The Pennsylvania State University

The Graduate School

Department of Communication Arts and Sciences

DEMOCRACY AND THE HACKER MOVEMENT:

INFORMATION TECHNOLOGIES AND POLITICAL ACTION

A Thesis in

Communication Arts and Sciences

by

Brett Lance Lunceford

Submitted in Partial Fulfillment
of the Requirements
for the Degree of

Doctor of Philosophy

December 2006

The thesis of Brett Lance Lunceford was reviewed and approved* by the following:

Thomas W. Benson
Edwin Erle Sparks Professor of Rhetoric
Thesis Advisor
Chair of Committee

J. Michael Hogan
Professor of Communication Arts and Sciences

Stephen H. Browne
Professor of Communication Arts and Sciences

Jorge Reina Schement
Distinguished Professor of Communications

James P. Dillard
Professor of Communication Arts and Sciences
Head of the Department of Communication Arts and Sciences

*Signatures are on file in the Graduate School

ABSTRACT

In order to understand how technology may influence democratic practice, it is necessary to understand the values of those who are creating and shaping technology because those who create technology instill within those technologies particular values. Hackers comprise one group that has a significant role in the creation and shaping of technology. As the United States moves closer toward becoming an information society, the hacker is a figure that embodies both peril and promise. If technology is to revolutionize democratic practice, citizens must begin to use technology in revolutionary ways. Hackers, through acts of "hacktivism" (politically motivated hacking), are using technology in inventive ways for political ends.

Living in an information society places constraints upon democratic practice. Because hackers are actively creating and shaping these constraints, they are likely to successfully negotiate these constraints. Hackers have evolved from a loose collective to a politically oriented social movement with a strong collective identity. Hackers are using their skills for political ends through acts of hacktivism. These politically motivated hacks provide clues concerning the prospects for a technologically enhanced democratic society.

Core tenets of hacker collective identity are embedded within hacker texts, manifestoes, and hacked Web pages. "The Conscience of a Hacker," also known as the hacker manifesto, provided a rallying cry for the nascent movement and began to articulate a collective identity for hackers. Instances of hacktivism demonstrate how this collective identity is enacted. An examination of a politically motivated hack of the *New*

York Times website reveals that the action served more to reinforce hacker collective identity and to confirm in/out group distinctions between hackers and the rest of society than to incite political action or foster support for their cause, fulfilling what Richard Gregg calls the “ego function of protest rhetoric.”

Because hacker collective identity is at odds with essential attributes of democracy, hackers are not likely to create a more democratic society. This conclusion casts doubt on the potential for new technologies to revolutionize democratic practice but there is still hope for a technologically enhanced form of democracy. The greatest potential for technology to positively influence democratic practice can be found in citizens using technology in unintended and inventive ways rather than through hackers and acts of hacktivism.

TABLE OF CONTENTS

LIST OF FIGURES vii

ACKNOWLEDGEMENTS viii

Chapter 1 Social Movements: It's Not Just Marching Anymore 1

- Questions of Definition: What is a Social Movement 5
- The New Social Movement Approach 10
- Outline of Chapters 13

Chapter 2 Democratic Practice in an Information Society 16

- What is Democracy? 18
  - Voice 19
  - Citizenship 23
  - Limitation of Governmental Power 26
- What Does an Information Society Look Like? 30
  - The Commodification of Information in an Information Society 33
  - Access to Information Technologies 39
  - The Interconnection of Individuals and Institutions in an Information Society 42
  - Identity and Citizenship in an Information Society 49
- Protest and Democracy in an Information Society 57

Chapter 3 Building a Hacker Collective Identity 63

- The Rhetorical Construction of the Hacker as Terrorist 67
  - The Hacker and the Creation of the National Information Infrastructure 69
  - Information Society / Panoptic Society 70
  - From Nerd to Nemesis: Constructing the Hacker as Terrorist 76
  - The Consequences of Constructing the Hacker as Terrorist 86
- The Creation of a Hacker Movement 92
  - In the Beginning There Was *Phrack* 94
  - Operation Sundevil and the Galvanization of the Hacker Movement 102
  - Kevin Mitnick and the Myth of the Superhacker 107
  - The Death of *Phrack* 115
- Entering the World of the Hacker: The Hacker Manifesto 118
  - A Shift in the Text 141
  - What Does the Hacker Manifesto Reveal About Hacker Collective Identity? 158
- Conclusion 163

Chapter 4 Hacktivism as Rhetorical Action 164

What is Hacktivism? 165
How is Hacktivism Done? 170
Social Engineering 171
Website Defacement 172
Email Bombs 173
Electronic Sit-ins / Denial of Service Attacks 173
What's New and Different about Hacktivism? 175
A Brief History of Hacktivism 175
The Question of Means and Ends in Hacktivism 179
Limitations of Traditional Protest Activity 191
Hacktivism Versus Culture Jamming 195
Case Study: The New York Times Hack 199
Interpretations of the Action 220
Ego Function of Protest Rhetoric 230
Hacktivism and Democracy 243

Chapter 5 Conclusion: What are the Prospects for a Technologically Mediated Democracy? 246

Identity in an Information Society and Identity as Citizen 248
The Creators of Technology and Their Values: What Kind of Democracy Would Hackers Create? 255
New Means of Protest 260
The Potential Efficacy of Hacktivism 268
The Potential for Democratic Practice in an Information Society 272

Bibliography 277

LIST OF FIGURES

Figure 1: Hacking For Girliez Logo 202

Figure 2: HFG Certified! Logo 202

Figure 3: Best Viewed with VI 205

Figure 4: Get Hacked Now! HFG 205

ACKNOWLEDGEMENTS

I am a member of the last generation that had a choice as to whether or not we would go online. By 1987 many of my friends had gone online, having discovered the joys of BBS systems. They told me that I should get online too, that I would love it. With a perception that extended far beyond what I should have possessed as a fifteen-year-old, I declined—not because I did not want to, but because I knew that they were right. I knew that once I entered, I would never return—and I haven't. I write this to remind the reader that the online world has not always existed and to remind myself that the digital realm has not always been an essential part of my life.

As with any dissertation, this work was not done in isolation. I am grateful to my dissertation committee—Thomas W. Benson, J. Michael Hogan, Stephen H. Browne, and Jorge Reina Schement—for their counsel as this project evolved. Each has provided valuable insights along the way and this work is much richer because of it. Professor Benson has a way of finding the one loose thread that unravels the entire argument—which was exactly what I needed in an advisor. I appreciate his thoughtful criticism and many hours of discussion concerning this work. I must also acknowledge Professor Hogan's efforts in shaping me from the writer that I was to the writer that I have become today. My colleagues have also been helpful as I have labored on this project, especially Michael Tumolo, Jennifer Biedendorf, Jill Weber, and Jessica Sheffield.

My family has helped me along the way, even when they had no idea what I was talking about (well, Shane always understood). My father would have been especially proud to see me get to this point. My brother Shane was always there to listen to my

ideas, providing technical knowledge and information that has greatly enriched this work. But the person who has had to endure my ramblings more than anyone is my lovely wife, Rebecca. I am truly blessed to have someone so loving and supportive of my work. I promise that it will not always be like this! If I had to dedicate this work to anyone, it would be to Shane and Kim's children, Nathan and Corbin. They are the future—may their world be more democratic than mine.

Above all, I acknowledge the hand of God in this work.

Parts of this work have been generously supported by a grant, residency, and course release provided by the Institute for the Arts and Humanities at the Pennsylvania State University. I am grateful for Loyd Blankenship's (The Mentor) permission to use the text of "The Conscience of a Hacker" and his willingness to discuss the text with me.

