearful of duplication technologies, Napster appeared to be the full realization of that fear. Consumers were freely trading copyrighted works, a piece of software was facilitating exchanges an order of magnitude greater than that of any previous system, and almost every use of the system seemed to result in an infringing action.

The responses were swift. Napster was quickly sued and shut down, and content distributors began to develop aggressive Digital Rights Management software. As Lessig writes, "copyright has always been at war with technology" (*Code* 172), but the 1980s and 90s, a period of significant technological growth, saw concerns of copyright framing that growth. From a policy standpoint, the context of the digital regulation in the early 2000s was one of property and of ownership.

The Napster moment, however, in coalescing fears and predictions of digital distribution, also did much to determine the direction of the digital conversation. Though Napster was revolutionary in terms of the technologies developed, it shifted the cultural focus away from those technologies and toward issues of property, copyright, and ownership. Much of the modern, commercial Web obscures its inner-workings from the end-user, and the Napster moment accelerated that shift.

DRM, Authorship, and the Inscription of Materiality

With the use of unauthorized peer-to-peer software growing in the early 2000s, the music industry—like many other content industries—quickly turned to Digital Rights Management (DRM) software. DRM wasn't a direct product of Napster and similar digital distribution networks, but the Napster moment surely helped to fuel industry interest in and development of

DRM. In a post-*Betamax* and post-Napster world, rife with consumer-grade media duplication technologies, many content industries backed the development of DRM tools which would—through various means—prevent the duplication of a given artifact. These tools, for example, were at the center of the DeCSS conflict documented in Chapter Four. In an attempt to prevent unauthorized duplication and distribution of films, many major film companies encoded their DVDs with the DeCSS software, which would limit the ways that a consumer could interact with content on a computer.

Dan Burk notes that shifts in copyright law and the development of DRM "represent a strategic response to the increasing de-materialization of the text that, ironically, rely upon the text's materiality" (226). In this way, the move to develop rights management software is an attempt to reinscribe materiality onto the digital artifact. If duplication is a core facet of digital texts, then copyright-protection software uses digital tools to rewrite a more limited type of digital file. As Burk writes, "Copyright assumes that the technological pressure point where control may be asserted is at the point of reproduction and so confers upon the author a copyright —that is, not only the right *to* copy, but also the right *to prevent copying* and related activity" (226). The reinscription of materiality also recreates a production process and the post-production use scenarios of artifacts created by that process.

To date, a significant portion of the reaction against this process has considered how it might affect the *transformative use* of copyrighted work. Much of Lawrence Lessig's scholarship, for example, has focused on this problem, and Lessig's work in developing the Creative Commons and its related licenses are one response to a shrinking public domain. Many Rhetoric and Writing scholars have revised and extended these concerns of copyright, and the connection seems natural: The concerns of intellectual property, and of creative freedom, are the

concerns of authorship. And yet even that relationship is tenuous: Martine Courant Rife posits that, "in academic contexts, we own the discourse of 'plagiarism' but we do not own the discourse of 'fair use'" ("Kairos"). The difference in terms is striking: Plagiarism connotes improper procedure or theft, whereas fair use implies comment or critique or creation. Considered generally, such a contrast infers that our profession might have more in common with the late 1990s music industry than we would care to admit.

Within the context of copyright law and the DMCA, however, the concepts of digital *copyright* and *ownership* have grown beyond those of their material predecessors. As John Tehranian observes, the continued regulation of copyright has "allowed government and putative rightsholders to invade the private sphere to regulate such previously protected activities as the sharing of family photo albums, the use of photocopied scholarly articles by students, and the enjoyment and study of motion pictures by cinephiles" (53). This point was exemplified in a February 2012 lawsuit between Cengage Learning, a publisher, and Kno, an e-textbook vender. The Kno application allowed readers to highlight passages of the text, annotating and marking them for later reference. Cengage argued that this facilitated copyright infringement, enabling the user to create "a derivative work" (DeSantis).

So although the purported goal of rights management software might be to limit duplication, the outcomes often go well beyond that. Tehranian notes that "technological and legal changes are increasingly undermining the access and use rights that consumers of copyrighted works have long enjoyed" (53), and he illustrates the point with a cogent example:

> By performing the equivalent of ripping holes in one's jeans (e.g., remixing a song or altering a brand name) a consumer of intellectual property runs afoul of a copyright holder's exclusive right to create derivative works or a trademark

> holder's right to prevent dilution. One can contextualize and communicate one's relationship with one's jeans by wearing them in public, but the equivalent act of publicly utilizing a copyrighted work would impinge on an author's exclusive right to control public displays and performances. (61)

Within this context, it is helpful to return to the SOPA issues documented in Chapter One. The SOPA bill was framed in terms of piracy and legality, with the bill positioned as an attempt to "promote prosperity, creativity, entrepreneurship, and innovation by combating the theft of U.S. property." Yet SOPA is very much about the technologies of digital distribution—how to monitor them, regulate them, and disable them.

DNS and Dissent

This connection was further emphasized by the January 2012 takedown of megaupload.com. Megaupload was a type of digital locker, allowing users to log in, store files, and exchange those files with other users. The site claimed four percent of all Internet traffic, and the U.S. Justice Department alleged that most of these visitors were searching for copyrighted content—and that the site facilitated infringement on a "massive scale." The U.S. Government's primary claim was that Megaupload encouraged piracy; in short, it rewarded users for uploading copyrighted content. The site then generated massive advertising and subscription fees while distributing that copyrighted content. Because all dot com domains—regardless of the server's geographic location—fall under U.S. purview (they're managed by Verisign, a U.S. company), a court order was issued, the DNS link was broken, and the site was taken offline (Kravets).