Chapter 1

Social Movements: It's Not Just Marching Anymore

This work examines how new forms of political activism—specifically hacktivism, or politically motivated hacking—may influence democratic practice in an information society.[1] The potential effects of new communication technologies on democracy have been widely debated. On one side are those who argue that the Internet will improve democracy and that greater involvement in digital communities will translate into stronger involvement in "real life" communities.[2] Jorge Reina Schement, for example, argues that closing the gap between those with access and those without will "breathe life into the economic, political, and social life of a democratic society that embraces all."[3] Conversely, Cass Sunstein suggests that the Internet may diminish democracy by allowing users to avoid exposure to opposing viewpoints, lessening civic engagement.[4] It is also possible to avoid any civic issues at all if the Internet becomes little more than an online strip mall, as Jeff Johnson argues.[5] Of course there is also some

---

[1] Although there are many definitions of hacking, I use the term to mean the unauthorized access of computer systems.

[2] See Jerry Berman and Daniel J Weitzner, "Technology and Democracy," *Social Research* 64, no. 3 (1997): 1313-19; Brock N Meeks, "Better Democracy through Technology," *Communications of the ACM* 40, no. 2 (1997): 75-78; David Schlosberg and John S. Dryzek, "Digital Democracy: Authentic or Virtual?" *Organization & Environment* 15, no. 3 (2002): 332-35.

[3] Jorge Reina Schement, "Democracy Digitized," *Broadcasting & Cable* 131, no. 15 (2001): 77.

[4] See Cass R. Sunstein, *Republic.Com* (Princeton, NJ: Princeton University Press, 2001).

[5] Jeff Johnson, "The Information Superhighway: A Worst-Case Scenario," *Communications of the ACM* 39, no. 2 (1996): 15-17.

middle ground between these two extremes, which seems more realistic.[6] One way to begin answering questions about the influence of new communication technologies on civic engagement and deliberative democracy is to examine how new media are being employed by social movements.

Opinions concerning social movement uses of new technologies seem to fluctuate between extreme optimism and the belief that nothing much has changed and that technology only reinforces entrenched ways of doing things.[7] Sylvia Tesh explains that even though new communication technologies such as the Internet allow for more rapid dissemination of information and a greater degree of interaction at a lower cost, it seems that social movements have not realized this potential and are doing little to use these technologies as a way to foster involvement.[8]

Some scholars have begun to catalogue the ways in which social movements are using new technologies in innovative ways. For example, Richard Kahn and Douglas Kellner discuss how social movements use cell phones, personal digital assistants (PDAs), global positioning systems (GPS), laptops, wireless internet access, and actions such as wardriving and blogging.[9] They cite a specific example of an activist named Remedy that used wireless internet and a laptop to create and update her weblog as she

---

[6] Even Jacques Ellul, who leans toward a rather bleak form of technological determinism, explains that if members of society can demystify technology, there is potential to make it work for democracy. See Jacques Ellul, "Technology and Democracy," in *Democracy in a Technological Society*, ed. Langdon Winner, 35-50 (Dordrecht: Kluwer, 1992).

[7] See Mario Diani, "Social Movement Networks Virtual and Real," *Information Communication & Society* 3, no. 3 (2000): 386-401; Richard Kahn and Douglas Kellner, "New Media and Internet Activism: From the 'Battle of Seattle' to Blogging," *New Media & Society* 6, no. 1 (2004): 87-95.

[8] Sylvia N Tesh, "The Internet and the Grass Roots," *Organization & Environment* 15, no. 3 (2002): 336-39.

[9] Wardriving is searching for unsecured wireless networks that one can freely access. Blogging is keeping an online journal, or weblog, as an individual or on behalf of an organization.

sat 300 feet up in a redwood.[10] Jenine Dallal provides another example of how social movements have integrated new technology into their activities, describing how Hizballah has adapted their messages specifically for the Internet and how they have managed their image both through linking and as participants in a digital war against Israeli hackers.[11] Even anarchists are organizing and using the internet for damage control when they receive unfavorable news coverage related to anti-globalization protest actions.[12]

New communication technologies not only allow social movements to enact new strategies for participation, but also help form a populace that can participate in new ways. John Clark and Nuno Themudo explain that "the Internet has allowed previously opaque processes of intergovernmental negotiations to become demystified and accessible. Citizens now feel quite well informed and empowered to intervene in these processes. Dot causes provide the opportunity."[13] But the populace is not just more well informed. Sherry Turkle argues that the Internet has helped to shape a new consciousness in its users, a new way of thinking and being.[14] According to Turkle, there is no longer a

---

[10] Kahn and Kellner, "New Media and Internet Activism: From the 'Battle of Seattle' to Blogging," 93.

[11] Jenine Abboushi Dallal, "Hizballah's Virtual Civil Society.," *Television & New Media* 2, no. 4 (2001): 367-72.

[12] Lynn Owens and L. Kendall Palmer, "Making the News: Anarchist Counter-Public Relations on the World Wide Web," *Critical Studies in Media Communication* 20, no. 4 (2003): 335-61.

[13] John Clark and Nuno Themudo, "The Age of Protest: Internet-Based 'Dot-Causes' and the 'Anti-Globalization' Movement," in *Globalizing Civic Engagement: Civil Society and Transnational Action*, ed. John Clark, 109-26 (London: Earthscan Publications, 2003), 117.

[14] Turkle makes a similar claim to that proposed by scholars such as Walter Ong, Jack Goody, and Eric Havelock that the advent of writing changed how people think. Ong, Havelock, and Goody all argue that the advent of writing and literacy allowed for linear, abstract thought. Ong argues that oral cultures were rooted in the physical lifeworld and that members of these cultures were unable to see things in terms of general, abstract forms. Turkle argues that users of the Internet now no longer differentiate between the real and the virtual, that they are essentially different, yet equal facets of the same reality. Moreover, she illustrates the tension between reality and the potential of false representation online that makes this

split between reality and virtual reality for users of the Internet—action in the real world and action in the virtual world are seen as different, yet roughly equal kinds of action by the actor.[15] Thus, not only have social movements changed, but the supporters themselves have changed.

It is clear that social movements are beginning to use technology in inventive ways, which bodes well for the possibility of a technologically enhanced democracy. If technology is to revolutionize democracy, we as a society must begin to use technology in revolutionary ways. Hackers are one such group and thus comprise an ideal group to study in examining the question of how technology can be used in revolutionary ways for political ends. In common usage, the term hacker defines one who illegally gains unauthorized access to computer systems. Although hackers may engage in illegal activities, this is an impoverished view of hacker identity. To be a hacker is to be a pioneer, using the technology in ways that others had not anticipated or imagined. Hackers have created a culture based on thinking outside of the box. Hackers are not only users of technology, but creators as well. Many hackers work in the technology sector

---

problematic. One issue for Turkle is the idea that individuals can have a persona that, although not physically accurate, such as a man posing as a woman online, can be as real to that person as their "real" identity. See Sherry Turkle, *Life on the Screen: Identity in the Age of the Internet* (New York: Simon & Schuster, 1995). For discussion on the change in consciousness wrought by the advent of literacy, see Jack Goody, *The Domestication of the Savage Mind, Themes in the Social Sciences* (Cambridge: Cambridge University Press, 1977); Jack Goody, *The Power of the Written Tradition* (Washington, DC: Smithsonian Institution Press, 2000); Eric Alfred Havelock, *The Muse Learns to Write: Reflections on Orality and Literacy from Antiquity to the Present* (New Haven, CT: Yale University Press, 1986); Eric Alfred Havelock, *Preface to Plato* (Cambridge: Belknap Press, 1963); Walter J. Ong, *Orality and Literacy: The Technologizing of the Word* (London: Methuen, 1982).

[15] For an excellent discussion of the perceived reality of virtual reality, see Julian Dibbell, "A Rape in Cyberspace," in *Cyberreader*, ed. Victor J. Vitanza, 454-72 (Boston: Allyn and Bacon, 1999); Turkle, *Life on the Screen: Identity in the Age of the Internet.*

and have an active role in shaping the hardware and software that we use. They endow these technological artifacts with the values of their collective identity.