This exact tactic was used again in February 2012 against the sports gambling website Bodog.com. Despite the fact that Bodog was based in Canada and registered through a Canadian

company, the U.S. Attorney's Office took its complaint directly to Verisign, the overseer of all dot com domains, and seized the domain (Gottfried).

Although digital lockers and online gambling might seem disconnected from the distribution of digital text or digital social action, the message here is harrowing. When we produce texts for the Web, we are operating in a heavily commercialized space and in a heavily monitored and regulated space. Increasingly, these spaces obscure their commercialization, disguising the mechanisms of distribution and circulation in the name of ease-of-use. How many organizations with dot com names understand that they aren't a distributed tool, but that they rather fall under the authority of Verisign, a single Northern Virginia-based company?

These threats to digital distribution also raise questions about both the tactical nature of the medium and of the legacies of print. Mathieu and George, in an exploration of homeless media advocacy, consider the impact and importance of alternative press papers, which "stand in stark contrast to the giant media conglomerates that produce most of the information most U.S. Americans hear, see, or read every day" (132). As Mathieu and George write, these independent print publications "can and do create troubles for large institutions" (133), but they're also (to some degree) protected by the legacy of print freedom, by the tactical mobility of the dissident publication, and by the technology of print publishing.

This is where analogies of print and digital distribution begin to fall apart and where we have to begin thinking differently about dissent in digital spaces. To impose the equivalent of a DNS-seizing mandate on a dissident print publication would be to seize the means of production and distribution. In the scenario of SOPA or of the Megaupload takedown, the typical response to unsanctioned behavior has been to seize the domain at the DNS level and to thus take the entire site offline.

For example, Operation Payback, a 2010 hacktivist response to the de-funding of Wikileaks, offers another perspective on the issue of dissent and digital circulation. Operation Payback consisted of DDoS attacks on the websites of PayPal and Visa, corporations that had withdrawn support from Wikileaks. The DDoS attacks were impromptu, loosely organized, and largely coordinated through Twitter—a service that had promoted its role in the 2009 Iranian election protests, the 2011 Arab Spring, and other instances of political uprising and revolution ("Up, Up, and Away"; "The Tweets Must Flow"). And yet Operation Payback, an instance of digital dissent in the United States, was quickly shutdown by Twitter, its accounts suspended. Digital distribution services like Twitter are often so accessible and ubiquitous that they can appear transparent—networks of users publishing text in a seemingly neutral environment. Yet these digital services are highly commercial spaces, existing within a networked sphere and determining the constraints of acceptable discourse within their electronic borders. As Clay Shirky reminds us, the Web is "a corporate sphere that tolerates public speech" (qtd. in Vance and Helft), and the boundaries of that tolerance have a tremendous impact on the circulation of digital texts and ideas.

Public Spheres, Digital Spaces

A consideration of commercial boundaries and transgressive activities in digital spaces ultimately brings us to a consideration of publics. With the the emergence of widespread digital network technologies in the 1990s, many of which focused on forums and discussion spaces, notions of a Habermasian digital public sphere found intellectual traction (Dean 96-97). Habermas, in his examination of shifting social conditions in the eighteenth century—specifically, the growth of print culture, coffee houses, and salons—"conceptualize[d] the public

sphere in terms of the public use of reason," reading democratic practice as a place for discourse and the deliberation of ideas (Dean 96). This was a shift away from an aristocratic notion of publicness in which "power is displayed before a public," in which "the monarch's presence was always public, and courtliness always had an audience," and in which "the publicity of the court was always embodied and authoritative" (Warner 47). In his reading of Habermas, Warner notes that in the shift toward a bourgeois space for critical discussion, "a public that 'from the outset was a reading public' became 'the abstract counterpart of public authority' and 'came into awareness of itself as the latter's opponent, that is, as the public of the now emerging *public sphere of society*.'" In this way, as Warner explains, the public "was no longer opposed to the private. It *was* private" (47).

Warner also argues that "the important point for [Habermas] is that the emancipatory potential of the public sphere was abandoned rather than radicalized and that changing conditions have now made its realization more difficult than ever," a product of "the asymmetrical nature of mass culture" and "the growing impenetration of the state and civil society" (49). Downey and Fenton follow this line of thought, writing that, "a central question for Habermas is whether these groups in civil society can intervene in the mass media public sphere and change the agenda through bringing about a critical process of communication," a process that "can be exceedingly difficult to do in a market-led, mass-mediated system enveloped in its own professional ideologies about what is and is not newsworthy, about who is a credible source of opinion and information and who is not" (188).

Although many have questioned whether the Internet is a public sphere, or how various publics might function within it, there are a number of questions about the roles of media, ownership, and commercialization in digital spaces. Jodi Dean reads digital networks in terms of

communicative capitalism, arguing that, "Rather than actively organized in parties and unions, politics has become a domain of financially mediated and professionalized practices centered on advertising, public relations, and the means of mass communication." In Dean's view, "the deluge of screens and spectacles undermines political opportunity and efficacy for most of the world's people," creating a digital space in which "the standards of a finance and consumption-driven entertainment culture set the very terms of democratic governance today" (102).

As Downey and Fenton note, however, Habermas later updated this position, questioning if, "autonomous public spheres [can] bring conflicts from the periphery to the centre of public life via the mass media in order to generate critical debate amongst a wider public" (188). To consider this, they turn to Negt and Kluge's concept of anti-publicness. Although much of cultural studies has considered how resistance can be fostered in popular activities and consumption, Negt and Kluge see a larger imperative in the transformation of production. "The possibility that production could be organized differently," Downey and Fenton write, "in the interest of the producing/experiencing subjects rather than profit, provides a standard of critique for prevailing products and practices," a position that "most effectively takes the form of counter-productions, of an alternative media practice that intervenes in the contemporary dominant public sphere" (193).