Hackers are using technology to forward political ends, often in transgressive and inventive ways. They seem to have evolved from a loose collective into a social movement. Although there is dissent even among hackers as to whether or not they form a social movement or simply a community, it is clear that hackers have developed a strong collective identity, which makes the new social movement perspective useful in studying them. But what makes a group of individual hackers a social movement rather than simply a group or a community of hackers? When considering social movement rhetoric, it is important to understand just what constitutes a social movement. Rhetorical scholars and sociologists both suggest possible ways to define social movements.

Questions of Definition: What is a Social Movement

Although social movement rhetoric had been studied as early as 1940, the civil rights movement rekindled scholarly attention to social movements.[16] Rhetorical scholars during this time borrowed heavily from sociological theories of social movements, but they expressed a creeping sense of discontent with these constructs. Robert Cathcart argued that sociological definitions of social movements are "*ill-suited* to the formulation

---

[16] For early research on social movement rhetoric, see S. Judson Crandell, "The Beginnings of a Methodology for Social Control Studies in Public Address," *Quarterly Journal of Speech* 33, no. 1 (1947): 36-39; Leland M. Griffin, "The Rhetoric of Historical Movements," *Quarterly Journal of Speech* 38, no. 2 (1952): 184-88; Leland M. Griffin, "The Rhetorical Structure of the Antimasonic Movement," in *The Rhetorical Idiom*, ed. Donald Bryant, 145-60 (Ithaca, NY: Cornell University Press, 1958); Robert G. Gunderson, "'The Calamity Howlers,'" *Quarterly Journal of Speech* 26, no. 3 (1940): 401-11.

of an adequate theory of the rhetoric of movements" and that a rhetorical definition of social movements "could make us masters of our own house rather than slaves to the historians and social scientists."[17] Charles Wilkinson likewise sought to formulate a rhetorical definition of social movements: "Movements, rhetorically defined, are: languaging strategies by which a significantly vocal part of an established society, experiencing a sustained dialectical tension growing out of moral (ethical) conflict, agitate to induce cooperation in others, either directly or indirectly, thereby affecting the status quo."[18] Malcolm Sillars provides the broadest definition of social movements: "Movements, then, are collective actions which are perceived by a critic. They are defined by that critic in terms of the most useful rhetorical events, conflicts, or strategies which will best explain the critic's view of the movement."[19]

The impulse to formulate a rhetorical definition of social movements stemmed from a desire to distance rhetorical studies of social movements from sociological studies. However, rhetorical scholars like Herbert Simons draw heavily from sociological theories of social movements yet still examine social movements through the lens of rhetoric. Rhetoricians can employ sociological theory as rhetoricians—using sociological theory does not mean that one must examine the phenomenon as a sociologist.

In 1980, *Central States Speech Journal* brought together communication scholars to grapple with what were then the pressing questions concerning social movements: "is

---

[17] Robert S. Cathcart, "New Approaches to the Study of Movements: Defining Movements Rhetorically," *Western Speech* 36 (1972): 82, 88.
[18] Charles A. Wilkinson, "A Rhetorical Definition of Movements," *Central States Speech Journal* 27 (1976): 91.
[19] Malcolm O. Sillars, "Defining Social Movements Rhetorically: Casting the Widest Net," *Southern Speech Communication Journal* (1980): 30.

social movement rhetoric unique?" and "what is a social movement?" The first question (as originally posed) now receives little attention. Stephen Lucas stated that we need more studies and less controversy over terms.[20] However, the question is still implicit in methodological concerns. The debate concerning the question "what is a social movement?" focused on two possibilities—movement as empirically observable phenomenon and movement as rhetorically constructed meaning.

Michael Calvin McGee bluntly states that a "social movement is a set of meanings and not a phenomenon."[21] However, he does not fully address the question of who is constructing the meaning. McGee's other work suggests that the audience creates meaning and the speaker interprets it.[22] I suggest that meaning is created by all involved—speakers, audience members, and the critic. Meaning is embedded in the text and contains clues of the implied auditor and the implied speaker.[23]

The notion of social movements as rhetorically constructed meanings is useful, but McGee misrepresents sociological scholarship in order to make his point.[24] Lucas points out that "it is a mistake to imply that the vast majority of contemporary scholars claim that social movements exist 'apart from consciousness and independent of the

---

[20] Stephen E. Lucas, "Coming to Terms with Movement Studies," *Central States Speech Journal* 31, no. 4 (1980): 255-266.
[21] Michael Calvin McGee, "'Social Movement': Phenomenon or Meaning?" *Central States Speech Journal* 31, no. 4 (1980): 233.
[22] See Michael Calvin McGee, "Text, Context, and the Fragmentation of Contemporary Culture," *Western Journal of Communication* 54, no. 3 (1990): 274-89.
[23] See Edwin Black, "The Second Persona," *Quarterly Journal of Speech* 56 (1970): 109-19. For more on the implied author, see Wayne C. Booth, *The Rhetoric of Fiction* (Chicago: University of Chicago Press, 1961), 71-77.
[24] For critiques of McGee's position, see Lucas, "Coming to Terms with Movement Studies"; Herbert W. Simons, "On Terms, Definitions and Theoretical Distinctiveness: Comments on Papers by McGee and Zarefsky," *Central States Speech Journal* 31 (1980): 306-15.

discourse which communicates that consciousness.'"[25] Sociologists John McCarthy and Mayer Zald had previously defined a social movement as "a set of opinions and beliefs in a population which represents preferences for changing some elements of the social structure and/or reward distribution of a society."[26] Even Neil Smelser, one of the more traditional collective behavior scholars, recognized the link between action and rhetoric when he defined collective behavior as "mobilization on the basis of a belief which redefines social action."[27] Arthur Frank bluntly stated that "any sociological study has at least an implicit concern with reality construction, considered as the generation and maintenance of some organization of affairs, whether a family or a factory, a friendship or an illness."[28] All of these scholars had made it clear prior to McGee's essay that social movements were more than simply aggregates of people protesting. In fact, McCarthy and Zald's definition of social movements as "a set of opinions and beliefs" is strikingly similar to McGee's assumption that social movements are a "set of meanings." Therefore, it seems unfair to critique sociological research for lacking sensitivity to the rhetorically constructed nature of social movements.[29]

---

[25] Lucas, "Coming to Terms with Movement Studies"; McGee, "'Social Movement': Phenomenon or Meaning?"

[26] John D. McCarthy and Mayer N. Zald, "Resource Mobilization and Social Movements: A Partial Theory," *American Journal of Sociology* 82, no. 6 (1977): 1217-1218.

[27] Neil J. Smelser, *Theory of Collective Behavior* (New York: Free Press, 1962), 8.

[28] Arthur W. Frank III, "Reality Construction in Interaction," *Annual Review of Sociology* 5 (1979): 167.

[29] There is a large literature in sociology concerning the framing processes used by social movements. Although much of the framing literature came after McGee's critique, Goffman's 1974 work *Frame Analysis: An Essay on the Organization of Experience* provided the framework for later studies in framing and preceded McGee. For sociological work on framing, see Robert D Benford and David A Snow, "Framing Processes and Social Movements: An Overview and Assessment," *Annual Review of Sociology* 26 (2000): 611-39; Robert D. Benford, "Frame Disputes within the Nuclear Disarmament Movement," *Social Forces* 71, no. 3 (1993): 677-701; Daniel M. Cress and David A. Snow, "The Outcomes of Homeless Mobilization: The Influence of Organization, Disruption, Political Mediation, and Framing," *American Journal of Sociology* 105, no. 4 (2000): 1063-104; Jurgen Gerhards and Dieter Rucht,