Each of these considerations seems to work within and struggle against the functions of a highly commercialized Web. If Habermas, in his initial Adorno-like reading, saw mass media and consumption as the point of disruption in a critically and discursively organized public sphere, how might we reconcile that viewpoint with today's advertising and consumption-driven Web?

Digital Disruption

Craig Calhoun, in a 2002 talk, offered a strong and ultimately rather accurate vision for publicness and dissent in digital spaces. Considering whether digital technologies could encourage communication that furthers public engagement and political participation rather than simply reifying commercial practices, Calhoun said, "If not, then web-based resistance to power —viruses, hacking, site flooding, and other information technology and web-based strategies for attacking corporations, states, other users—may become more prominent" (18). Ten years later, it is difficult to read Calhoun's remark and not see something of the current moment—especially in the case of hacktivism. The actions of groups like Anonymous seem like a response to a commercially owned Web and a system of power that reifies corporate influence. If, as Dean and (to some degree) Calhoun note, that public participation on the Web has veered strongly toward capitalist goals and toward commercial consumption, hacktivism seems a very specific response to that structure of power.

We might read that relationship, for example, in the 2010 Operation Payback attacks on Paypal and Visa, a moment that highlights the tension between public discourse and commercial influence. When Paypal and Visa cut off donations to Wikileaks, they acted both in support of a U.S. government mandate and in a tacit assertion that the Wikileaks release of private state information was unsanctioned. Because of the limited options for transferring money across digital spaces, the Paypal and Visa actions were powerful, reifying the notion that individual support and discourse is frequently routed through a number of owned channels. New media—like old media—might thus seem to be a system of relationships among major commercial entities rather than a Habermasian public sphere. Although individuals are able to maneuver

within or around those systems, the nature of property, distribution, and ownership separates digital spaces from the coffee houses and salons of the eighteenth century.

This isn't to say, however, that commercialized new media systems are debilitating or that there isn't a means of resisting or challenging them. Downey and Fenton, for example, raise the question of how "autonomous public spheres bring conflicts from the periphery to the centre of public life via the mass media in order to generate critical debate" (188), a concern which echoes both the work of hacktivism and of other activist publics. In particular, Downey and Fenton's question echoes the work of Abbie Hoffman and the Yippies, of the work of spectacle. Similarly, the tactical moves of Anonymous are loosely organized and limited to the momentary, but they generate the same sort of media awareness. This awareness, in turn, has done much to further participation within the group. For example, Gabriella Coleman has noted how the Operation Payback protests led "to one of the most populated channels in the history of Internet Relay Chat with a large infantry of geeks logging on to IRC to watch or lend a helping hand—at one point there were seven thousand people on the main channel" ("Anonymous: From the Lulz").

Most relevant to the concerns of this project, however, are the ways in which these attacks—and the hacktivist public—focus on *systems* rather than *property*. This perspective is important. As I discussed in the previous section, much of the legal conversation about digital spaces has dealt with copyright, permission, and ownership—a conversation that extends into policy and into education. A generalized hacker history, however, instead focuses on networks and systems. The practices of memory discussed in Chapter Three, for example, are means of analyzing networks and creating a collective body of knowledge about those spaces. Although concerns of property and ownership are entangled in that project (specifically, AT&T *owned* the

phone network and many of the documents published about it), the focus of *YIPL* and *TAP* wasn't centered on ownership. Instead, the focus was one of systems and networks, of a question centered on nodes and lines that extend through public space and facilitate discourse.

Likewise, much of the editorial concern across the history of *2600* deals with the regulation of digital spaces by a government that doesn't seem to understand the technologies at work within those spaces. This is another trend echoed in the conversations about SOPA: The real issues, as policy makers see them, are privacy and ownership; the rest should be left to the nerds. With this in mind, how can we develop a more helpful view of technology and authorship? How might we think through the idea of digital publics in an era concerned with a neoliberal approach to regulation and with a market-based focus on property?

Mythinformation, Sleepwalking, and Circulation

To offer a helpful generalization, I would argue that, in my experience, institutional academic responses to technology tend to fall into two camps. The first of these is the uncritical consumption of technology, the commercially idealized future at work in the Clinton-Gore administration's *Getting America's Children Ready for the Twenty-First Century*. This stance connects to Langdon Winner's notion of mythinformation, what Winner saw as a mid-1980s uncritical enthusiasm for technologies. That enthusiasm ultimately supports rampant consumerism but in doing so fails to acknowledge some of the more troubling facets of technological growth. As Winner sees it, mythinformation becomes more a tool for selling computers than a vehicle for any sort of social change, and he sees within computers the potential for reinscribing dangerous social norms, structures, and precedents, and for the erosion of personal liberties and freedoms (105). Mythinformation also, in placing primary value on the

mindless acquisition of technology, underscores the importance of property while downplaying or avoiding the mechanisms at work.

The mythinformation perspective facilitates many of the institutions described earlier in this chapter. Verisign (and ICANN, the corporation tasked with managing the domain name system) can disrupt dot com domains, taking them offline, because a cultural perspective of mythinformation pushes technological reporting and commentary toward issues of consumption —see, for example, the wealth of gadget blogs and the press coverage surrounding the release of an updated operating system. In a culture of mythinformation, the seizure of a bodog.com just doesn't generate the level of awareness that a new version of the iPhone might. Unfortunately, the institutional academic consumption of technology often works in a similar manner: Computer labs are refreshed at quick intervals and students are required to buy compulsory software licenses as these are allegedly the tools that one must know and understand to be competitive in a digital world.

Another stance might be viewed through a lens of what Winner sees as technological sleepwalking. Winner pays specific attention to the relationship between technology and society: How technologies are influenced by social structures and how they then reinscribe those patterns and structures. Artifacts, in Winner's estimation, have political properties, and if we fail to address those properties, we fail to fully understand the political implications of our technologies —we sleepwalk through them.

Following Cynthia Selfe's late-90s critique of technology in the field of Rhetoric and Composition, I would argue that—for too long—much of the field, and much of the technology purchasing public, has been sleepwalking. And this sleepwalking directly connects to the considerations of delivery put forward by Welch, Trimbur, and others: When we de-materialize

texts, whether delivered via print or digital mechanisms, we sleepwalk through them, obscuring the work of economies and social structures. To read public policy through an analogy of Rhetoric and Composition, SOPA is something of a current-traditional approach to digital texts; it focuses on a reductive approach to the forms of infringement without recognizing the complex networks and economies of circulation. And if we continue to sleepwalk through digital technologies, through the spaces of composing and distributing texts, we risk the further encroachment of bills like SOPA.

In my reading, however, narratives of hacking render an alternative. They show a way of tracing, mapping, and exposing systems, and in doing so bring the obscured back to the forefront. In privileging the work of circulation and movement, we might shift away from a cultural stance that centers on property and turn instead toward economies and publics. This, in my estimation, is the current direction of digital spaces—a world that moves toward not just the production of texts, but also to the very tangible means of distributing them. At the moment, this has created something of a distribution culture, a space in which digital authorship is extremely focused on textual inertia—on the *like*, the *tumblr*, the *retweet*.

It is from this perspective that Phyllis Ryder suggests we think beyond deliberation as the key facet of a digital public, writing that "the non-deliberative exchanges on Facebook and Twitter create a sense of capacity and joint mission by relying on another element of public formulation: circulation" (32). Ryder, in assessing the impact of social networking on a local non-profit, arrives at the conclusion that "we can see that a great deal of public formation relies on people's ability not only to *generate* discourse, but also to *circulate* it" (54).

This notion, as I read it, is one of the two major enterprises of the *2600* hacker public. Systems and technologies aren't pieced apart in isolation; instead, technologies are examined and

experimented with and then the results are printed or posted or shared. Circulation is thus a key component of the work that occurs in *2600*. Additionally, that act of circulation is situated in a pedagogical awareness, whether it is to discuss the problems with a phone tax that subsidizes the Vietnam War, a DVD encryption tool that limits playback to one of two commercial operating systems, or a bill that threatens the framework of the Web. In short, the act of exploiting is also one of informing; the tactic both disrupts the strategy and works to generate an awareness of why that disruption is important.

The second enterprise is one that focuses on the spaces—or technologies—in which that discourse circulates. This is the area where our field has a tremendous expertise to offer, and, I think, a major responsibility to uphold. To underscore this point, I want to echo Karl Stolley's call in "The Lo-Fi Manifesto," where he argues that "Discourse posted on the open Web can hardly be considered free if access requires costly software or particular devices" and that "production literacies should aim to prepare digital producers to talk back to and shape the communities and technologies supporting digital discourse." Stolley's focus is mostly on commercial and free/open source software communities, but his argument extends into the space of networks, architecture, and digital infrastructure. If it is our job to prepare students for the production and circulation of texts in digital spaces, we must work to explore and understand those spaces. Only through a focus on the processes and technologies of circulation can we hope to facilitate publics that move beyond consumption—that speak back to and shape the direction of digital discourse.

Conclusion: Rewiring the Master Switch

As I stated in Chapter One, I believe that histories of hacking—as well as histories of other activist, enthusiast, and DIY interactions with networks and media—can help us reconceptualize the ways that technologies factor into scholarly work and curricular standards. However, I also feel that our purview must move beyond those borders, into public work and into policy. Wu's concept of the Cycle reminds us that although technologies shift, patterns of commercialization and regulation are trends that we must study and to which we must respond.

There are many models for this work: publications like *Kairos*, *Computers and Composition Digital Press*, and *The WAC Clearinghouse*, among others. These presses and publications are attempts to build new spaces, to re-situate our traditionally print-driven work in digital contexts. As Cindy Selfe has noted, however, the larger task is difficult: "It is a huge undertaking," she writes, "to re-imagine a form that our profession has lived with for so long" ("Boundaries Redrawn"). And yet the stakes are high. We must start moving past what Selfe calls *book-ness*, but we must also move toward the consideration of circulation that will accompany a digital shift in our work. Such a move requires a close look at the functions of memory and delivery in highly commercialized spaces. Said simply: We must start paying attention.

I also acknowledge that it is easy to make these calls—to assert that the field should make an adjustment of some paramount importance. In closing this dissertation, I acknowledge that the best place to demonstrate this change is within my own work. Drawing from my experience with this dissertation project, I hope to set a trajectory that is centered on publicness, networks, circulation, and media archaeology. I think the practices and narratives outlined in this project can help us to better understand the roles of experimentation and the work of publics in digital spaces—histories through which we can extend and enhance our understanding of authorship and

discourse. The stakes are high, and there is much work to be done. But I, for one, look forward to path ahead.

Works Cited

"2600 Bulletin Board Online." *2600: The Hacker Quarterly* 2.2 (February 1985). Print.

"2600 Writer Indicted." *2600: The Hacker Quarterly* 1.6 (June 1984). Print.