Simons argues that social movements are empirically observable phenomena, reminding McGee that "when he relegates social movements to mere 'interpretations' while insisting that 'angry picketers' or even 'Standard Oil' are objective, empirical, 'out there' phenomena that remain unchanged regardless of our political views, I am prompted to remind him of another essay of his in which he argued that social constructions such as these are brought into being and shaped by discourse."[30] Simons attempts to bridge the gap between movement as meaning and movement as phenomenon when he states, "I do not separate categories from their users, phenomena from meanings, or objects from their descriptions, and I allow for judgments or interpretations as a prerequisite for labeling a given collective as a social movement 'phenomenon.'"[31] Simons points out that the split between phenomenon and meaning is a false dichotomy, stating that "we would be well advised to substitute 'both-and' thinking for much of our 'either-or' thinking."[32]

Alberto Melucci argues, "A discipline that sets out to study social movements can accomplish its task meaningfully only if it starts out from a theory that can account for the specificity and autonomy of social *action*, and can give a foundation to its *collective*

"Mesomobilization: Organizing and Framing in Two Protest Campaigns in West Germany," *American Journal of Sociology* 98, no. 3 (1992): 555-96; Erving Goffman, *Frame Analysis: An Essay on the Organization of Experience* (Cambridge, MA: Harvard University Press, 1974); Charlotte Ryan, "Framing, the News Media, and Collective Action," *Journal of Broadcasting & Electronic Media* 45, no. 1 (2001): 175-82; David A. Snow et al., "Frame Alignment Processes, Micromobilization, and Movement Participation," *American Sociological Review* 51, no. 4 (1986): 464-81.

[30] Simons, "On Terms, Definitions and Theoretical Distinctiveness: Comments on Papers by McGee and Zarefsky," 310. Here Simons refers to Michael C. McGee, "In Search of 'the People': A Rhetorical Alternative," *Quarterly Journal of Speech* 61, no. 3 (1975): 235-49.

[31] Simons, "On Terms, Definitions and Theoretical Distinctiveness: Comments on Papers by McGee and Zarefsky," 310.

[32] Ibid., 315.

character as something different from the sum total of aggregate individual behaviors."[33] This collective character makes hackers an interesting case study. Although some hackers would argue that they are simply a group of individuals united by a love for technological inquiry, there is more to this movement than an "aggregate of individual behaviors." Hackers have developed a strong collective identity that dictates their belief structures and influences the means by which hackers work to achieve political ends. They work to create a collective identity at conventions in physical space and in the virtual realm. Hackers work toward myriad political goals, but even when hackers are working for human rights or fighting the spread of globalization, they are always hackers first. This, more than anything, demonstrates that hackers are not merely parts of other social movements, but constitute a distinct social movement.

The New Social Movement Approach

Because the core work of the hacker movement seems to be the creation and reinforcement of their collective identity, the new social movement (NSM) approach is well suited to examining this movement. According to Alan Scott, three characteristics define new social movements: new social movements are primarily social, located within civil society, and "attempt to bring about change through changing values and developing alternative lifestyles."[34] Scott emphasizes that new social movements are "primarily

---

[33] Alberto Melucci, *Challenging Codes: Collective Action in the Information Age* (Cambridge: Cambridge University Press, 1996), 14.
[34] Alan Scott, *Ideology and the New Social Movements* (London: Unwin Hyman, 1990), 16-17.

social or cultural in nature and only secondarily, if at all, political."[35] Nelson Pichardo explains, "On the macro level, the NSM paradigm concentrates on the relationship between the rise of contemporary social movements and the larger economic structure, and on the role of culture in such movements. On the micro level, the paradigm is concerned with how issues of identity and personal behavior are bound up in social movements."[36]

Maurice Charland, drawing heavily from Louis Althusser, explains the difficulty of building a collective identity in his study of the *Peuple Quebecois*.[37] The main lesson from Charland's study is that interpellation is not enough. Thomas Benson demonstrates that the process of building a collective identity takes place in an exchange between speakers and audience members. Not only must the audience member identify with the proffered identity, he or she must also be willing to accept this identity from the person or organization who defines it.[38] Thus, it is not only the implied audience that is important to consider, but also the *ethos* created by the implied speaker. For hackers, this is particularly important; Manuel Castells observed, "Only hackers can judge hackers. Only the capacity to create technology (coming from any context), and to share it with the community, are respected values."[39]

---

[35] Ibid., 16.
[36] Nelson A. Pichardo, "New Social Movements: A Critical Review," *Annual Review of Sociology* 23 (1997): 411.
[37] Maurice Charland, "Constitutive Rhetoric: The Case of the *Peuple Quebecois*," *Quarterly Journal of Speech* 73, no. 2 (1987): 133-50. See also, Louis Althusser, *Lenin and Philosophy and Other Essays*, trans. Ben Brewster (New York: Monthly Review Press, 1971).
[38] Thomas W. Benson, "Rhetoric as a Way of Being," in *American Rhetoric: Context and Criticism*, ed. Thomas W. Benson, 293-322 (Carbondale: Southern Illinois University Press, 1989).
[39] Manuel Castells, *The Internet Galaxy: Reflections on the Internet, Business, and Society* (Oxford: Oxford University Press, 2001), 60.

Although the core work of the hacker movement concerns building a collective identity, this does not mean that hackers are apolitical—quite the contrary. Even so, this area has received little attention; most research on hackers focuses on stopping them or preventing their unauthorized access to computer systems. Hacktivism (politically motivated hacking) is the element of the hacker movement that shows the most promise for demonstrating how technology can be used to enhance democratic practice. As with any political strategy, the means of protest are often contested within the hacker community, but hackers largely seem to agree that hacking is a viable mode of political action. Because many hacking tools are readily available online, the ability to become a hacktivist has become democratized. Hugh Martin explains that "electronic protesting these days is a simple matter of downloading easy-to-use software from the Web, or of visiting a protest site where you can set your browser to bombard a target site with requests for information. Anyone can be a hacktivist."[40] Some hackers are doing this by design, making the work of hacking as easy as running a simple program or going to a particular website.[41] What sets hackers apart is the ability to *create* these techniques. In this sense, hackers are leading the way to a different form of protest, building on previous forms and taking their political actions into the digital realm.

---

[40] Hugh J. Martin, "Hacktivism: The New Protest Movement?" *Spark-Online*, 2000, http://www .spark-online.com/april00/trends/martin.html (accessed April 27, 2003), para. 6.

[41] One example of this is the electrohippies collective action against the 1999 World Trade Organization meeting in Seattle. To participate in this electronic sit-in, one needed only to access a website.

Outline of Chapters

In chapter two, I discuss the constraints of democratic practice in an information society. Scholars such as Daniel Bell and Alvin Toffler have argued that the industrial age is ending and that the United States and other nations are creating new societies based on information and networks.[42] I discuss various conceptions of democracy and explore the constraints that living in an information society places upon democratic practice. These constraints are broken into two categories: structural and identity. Structural constraints include access to information, information literacy of the population, and media consolidation. When considering identity constraints, I draw on scholars such as Sherry Turkle who argue that the information age has allowed for a shift in consciousness comparable to the shift in consciousness brought about by the advent of literacy.[43] I explore issues of citizenship and national identity in light of this more fluid conception of identity. I conclude the chapter with a discussion of how these constraints may influence social movement and protest activities.

In chapter three, I discuss the construction of a hacker collective identity. I begin by examining the sustained efforts to demonize hackers in congressional testimony, legislation, and the news media. I then examine the historical precedent that led up to this demonization, including events such as Operation Sundevil and the widespread media

---

[42] For theories concerning the information society, see Daniel Bell, *The Coming of Post-Industrial Society: A Venture in Social Forecasting*, Special anniversary ed. (New York: Basic Books, 1999); Manuel Castells, *The Rise of the Network Society*, 2nd ed. (Oxford: Blackwell Publishers, 2000); Jorge Reina Schement and Terry Curtis, *Tendencies and Tensions of the Information Age: The Production and Distribution of Information in the United States* (New Brunswick, NJ: Transaction Publishers, 1997); Alvin Toffler, *The Third Wave* (New York: William Morrow and Company, 1980).