"A Trip to England." *2600: The Hacker Quarterly* 3.8 (August 1986). Print.

"Ahoy!" *2600: The Hacker Quarterly* 1.1 (January 1984). Print.

"Alleged 911 Hacker Pleads Not Guilty." "Alleged 911 Hacker Pleads Not Guilty." *The Washington Times* 19 Feb. 1990. Web. LexisNexis. 18 Sep 2011.

Alderman, John. *Sonic Boom: Napster, MP3, and the New Pioneers of Music*. New York: Basic Books, 2001. Print.

"Apple market value hits $500 billion, where few have gone and none have stayed." Washingtonpost.com. *The Washington Post*, 29 February 2012. Web. 29 February 2012.

Berners-Lee, Tim, and Mark Fischetti. *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor*. San Francisco: HarperSanFrancisco, 1999. Print.

Bianco, Jamie "Skye." "The Digital Humanities Which Is Not One." *Debates in the Digital Humanities*. Ed. Matthew K. Gold. Minneapolis: University of Minnesota Press, 2011. 96-112. Print.

Blagdon, Jeff. "Twitter, Facebook, Google and others take out full-page NYT ad to protest copyright." *Theverge.com*. The Verge, 17 Nov 2011. Web. 6 Feb 2012.

Bolter, Jay David. "Hypertext and the Rhetorical Canons." *Rhetorical Memory and Delivery: Classical Concepts for Contemporary Communication and Composition*. Ed. John Frederick Reynolds. Hillsdale, NJ: Lawrence Erlbaum Associates: 1993. 97-111. Print.

Brooke, Collin Gifford. *Lingua Fracta: Towards a Rhetoric of New Media*. Cresskill, NJ: Hampton Press, 2009. Print.

Bodroghkozy, Aniko. *Groove Tube: Sixties Television and the Youth Rebellion*. Durham: Duke University Press, 2001. Print.

Burgess, John. "AT&T Long-Distance Lines Fail; Software Suspected." *The Washington Post* 16 Jan. 1990. Web. LexisNexis. 18 Sep 2011.

Burk, Dan L. "Materiality and Textuality in Digital Rights Management." *Computers and Composition* 27.3 (2010): 225–234. Print.

Bush, Vannevar. "As we may think." *Interactions* 3.2 (1996): 35–46. Web.

Calhoun, Craig. "Information technology and the international public sphere." *Shaping the Network Society: The New Role of Civil Society in Cyberspace*. Eds. Douglas Schuler and Peter Day. Cambridge: The MIT Press, 2004. 229-251. Print.

Carruthers, Mary. *The Book of Memory: A Study of Memory in Medieval Culture*. Cambridge: Cambridge University Press, 1990. Print.

Cohen, Phil. "Subcultural conflict and working-class community." *Culture, Media, Language*. Eds. Stuart Hall, Dorothy Hobson, Andrew Lowe, and Paul Willis. New York: Routledge, 1996. Print.

Coleman, E. Gabriella. "Anonymous: From the Lulz to the Collective Action." *The New Everyday MediaCommons: A Digital Scholarly Network*. 06 April 2011. Web. 06 April 2011.

Coleman, Gabriella and Michael Ralph. "Is It A Crime? The Transgressive Politics of Hacking in Anonymous." *OWNI.eu*, News, Augmented. 29 Sep 2011. Web. 30 Sep 2011.

"Commentary: The Treat To Us All." *2600: The Hacker Quarterly* 2.8 (August, 1985). Print.

Connors, Robert J. "Actio: A Rhetoric of Written Delivery (Iteration Two)." Rhetorical Memory and Delivery: *Classical Concepts for Contemporary Composition and Communication*. Ed. John Frederick Reynolds. Hillsdale, NJ: Lawrence Erlbaum Associates: 1993. 65-77. Print.

Connors, Robert J. "Dreams and Play: Historical Method and Methodology." *Methods and Methodology in Composition Research*. Eds. Gesa Kirsch and Patricia A. Sullivan. Carbondale: Southern Illinois University Press, 1992. Print.

Corbett, Edward P.J. and Robert J. Connors. *Classical Rhetoric for the Modern Student*. Oxford: Oxford University Press, 1999. Print.

de Certeau, Michel. *The Practices of Everyday Life*. Berkeley: University of California Press, 1984. Print.

Dean, Jodi. "Why the Net Is Not a Public Sphere." *Constellations* 10.1 (2003): 95–112. Print.

Denning, Dorothy E. "The United States vs. Craig Neidorf." *Communications of the ACM* 34.3 (1991): 23–43. Print.

DeSantis, Nick. "E-Textbook Vendor Sues Publisher for Ending Licensing Agreement." *Chronicle.com* The Chronicle of Higher Education, 22 February 2012. Web. 22 February 2012.

DeVoss, Dànielle Nicole, and James E. Porter. "Why Napster Matters to Writing: Filesharing as a New Ethic of Digital Delivery." *Computers and Composition* 23.2 (2006): 178–210. Print.

Digital Millennium Copyright Act. Pub. L. 105-304. 112 Stat. 2860. 28 Oct 1998. Washington: Library of Congress THOMAS, 2012. Web. 18 Sep 2011.

Downey, John, and Natalie Fenton. "New Media, Counter Publicity and the Public Sphere." *New Media & Society* 5.2 (2003): 185. Print.

"DVD Encryption Cracked." *2600.com*. 12 Nov 1999. Web. 18 Sep 2011.

"For Your Own Good." *2600: The Hacker Quarterly* 7.1 (Spring 1990). Print.

"Free Phone Calls." *2600: The Hacker Quarterly* 7.2 (Summer 1990). Print.

Gaillet, Lynee Lewis. "Archival Survival: Navigating Historical Research." *Working in the archives: practical research methods for rhetoric and composition*. Ed. Alexis E. Ramsey. Carbondale: Southern Illinois University Press, 2010. 28-39. Print.

Gates, Bill. "DigiBarn Newsletters: Bill Gates' Open Letter to Hobbyists in Homebrew Club Newsletter Vol 2, Issue 1 (Feb 3, 1976)." *digibarn.com*. Web. 7 Nov 2011.

Gottfried, Jonathan. "Don't bet on 'Linsanity': US seizes online gambling domain over sports wagers." *Arstechnica.com* Law & Disorder: Tech law and policy in the digital age, 2 March 2012. Web. 2 March 2012.

"Hackers in Jail." *2600: The Hacker Quarterly* 6.1 (Spring 1989). Print.

"'Hackers' Score a New Pentagon Hit." *U.S. News & World Report* 29 July 1985. LexisNexis. Web. 18 Sep 2011.

Hacking Ma Bell: The First Hacker Newsletter - Youth International Party Line, The First Three Years. Warcry Communications, 2010. Print.

Hall, Stuart. "Cultural Studies and the Centre: some problematics and problems." *Culture, Media, Language*. Eds. Stuart Hall, Dorothy Hobson, Andrew Lowe, and Paul Willis. New York: Routledge, 1996. Print.

Horner, Winifred Bryan. "Reinventing Memory and Delivery." *Inventing a Discipline: Rhetoric Scholarship in Honor of Richard E. Young*. Ed. Maureen Daly Goggin. Urbana, IL: NCTE, 2000. pp173-184. Print.

"Introduction." Phrack 1 (1985). Web. *Phrack.org*. 23 Sep 2011.

Joselit, David. "Yippie Pop: Abbie Hoffman, Andy Warhol, and Sixties Media Politics." *Grey Room* (2002): 62–79. Print.

Kelty, Christopher. *Two Bits: The Cultural Significance of Free Software*. Durham: Duke University Press, 2008. Print.

Kirschenbaum, Matthew. *Mechanisms: New Media and the Forensic Imagination*. Cambridge, MA: The MIT Press, 2008. Print.

Kravets, David. "Feds Shutter Megaupload, Arrest Executives." *Wired.com* Threat Level: Privacy, Crime and Security Online, 19 January 2012. Web. 19 January 2012.

Lessig, Lawrence. *Code: Version 2.0*. New York: Basic Books, 2006. Print.

Lessig, Lawrence. *The Future of Ideas: The Fate of the Commons in a Connected World*. New York: Random House, 2001. Print.

Levy, Steven. *Hackers: Heroes of the Computer Revolution*. Sebastopol, CA: O'Reilly Media, 2010. Print.

Lievrouw, Leah A. *Alternative and Activist New Media*. Malden, MA: Polity Press, 2011. Print.

Logie, John. *Peers, Pirates, and Persuasion*. West Lafayette, IN: Parlor Press, 2006. Print.

Losh, Elizabeth. "Hacktivism and the Humanities." *Debates in the Digital Humanities*. Ed. Matthew K. Gold. Minneapolis: University of Minnesota Press, 2011. 161-186. Print.

Lunsford, Andrea A. "Writing, Technologies, and the Fifth Canon." *Computers and Composition* 23.2 (2006): 169–177. Web. 16 June 2011.

Mahony, Patrick. "McLuhan in the Light of Classical Rhetoric." *College Composition and Communication* 20.1 (1969): pp.12-17. Print.

Mathieu, Paula, and Diana George. "Not Going It Alone: Public Writing, Independent Media, and the Circulation of Homeless Advocacy." *College Composition and Communication* 61.1 (2009): 130-149. Print.

"Message Sent." *2600: The Hacker Quarterly* 16.1 (Spring 1998). Print.

"More about SOPA and PIPA." *Google.com* End Piracy, Not Liberty. Web. 6 Feb 2012. <http://www.google.com/landing/takeaction/sopa-pipa/>

"More on Trashing: What to look for, how to act, where to go." *2600: The Hacker Quarterly* 1.9 (September 1984). Print.

"Moving Satellites Right Up There in the Blue... What Was Really Going On?" *2600: The Hacker Quarterly* 2.8 (August 1985). Print.

"Negative Feedback." *2600: The Hacker Quarterly* 7.2 (Summer 1990). Print.

Nelson, Ted. "Computer Lib/Dream Machines." *The New Media Reader*. Ed. Noah Wardrip-Fruin and Nick Montfort. Cambridge, MA: The MIT Press, 2003. 303-331. Print.

"New Readers!" *The Youth International Party Line* 12 (August 1972): n. pag. Artofhacking.org. Web. 18 Feb 2009.

"No Fancy Excuses." *Technological American Party* 21 (August-September 1973): n. pag. Artofhacking.org. Web. 18 Feb 2009.

Oakes, Kaya. *Slanted and Enchanted: The Evolution of Indie Culture*. New York: Henry Holt and Company, 2009. Print.

Orth, Maureen. "For Whom Ma Bell Tolls Not." *The Los Angeles Times* 31 October 1971. ProQuest Historical Newspapers. Web. 18 Sep 2011.

Porter, James E. "Recovering Delivery for Digital Rhetoric." *Computers and Composition* 26.4 (2009): 207–224. Web. 16 June 2011.

Prior, Paul, et al. "Re-situating and Re-mediating the Canons: A Cultural-Historical Remapping of Rhetorical Activity." *Kairos: A Journal of Rhetoric, Technology, and Pedagogy* 11.3 (2007): n. pag. Web. 6 June 2011.