[43] See note 14 above.

coverage of Kevin Mitnick through hacker texts, especially *Phrack*. I argue that government actions, such as Operation Sundevil, provided the motivation for hackers to organize. Although hackers were involved in political action before 1990, Operation Sundevil put them on the defensive. I conclude the chapter with an extended analysis of "The Conscience of a Hacker," better known as the hacker manifesto, in order to gain further insight into the collective identity of the hacker movement.

In chapter four, I examine hacktivism as a means for political action and as a rhetorical strategy. I discuss the means by which hacktivism is accomplished and provide a brief history of hacktivism, touching on some of the debates concerning means and ends within the hacker community. I then describe the ways that hacktivism overcomes some of the limitations of traditional means of protest. In order to examine some of the rituals and norms of hacktivism, I provide an extended case study of a politically motivated hack of the *New York Times* website. Although this hack was largely considered a "free Kevin Mitnick" statement, the code within the hack served to reinforce in/out group boundaries and hacker identity. I conclude with a discussion of the implications for democratic practice that can be distilled from the norms and rituals of the hacking community. I argue that the hack served to fulfill what Richard Gregg describes as "the ego function of protest rhetoric," rather than seeking to enact actual change within the society at large.[44]

Chapter five discusses the potential for a technologically enhanced democratic society by examining four major themes: the construction of identity within an

---

[44] Richard B. Gregg, "The Ego-Function of the Rhetoric of Protest," *Philosophy and Rhetoric* 4 (1971): 71-91.

information society; the question of who manufactures and designs technology and what values those people instill within the technologies; the ways that citizens may use new, more democratic means of protest and civic engagement; and the efficacy of unconventional means of political expression such as hacktivism. I examine these themes within the context of hacker collective identity and values. I conclude with a brief, cautionary forecast considering the outlook for democratic practice in an information society and provide possibilities for how society can use these technologies in more democratic ways.

This study contributes to scholarly research in rhetorical studies, democratic theory, social movements, and information society studies. Most importantly, this study provides an alternate way of viewing hackers. Although hackers are often dismissed as mere criminals or, worse yet, terrorists, hackers should be examined as a social movement with political motivations. Examining the collective identity of hackers provides a glimpse of how technology may evolve and the potential for these technologies to enhance democratic practice. I found that the collective identity of hackers is essentially non-democratic. Rather than bringing groups together, hacker collective identity requires a strong distinction between hackers and everyone else and fosters a sense of intellectual and moral superiority among hackers that denies the potential for the masses to participate in hacktivism. However, hacktivism still shows potential as a way for disenfranchised minorities to have their voices heard, especially when facilitated by groups with strong democratic values, such as the electrohippies collective. As such, it should be examined carefully before discarding this potentially democratizing tool of political action.

Chapter 2

Democratic Practice in an Information Society

The assertion that technology will affect democratic practice is not new, as demonstrated by this exultation from the past describing a new technology:

- Will elicit a new national loyalty and produce a more contented citizenry.
- The government will be a living thing to its citizens instead of an abstract and unseen force.
- Elected representatives will not be able to evade their responsibilities to those who put them in office.
- At last we may have covenants literally openly arrived at.
- The people's university of the air will have a greater student body than all our universities put together.[45]

This may sound like the current hype over the Internet and new media, but the year was 1922 and the magazine was *Radio Broadcast*. Thus, it is with an understanding of the perils of prediction that I embark on an exploration of how new communication technologies such as the Internet may influence democratic practice.

That technological advances affect democratic practice seems clear but specific effects of technology on a given society are often difficult to predict. When considering

---

[45] *Radio Broadcast* (May 1922), quoted in Erik Barnouw, "New Look," in *Conglomerates and the Media*, ed. Patricia Aufderheide, et al., 15-29 (New York: New Press, 1997), 17.

the effects of technology on democracy, it is easy to slip into a kind of technological determinism. Karl Marx stated, "In acquiring new productive forces men change their mode of production; and in changing their mode of production, in changing the way of earning their living, they change all their social relations. The hand-mill gives you society with the feudal lord; the steam-mill society with the industrial capitalist."[46] But technology always has unintended consequences. It is impossible to predict all of the possible ways that technology will be used; history is full of short-sighted technologists who have failed to see the social impact of their own inventions. Rather than considering technology in a deterministic fashion, it is more useful to consider the ways that technology constrains future action; in other words, particular technologies invite particular kinds of responses. For example, Kathleen Jamieson demonstrates how the rhetorical constraints of television rewarded behaviors and attributes that were unnecessary in other media such as radio or print.[47]

Just as the printing press, radio, and television have altered the fabric of society, it is clear that *something* is happening with new communication technologies. This chapter examines the potential constraints that these technologies may place on democratic practice. Democracy is defined by three overarching components: the ability for individual citizens to have a voice in political matters, the nature of citizenship, and the limitation of government power. How these three dimensions of democratic practice are performed is influenced by the kind of society in which that form of democracy is

---

[46] Karl Marx and Friedrich Engels, "The Poverty of Philosophy," in *Karl Marx, Frederick Engels: Collected Works,* 47 vols. (Moscow: Progress Publishers, 1975), 6:166.
[47] Kathleen Hall Jamieson, *Eloquence in an Electronic Age: The Transformation of Political Speechmaking* (New York: Oxford University Press, 1988).

enacted. There are varied forms of democracy and different forms of society invite particular forms. In both the scholarly and popular press, the United States is often referred to as an information society, thus it is necessary to examine the constraints that such a society could place on democratic practice. Some of these constraints include the nature of identity in an information society, access to information and information technologies, and the interconnection of individuals and institutions. The chapter concludes with a discussion of how these constraints may influence social movement and protest activities.

What is Democracy?

Defining democracy is a daunting task—Henry Jenkins and David Thorburn point out that "'democracy' itself is a disputed term," and ask, "Is democracy a particular structure of governance or a culture of citizenship or some complex hybrid of the two?"[48] Because the two are connected, it must be both a culture and a political system. Barry Hague and Brian Loader state that "democracy is about more than voting or providing better public information to the citizen. . . . Democracy has at its heart self-determination, participation, voice and autonomy."[49] Implicit in the idea of democracy is the belief that the citizenry are capable and willing to make decisions in the public interest.

---

[48] Henry Jenkins and David Thorburn, "Introduction: The Digital Revolution, the Informed Citizen, and the Culture of Democracy," in *Democracy and New Media*, ed. Henry Jenkins, David Thorburn, and Brad Seawell, 1-17 (Cambridge, MA: MIT Press, 2003), 2.

[49] Barry N. Hague and Brian Loader, "Digital Democracy: An Introduction," in *Digital Democracy: Discourse and Decision Making in the Information Age*, ed. Barry N. Hague and Brian Loader, 3-22 (London: Routledge, 1999), 7.

Many scholars have described the necessary conditions for democracy. Vincent Mosco argues that "a fully democratic society is one in which citizens are actively involved in creating economic, sociocultural, and political participation and equality."[50] Alain Touraine describes three dimensions of democracy: rulers must be representative; voters are, and regard themselves as, citizens; and there must be limitations on the power of the rulers.[51] Victor Bekkers and Hein Van Duivenboden lay out four democratic principles: legal equality; legal security, or predictability; rule of law; and checks and balances.[52] Democratic practice requires that people are able to have an impact on decisions that affect them, citizens who believe themselves to be citizens and act together as such, and the limitation of government power. Other important elements of democracy, such as legal equality of citizens and respect for the rule of law, can be adequately accounted for within these principles.