"Private Sector Returning." *2600: The Hacker Quarterly* 3.1 (January 1986). Print.

"Prosecutor Says Juveniles Used Computers to Access Defense Information." *The Associated Press* 16 July 1985. LexisNexis. Web. 18 Sep 2011.

Reyman, Jessica. *The Rhetoric of Intellectual Property: Copyright Law and the Regulation of Digital Culture*. New York: Routledge, 2010. Print.

Rife, Martine Courant. "Why Kairos matters to writing: A reflection on its intellectual property conversation and developing law during the last ten years." *Kairos: A Journal of Rhetoric, Technology, and Pedagogy* 11.1 (2006): n. pag. Web. 20 Feb 2012.

Rosenbaum, Ron. "Secrets of the Little Blue Box." *Harpers* Oct. 1971: 117–125, 222–226. Print.

Rosenberg, Scott. *Dreaming in Code: two dozen programmers, three years, 4,732 bugs, and one quest for transcendent software*. New York: Crown Publishers, 2007. Print.

Ryder, Phyllis. "Public 2.0. Social Networking, Nonprofits, and the Rhetorical Work of Public Making." *Reflections* 10.1 (2010): 29–56. Print.

Schoen, Seth. "DeCSS Haiku." *Gallery of CSS Descramblers*. 23 February 2001. Web. 18 Sep 2011.

"SEIZED! 2600 Bulletin Board is Implicated in Raid on Jersey Hackers." *2600: The Hacker Quarterly* 2.8 (August 1985). Print.

Selfe, Cynthia L. "Technology and Literacy: a Story About the Perils of Not Paying Attention." *College Composition and Communication* 50.3, (1999): 411–436. Print.

Selfe, Cynthia L. "Boundaries Redrawn: Escaping the Intellectual Gravity of Book-ness." *The Scholar Electric* Computers and Composition Digital Press. 11 May 2011. Web. 11 May 2011.

Sennett, Richard. *The Craftsman*. New Haven: Yale University Press, 2008. Print.

Sherman, Cary H. "What Wikipedia Won't Tell You." *The New York Times* 7 Feb 2012. Web. 7 Feb 2012.

"Sherwood Forest Shut Down by Secret Service: An All Too Familiar Story." *2600: The Hacker Quarterly* 2.6 (June 1985). Print.

"Some Thoughts on Garbage Picking." *2600: The Hacker Quarterly* 1.2 (February 1984). Print.

Sony Corp. of America v. Universal City Studios, Inc. No. 81-1687. Supreme Court of the U.S. 17 January 1984. Web. 22 February 2012.

"Statement of Purpose." *The Youth International Party Line* 3 (August 1971): n. pag. Artofhacking.org. Web. 18 Feb 2009.

"Statement of Purpose." *The Youth International Party Line* 6 (November 1971): n. pag. Artofhacking.org. Web. 18 Feb 2009.

Sterling, Bruce. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. New York: Bantam, 1992. Print.

Stolley, Karl. "The Lo-Fi Manifesto." *Kairos: A Journal of Rhetoric, Technology, and Pedagogy* 12.3 (2008): n. pag. Web. 20 Feb 2012.

"TAP: The Legend Is Dead." *2600: The Hacker Quarterly* 4.1 (January 1987). Print.

"TAP/YIPL 40th Anniversary." *2600 San Francisco Weblog*. 2600sf.com: Web. 16 Dec 2011.

Tapscott, Don and Anthony D. Williams. *Wikinomics: How Mass Collaboration Changes Everything*. New York: Portfolio, 2008. Print.

"Teen-Agers Accused of Breaking Into Pentagon Computer Program." *The Associated Press* 18 July 1985. Web. LexisNexis. 18 Sep 2011.

Tehranian, John. *Infringement Nation: Copyright 2.0 and You*. New York: Oxford University Press, 2011. Print.

"The Day The Phone System Really Died." *2600: The Hacker Quarterly* 6.4 (Winter 1989-90). Print.

"The Dumbest Rip-Off." *The Youth International Party Line* 2 (July 1971): n. pag. Artofhacking.org. Web. 18 Feb 2009.

"The Jargon File." *Catb.org/jargon*. Web. 18 Sep 2011.

"The Neidorf/Phrack Trial: Day by Day." *2600: The Hacker Quarterly* 7.2 (Summer, 1990). Print.

"The New TAP." *2600: The Hacker Quarterly* 6.2 (Summer 1989). Print.

"The Next Chapter." *2600: The Hacker Quarterly* 17.1 (Spring 2000). Print.

"The Tweets Must Flow." *Twitter.com*. Twitter, 28 January 2011. Web. 28 January 2011.

"The Youth International Party Line's First Issue." *The Youth International Party Line* 1 (June 1971): n. pag. Artofhacking.org. Web. 18 Feb 2009.

Thomas, Douglas. *Hacker Culture*. Minneapolis: University of Minnesota Press, 2002. Print.

Touretzky, David. *Gallery of CSS Descramblers*. 13 Feb 2008. Web. 18 Sep 2011.

"Trashing: America's Source for Information." *2600: The Hacker Quarterly* 3.10 (October 1986). Print.

Trimbur, John. "Composition and the Circulation of Writing." *College Composition and Communication* 52.2 (2000): 188-219. Print.

Tsukayama, Hayley. "SOPA action delayed in House until 'wider consensus'." *The Washington Post*. 20 Jan 2012. Web. 20 Jan 2012.

Universal City Studios Inc. v. Shawn C. Reimerdes. No. 00-0277. United States District Court Southern District of New York. 17 Aug 2000. Web. 18 Sep 2011.