Voice

Above all, democracy should be deliberative. Arthur Isak Appelbaum provides what he considers to be the widest definition of deliberative democracy: "Any practice of interactive communication in which actors in a democracy seek to affect the decisions of one another by influencing beliefs about politically relevant facts, values, concepts, or

---

[50] Vincent Mosco, "Computers and Democracy," in *The Information Society: Evolving Landscapes*, ed. Jacques Berleur, et al., 215-31 (New York: Springer-Verlag, 1990), 216.
[51] Alain Touraine, *What Is Democracy?* trans. David Macey (Boulder, CO: WestviewPress, 1997), 26-27.
[52] Victor J. J. M. Bekkers and Hein P. M. Van Duivenboden, "Democracy and Datacoupling," in *Orwell in Athens: A Perspective on Informatization and Democracy*, ed. Wim B. H. J. van de Donk, I. Th M. Snellen, and P. W. Tops, 213-23 (Amsterdam: IOS Press, 1995), 214-215.

interests"[53] Jürgen Habermas explains that in the salons and coffee houses of the eighteenth century, "the authority of the better argument could assert itself against that of social hierarchy and in the end can carry the day," with individuals bracketing out differences in an attempt to reach the best possible solution to public concerns.[54] Although Habermas pointed out that this egalitarian ideal was never completely realized in practice, it was, and still remains, a normative standard.[55] Stephen Frantzich argues that "requiring more of democracy than simply recording potentially poorly grounded preferences requires relatively open access to a wide variety of voices, allowing all ideas to be tested in the forge of open discussion. The 'winners' in such battles over words are not necessarily based on who won in the past or the loudness of the voices, but rather on the ability of the speakers to make their ideas compelling to a broad range of legitimate participants."[56]

There is more to deliberative democracy than simply having a venue in which to speak; citizens must actually take the initiative to express their thoughts, opinions, and concerns. Mosco argues that democracy is "the fullest possible public participation in the decisions that affect our lives."[57] Active participation is important because, as Frantzich explains, "democratic governments are based on the principle of responsiveness to the needs and desires *of those who make their needs and desires known.* . . . Just as

---

[53] Arthur Isak Applbaum, "Failure in the Cybermarketplace of Ideas," in *Governance.Com: Democracy in the Information Age*, ed. Elaine Ciulla Kamarck and Joseph S. Nye, 17-31 (Washington, DC: Brookings Institution Press, 2002), 23-24.
[54] Jürgen Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*, trans. Thomas Burger (Cambridge, MA: MIT Press, 1989), 36.
[55] Ibid.
[56] Stephen E. Frantzich, *Cyberage Politics 101: Mobility, Technology and Democracy* (New York: Peter Lang, 2002), 126.
[57] Mosco, "Computers and Democracy," 215.

democracy is not a spectator sport, it is also clear that one is unlikely to win if one does not play."[58] But government officials must also desire input from the citizenry. Hague and Loader state that "'strong democracy' requires strong and interactive links between the state and civil society, between government and the governed."[59] Without this link between the state and the citizenry, it matters little if the citizenry have the desire, skill, or ability to participate.

To argue that citizens must take the initiative to participate assumes that all citizens have the same ability to participate. James Hyland states, "'Democracy,' after all, even at its broadest and most vague, must be referring to some distributional situation among members of a group; and if it implies approval will do so on the basis of some degree of approach to 'equality,' in some sense or other."[60] American history is riddled with examples of structural barriers to participation. Even after universal suffrage was enacted, institutions such as the poll tax kept the poor and minorities from casting their vote. There were also literacy tests, intimidation, and threats to disenfranchise undesirable voters.[61] Citizens require not only an available venue in which to express their views, but also the realistic ability to express those views.

---

[58] Frantzich, *Cyberage Politics 101: Mobility, Technology and Democracy*, 130.
[59] Hague and Loader, "Digital Democracy: An Introduction," 13.
[60] James L. Hyland, *Democratic Theory: The Philosophical Foundations* (Manchester: Manchester University Press, 1995), 43.
[61] For more on systematic disenfranchisement of certain groups, especially the poor, minorities, and non-English speakers, see Joseph L. Bernd and Lynwood M. Holland, "Recent Restrictions Upon Negro Suffrage: The Case of Georgia," *The Journal of Politics* 21, no. 3 (1959): 487-513; "Disenfranchisement by Means of the Poll Tax," *Harvard Law Review* 53, no. 4 (1940): 645-52; Sandra Guerra, "Voting Rights and the Constitution: The Disenfranchisement of Non-English Speaking Citizens," *The Yale Law Journal* 97, no. 7 (1988): 1419-37; Bernard Schwartz, "The Negro and the Law in the United States," *The Modern Law Review* 14, no. 4 (1951): 446-61.

Access to the public forum and the ability and desire to express one's opinion is not enough—citizens must be able to formulate competent judgments on issues of public policy. Thomas Jefferson recognized that citizens would not always make ideal decisions, but with accurate information these episodes would be limited: "The way to prevent these irregular interspersions of the people is to give them full information of their affairs thro' the channel of the public papers, & to contrive that those papers should penetrate the whole mass of the people . . . every man should receive those papers & be capable of reading them."[62] Walter Lippmann takes a dim view of the public's ability to parse the information required to make informed decisions on public matters, arguing that state of affairs—even in 1922—was too complex to be understood completely by the layperson, the legislator, or even the expert.[63] John Dewey agrees with this state of affairs: "There are too many publics and too much of public concern for our existing resources to cope with."[64] For Dewey, salvation comes through communication and community: "Till the Great Society is converted into a Great Community, the Public will remain in eclipse. Communication can alone create a great community."[65] A similar impulse seems to drive those who believe that new communication technologies will revitalize democratic practice: communication creates community and community creates a stronger democracy.

---

[62] Thomas Jefferson, "To Edward Carrington," in *Thomas Jefferson, Political Writings*, ed. Joyce Oldham Appleby and Terence Ball, 152-54 (New York: Cambridge University Press, 1999), 153.
[63] See Walter Lippmann, *Public Opinion*, 1st Free Press pbks. ed. (New York: Free Press Paperbacks, 1997), 143, 233-235, 250-251.
[64] John Dewey, *The Public and Its Problems* (Athens, OH: Swallow Press, 1991), 126.
[65] Ibid., 142.

Citizenship

Touraine argues that for democracy to function, people must consider themselves to be citizens and behave as such.[66] Citizenship is often conflated with nationality, but the notion of citizenship I refer to here is something that is enacted—citizenship as a verb rather than a noun. Robert Asen writes, "Rather than asking what counts as citizenship, we should ask: how do people enact citizenship? Reorienting our framework from a question of *what* to a question of *how* usefully redirects our attention from acts to action. Inquiring into the *how* of citizenship recognizes citizenship as a process. From this perspective, citizenship does not appear in specific acts per se, but signals a process that may encompass a number of different activities."[67]

Citizenship is not only something that one does, but also something that one is; citizenship is tied to identity. Touraine misses a vital part of the equation—not only must each citizen believe that he or she is a citizen, each must also extend that belief to others who are legally granted that status. There have been many efforts to disenfranchise citizens who, despite legal entitlement to full democratic participation, were considered undesirable by other citizens.[68] Although legal structures are in place to allow access to voting or to an individual's representatives, the impulse to silence certain factions of society indicates a larger problem. An integral part of citizenship is considering the public good as a whole, and not just that which is good based on one's prejudices.

---

[66] For more on Touraine's conception of citizenship, see Touraine, *What Is Democracy?* See esp. chap. 5, "Citizenship."
[67] Robert Asen, "A Discourse Theory of Citizenship," *Quarterly Journal of Speech* 90, no. 2 (2004): 191.
[68] See note 61 above.

Citizens should consider the idea and not dismiss it because of the person's attributes. Richard Sennett argues that the ideal enactment of citizenship is a society that is able to interact as if they were strangers in public: "The extent to which people can learn to pursue aggressively their interests in society is the extent to which they learn to act impersonally."[69]

Almost every critique of democracy centers on the weakness of human beings. Individuals occupy divergent roles as citizens and consumers. These roles often stand in opposition as individual citizens weigh the collective good against individual wants and needs. Benjamin Barber illustrates the often contradictory nature of these roles:

> Consumers make private choices about their private needs and wants. Citizens make choices about the public needs and the public goods of the nation. There is no way, as private consumers, we can do that. We all know that. I love driving a fast car. As a consumer, I love it, but as a citizen, I helped to make laws that limit the size and speed of cars because I know having a lot of large, gas-guzzling, fast-moving cars is dangerous for the health of me, my children, and every citizen of the United States. I know the difference between those two things. I can distinguish the citizen in me and the consumer in me. You can't turn over civic public choices to private consumers. We cannot, one by one, as private persons deal with the social consequences of those private choices. That's why we have

---

[69] Richard Sennett, *The Fall of Public Man* (New York: W.W. Norton, 1996), 349.

> public institutions. That's why we have government: precisely to make the tough choices about and deal with the social consequences of private choices.[70]

Society cannot ask consumers to do the work of citizens. There will be times when the majority will desire solutions that, although they may appear acceptable in the short term, could have dire long term consequences. For example, vigilantism may seem an appropriate short term solution to skyrocketing crime rates, but in the long term may decrease respect for due process and the idea that an accused criminal is considered innocent until proven guilty. Short term solutions are not always in the public interest and may result from a desire for immediate gratification, security, or self-preservation.[71]

Individual citizens may experience difficulty separating their own self-interest from the common good, especially when the common good is not in that citizen's self interest. The hope of democracy is that the greater the number of citizens that consider the issues, the more likely that wisdom will prevail. Stephen Frantzich states that "democracy is the recurrent suspicion that over half the people are right over half the

---

[70] Ira Magaziner and Benjamin Barber, "Democracy and Cyberspace: First Principles," in *Democracy and New Media*, ed. Henry Jenkins, David Thorburn, and Brad Seawell, 113-31 (Cambridge, MA: MIT Press, 2003), 130-131.

[71] Anthony Mawson argues that rather than panicking, when disaster strikes, people seek familiar people and surroundings. See Anthony R. Mawson, "Understanding Mass Panic and Other Collective Responses to Threat and Disaster," *Psychiatry* 68, no. 2 (2005): 95-113. Once the immediate threat has passed, individuals seem to seek security from future threat. When threatened, people have a tendency to think in terms of emotion rather than logically. Carol Gordon and Asher Arian found that policy was likely to be emotion driven under conditions of high threat while during times of low threat, rational, logical consideration was more likely to drive policy decisions. See Carol Gordon and Asher Arian, "Threat and Decision Making," *The Journal of Conflict Resolution* 45, no. 2 (2001): 196-215. Part of this may come as a result of the processes that people under stress use to make decisions. Deborah Gladstein and Nora Reilly found that "[group] members react to external environmental threat by using less information and fewer communication channels and by having less interaction than they would under nonthreatening conditions." See Deborah L. Gladstein and Nora P. Reilly, "Group Decision Making under Threat: The Tycoon Game," *Academy of Management Journal* 28, no. 3 (1985): 622.

time."[72] While it seems wise to place some limitation on the power of the people, especially when the voice of the people reflects the consumer rather than the citizen, it is essential to place limitations on the power of the government because the problems that exist with individuals are magnified with government officials. Individuals may seek their own interests but government officials can actually legislate their own interests.

Limitation of Governmental Power

The ability of citizens to express opinion means little if the representatives cannot or will not listen or if the representatives do not value the views of the citizenry. Iris Marion Young argues, "The normative legitimacy of a democratic decision depends on the degree to which those affected by it have been included in the decision-making processes and have had the opportunity to influence the outcomes."[73] The founders of the United States recognized the need for a system of checks and balances. When government officials are given power without consequence, they tend to act only in their own interests. If the voice of the citizenry is to have any effect whatsoever, there must be limitations on governmental power. It is commonly stated that the power of the government springs from the people, but if this is the case, then why do citizens often fail to vote or contact their representatives because they do not believe that their actions will change anything?[74] There seems to be a disconnect between the *actual* power of the

---

[72] Frantzich, *Cyberage Politics 101: Mobility, Technology and Democracy*, 93.
[73] Iris Marion Young, *Inclusion and Democracy* (Oxford: Oxford University Press, 2000), 5-6.
[74] Michael Calvin McGee describes the problems of making an appeal based on the will of the people. See McGee, "In Search of 'the People': A Rhetorical Alternative."

people and the *perceived* power of the people. Even so, the idea that members of the United States government have an obligation to fulfill the will of the people is an institutionalized belief among both citizens and government officials, so governmental power is not absolute.

Democracies exist with varying degrees of governmental power. Arend Lijphart, in his analysis of thirty-six democratic nations, found that "consensus democracy [as opposed to majoritarian democracy] makes a difference. Indeed, consensus democracy—on the executives-parties dimension—makes a big difference with regard to almost all of the kinder and gentler qualities."[75] These kinder and gentler qualities include such issues as women's representation and political equality. Lijphart provides an exhaustive study of different governments, providing ten points that illustrate the differences between majoritarian and consensus governments. Authoritarian governments are those with power concentrated in the bare majority or, in some cases, the largest constituency. Consensus governments not only believe in the rule of the majority but show a desire to maximize the majority. Lijphart states that "the majoritarian model of democracy is exclusive, competitive, and adversarial, whereas the consensus model is characterized by inclusiveness, bargaining, and compromise."[76]

Although the level of governmental power has an effect on citizens, for a democratic government to claim legitimacy it must bend to the will of the people in most

---

[75] Arend Lijphart, *Patterns of Democracy: Government Forms and Performance in Thirty-Six Countries* (New Haven, CT: Yale University Press, 1999), 300.
[76] Ibid., 2.

respects. Social movements are an important part of this equation because, in theory at least, they demonstrate the will of the people. Touraine explains,

> Far from being antithetical, social movements and democracy are, in contrast, indissociable. On the one hand, if a political system regards social movements simply as violent expressions of demands that cannot possibly be satisfied, it ceases to be representative and loses the trust of the electorate. . . . A government that tries to legitimize its actions in terms of the constraints of the system loses its democratic character, even if it remains tolerant and liberal. On the other hand, a social movement can exist only if a collective action has social objectives, or in other words, recognizes that society has general interests or values. In other words, a social movement can exist only if collective action does not reduce political life to a confrontation between camps or classes, even though it organizes and extends conflicts.[77]

Social movements are essential to a well functioning democracy because they focus government attention on the concerns of the citizenry. Hague and Loader state that "what 'strong democracy' requires is government committed to open and meaningful dialogue with the citizenry. What we should not expect is that the push towards such a condition will come from governments themselves."[78]

Social movements make clear the relationship between the government and the citizenry—citizens speak, the government responds to those wishes by enacting the desired reforms. However, Joseph Schumpeter turns the idea that the role of government

---

[77] Touraine, *What Is Democracy?* 57.
[78] Hague and Loader, "Digital Democracy: An Introduction," 13.

is to fulfill the will of the people on its head. Schumpeter argues that "the role of the people is to produce a government, or else an intermediate body which in turn will produce a national executive or government" and defines the democratic method as "that institutional arrangement for arriving at political decisions in which individuals acquire the power to decide by means of a competitive struggle for the people's vote."[79] Schumpeter seems to have difficulty accepting that there may be a common good, a will of the people, and the potential for a citizenry to rationally consider political issues.[80] But citizens, if given complete and proper information, *can* make rational decisions for the public good.

The ideal of deliberative democracy in which citizens come together to deliberate issues of civic importance and arrive at the solution that best reflects the public good is a normative one. In practice, public deliberation is fraught with emotion and ulterior motives and may or may not be rational. Even so, logical, rational decision making in governance by both governmental officials and the public can, and does, take place. Habermas suggests that "moral questions can in principle be decided rationally, i.e., in terms of *justice* or the generalizability of interests."[81] Anthony Downs explains that "the term *rational* is never applied to an agent's ends, but only to his means."[82] Downs elaborates that his usage of the term rational is that of a purely economic sense: "The economic definition [of rationality] refers solely to a man who moves toward his goals in

---

[79] Joseph Alois Schumpeter, *Capitalism, Socialism, and Democracy*, 4th ed. (London: Allen & Unwin, 1954), 269.
[80] See Ibid., 250-262.
[81] Jürgen Habermas, *Moral Consciousness and Communicative Action*, trans. Christian Lenhardt and Shierry Weber Nicholsen (Cambridge, MA: MIT Press, 1990), 108.
[82] Anthony Downs, *An Economic Theory of Democracy* (New York: Harper, 1957), 5.

a way which, to the best of his knowledge, uses the least possible input of scarce resources per unit of valued output."[83] This is a useful way to consider how citizens take part in democratic practice.