United States. Cong. House. Committee on the Judiciary. Markup of H.R. 3261, Stop Online Piracy Act. 112th Congress. Washington: House Judiciary Committee. 16 Dec 2012. Web. 6 Feb 2012.

United States. Cong. House. *Stop Online Piracy Act*. 112th Congress. HR 3261. Washington: Library of Congress THOMAS, 2012. Web. 6 Feb 2012.

"Up, Up, and Away." *Twitter.com*. Twitter, 16 June 2009. Web. 16 June 2009.

Vance, Ashlee and Miguel Helft. "Hackers Give Web Companies a Test of Free Speech." *The New York Times* 8 Dec 2010. Web. 9 Dec 2010.

"War Tax Resistance." *The Youth International Party Line* 1 (June 1971): n. pag. Artofhacking.org. Web. 18 Feb 2009.

Wark, McKenzie. *A Hacker Manifesto*. Cambridge, MA: Harvard University Press, 2004. Print.

Warner, Michael. *Publics and Counterpublics*. New York: Zone Books, 2005. Print.

Welch, Kathleen E. *Electric Rhetoric: Classical Rhetoric, Oralism, and a New Literacy*. Cambridge, MA: The MIT Press, 1999. Print.

Welch, Kathleen E. "Electrifying Classical Rhetoric: Ancient Media, Modern Technology, and Contemporary Composition." Jacweb.org. Web.

Wiener, Norbert. "Men, Machines, and the World About." *The New Media Reader*. Ed. Noah Wardrip-Fruin and Nick Montfort. Cambridge, MA: The MIT Press, 2003. 65-72. Print.

"Wikipedia:SOPA Initiative." *Wikipedia: The Free Encyclopedia*. Wikimedia Foundation, Inc. 30 Jan 2012. Web. 06 Feb 2012.

Winner, Langdon. *The Whale and the Reactor: A Search for Limits in an Age of High Technology*. Chicago: University of Chicago Press, 1986. Print.

Woodson, Linda. *A Handbook of Modern Rhetorical Terms*. Urbana, IL: NCTE, 1979. Print.

Wu, Tim. *The master switch: The Rise and Fall of Information Empires*. New York: Knopf, 2010. Print.

Appendix A: Image Permissions

Figure 1 [Fair Use]
"Screenshot of the January 18, 2012 Wikipedia Blackout." *Wikimedia Commons*. http://en.wikipedia.org/wiki/File:History_Wikipedia_English_SOPA_2012_Blackout2.jpg. Retrieved on 22 January 2012. Fair Use determination attached.

Figure 2 [Creative Commons Licensed]
"Screenshot of a website defacement attack." *Cyber War News*. http://www.cyberwarnews.info/2012/01/14/asus-websites-hacked/ Retrieved on January 14, 2012. Used with permission via a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 License.

Figure 3 [Creative Commons Licensed]
"2nd Anniversary 13." *Flickr*. http://www.flickr.com/photos/anonymous9000/4280254856/ Retrieved on 16 December 2011. Used with permission via a Creative Commons Attribution 2.0 Generic License.

Figure 4 [Public Domain]
"The Anonymous Flag." *Wikimedia Commons*. http://commons.wikimedia.org/wiki/File:Anonymous_Flag.svg Retrieved on 16 December 2011. Works in the MediaCommons have been released to the public domain.

Figure 5 [Fair Use]
"Lulz Security." *Wikipedia*. http://en.wikipedia.org/wiki/File:Lulz_Security.svg Retrieved on 16 December 2011. Fair Use determination attached.

Virginia Tech ETD Fair Use Analysis Results

This is not a replacement for professional legal advice but an effort to assist you in making a sound decision.

Name: Timothy Alan Lockridge

Description of item under review for fair use: Figure 1. "Screenshot of the January 18, 2012 Wikipedia Blackout." Wikimedia Commons. http://en.wikipedia.org/wiki/File:History_Wikipedia_English_SOPA_2012_Blackout2.jpg. Retrieved on 22 January 2012.

Report generated on: 04-05-2012 at : 14:25:23

Based on the information you provided:

Factor 1

Your consideration of the purpose and character of your use of the copyright work weighs: ***in favor of fair use***

Factor 2

Your consideration of the nature of the copyrighted work you used weighs: ***against fair use***

Factor 3

Your consideration of the amount and substantiality of your use of the copyrighted work weighs: ***in favor of fair use***

Factor 4

Your consideration of the effect or potential effect on the market after your use of the copyrighted work weighs: ***in favor of fair use***

Based on the information you provided, your use of the copyrighted work weighs: *in favor of fair use*

Virginia Tech ETD Fair Use Analysis Results

This is not a replacement for professional legal advice but an effort to assist you in making a sound decision.

Name: Timothy Alan Lockridge

Description of item under review for fair use: Figure 5 “Lulz Security.” Wikipedia. http://en.wikipedia.org/wiki/File:Lulz_Security.svg Retrieved on 16 December 2011. Fair Use determination attached.

Report generated on: 04-05-2012 at : 14:30:54

Based on the information you provided:

Factor 1

Your consideration of the purpose and character of your use of the copyright work weighs: ***in favor of fair use***

Factor 2

Your consideration of the nature of the copyrighted work you used weighs: ***against fair use***

Factor 3

Your consideration of the amount and substantiality of your use of the copyrighted work weighs: ***in favor of fair use***

Factor 4

Your consideration of the effect or potential effect on the market after your use of the copyrighted work weighs: ***in favor of fair use***

Based on the information you provided, your use of the copyrighted work weighs: *in favor of fair use*