Democratic practice is culturally bounded. To live in a democratic society means that citizens have a voice in political matters and that government power has limitations. Each incarnation of democratic society may have different ways of negotiating these facets depending on the constraints of that particular culture. Lijphart points out that there are many ways to enact democratic society. An information society is one possible form of society. Although there is no such thing as *the* information society, like democracy, certain characteristics place a particular nation or group into the category "information society." These characteristics place constraints on the role of the state, the nature and identity of the citizen, and the importance of access to information.

What Does an Information Society Look Like?

Drastic claims that technology has had or is now having a tremendous impact on the entirety of human society is nothing new. Willem Vanderburg makes similar claims concerning the industrial revolution: "The name Industrial Revolution is misleading because industrialization is a transformation of the entire way of life of a society. Underneath the individual technological, economic, social, legal, political, moral and religious changes, lies a larger pattern of change of which these specific changes are an

---

[83] Ibid.

integral part."[84] Western society is now moving from an industrialized age into an information age, or what Alvin Toffler calls the "Third Wave," which will purportedly have a tremendous impact in our everyday lives. "The Third Wave is not just a matter of technology and economics. It involves morality, culture and ideas as well as institutions and political structure. It implies, in short, a true transformation in human affairs."[85]

Although scholars argue that the United States is becoming an information society, networks allow people to transcend geographic boundaries, so it is a bit misleading to refer to a particular nation state as an information society. Because of the networked nature of information societies, any electronic democracy, while perhaps based on the American model, will not necessarily set out to provide representation to a particular governmental entity. This allows for the possibility of a new kind of democracy and a new kind of representation that is not based on geographic boundaries or on national identities. But the question of whom or what this democracy will represent is often pushed to the periphery. Some technophiles seem to assume that the new cyberdemocracy will represent the needs of humanity as a whole.[86] Although this is commendable in theory, there remain significant questions concerning whose values and

---

[84] Willem Vanderburg, "Political Imagination in a Technical Age," in *Democratic Theory and Technological Society*, ed. Richard B. Day, Ronald Beiner, and Joseph Masciulli, 3-35 (Armonk, NY: M.E. Sharpe, 1988), 15.

[85] Alvin Toffler and Heidi Toffler, *Creating a New Civilization: The Politics of the Third Wave* (Atlanta: Turner Pub., 1995), 11. For Toffler, the first wave represents agrarian society, the second wave represents industrialized society, and the third wave constitutes the rise of the information society. For a more extended notion of the third wave, see Toffler, *The Third Wave*.

[86] See John Perry Barlow, "A Declaration of the Independence of Cyberspace," February 8, 1996, http://homes.eff.org/~barlow/Declaration-Final.html (accessed July 26, 2005). Barlow makes a clear distinction between physical governments and cyberspace in which rules and laws are formulated by a sort of magical consensus. Although Barlow seems too enthusiastic about the liberatory effects of cyberspace, he does make a valuable distinction when he states, "We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies." The interplay between the virtual self and the physical self will be discussed more fully in the next chapter.

voices will be heard and followed. Even in relatively homogeneous populations, there are often significant differences of opinion in what constitutes the greatest good for society and in a heterogeneous population these differences would likely be exacerbated.

Predictions concerning the rise of the information society are often laden with utopian sentiment and emerging scholarship describes the potential for information societies to bring about a global public sphere. Nicholas Negroponte provides perhaps the most unabashedly utopian ideal of the Internet as virtual public sphere. He argues that war will eventually make no sense because digital space will become more important than physical space and that "nations, as we know them today, will erode because they are neither big enough to be global nor small enough to be local."[87] While the idea of a virtual public sphere that could abolish war is attractive, most scholars are more reserved concerning the potential of a virtual public sphere. Zizi Papacharissi states, "As public space, the internet provides yet another forum for political deliberation. As public sphere, the internet could facilitate discussion that promotes a democratic exchange of ideas and opinions."[88] However, she also notes that special interests may fragment the audience of these discourses, resulting in a kind of tribalization.[89] Even if the Internet could shape a new virtual public sphere, the problems of access are just as real now as they were in the eighteenth century salons described by Habermas.[90] Diana Saco explains, "If cyberspace,

---

[87] Nicholas Negroponte, "Beyond Digital," *Wired*, December 1998, 288.
[88] Zizi Papacharissi, "The Virtual Sphere: The Internet as a Public Sphere," *New Media & Society* 4, no. 1 (2002): 11.
[89] Ibid., 17. See also Sunstein, *Republic.Com*.
[90] Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. The main barrier to access in the eighteenth century public sphere was literacy and leisure time. In the twenty-first century, the barriers are much the same, only now it is digital literacy rather than print literacy.

in one respect, can break down (physical) barriers, allowing us to roam freely across an electronic frontier, it can also erect new (digital) barriers, both in terms of who gains access and of what can be accessed."[91]

But the question of what it means to live in an information society remains. Jorge Reina Schement identifies six major themes in the research attempting to define an information society: informational materialism, or information exchanged as an economic commodity; a large informational workforce; interconnectedness among individuals and institutions; the special status of scientific knowledge; a social environment with many messages and channels; widely diffused information technology.[92] Of these facets, the ones that seem most pertinent to a discussion of how living in an information society may affect democratic practice are the commodification of information, the interconnection of individuals and institutions, and access to information technologies. One element not included in this list, but nonetheless relevant, is the identity shift that living in an information society can promote. Because identity and citizenship are connected, a shift in identity may have consequences for how individuals enact citizenship.

The Commodification of Information in an Information Society

In 1822, James Madison wrote, "A popular Government, without popular information, or the means of acquiring it, is but a prologue to a farce or tragedy; or

---

[91] Diana Saco, *Cybering Democracy: Public Space and the Internet* (Minneapolis: University of Minnesota Press, 2002), 210.

[92] Jorge Reina Schement, "The Origins of the Information Society in the United States: Competing Visions," in *The Information Society: Economic, Social, and Structural Issues*, ed. Jerry Lee Salvaggio, 29-50 (Hillsdale, NJ: Lawrence Erlbaum Associates, 1989).

perhaps both. Knowledge will forever govern ignorance; and a people who mean to be their own governors, must arm themselves with the power which knowledge gives."[93] In a similar vein, James Mill stated that "the very foundation of a good choice is knowledge. The fuller and more perfect the knowledge, the better the chance, where all sinister interest is absent, of a good choice. How can the people receive the most perfect knowledge relative to the characters of those who present themselves to their choice, but by information conveyed freely, and without reserve, from one to another?"[94] It is difficult to argue against the idea that a well-informed citizenry is essential to a well functioning democracy but Bruce Bimber explains that "the link between information and engagement is as much a product of politics as a source. Despite its apparently deep Madisonian resonance, the familiar belief in the necessity of informed citizenship did not originate in the nation's founding. It arose during the time that the second American information revolution was under way, as attacks on patronage and party power led to the evolution of a new ideal of citizenship and as the rise of new policy problems processes created new informational demands on citizens and public officials."[95] But the link between an informed citizenry and a well functioning democracy is not as recent as Bimber suggests. As far back as Aristotle, political theorists have recognized the necessity of having a citizenry who understood the workings of the government. Aristotle defines "citizen" as "he who has power to take part in the deliberative or judicial

---

[93] James Madison, "To W. T. Barry, August 4, 1822," in *Letters and Other Writings of James Madison*, 4 vols. (Philadelphia: J. B. Lippincott & Co., 1865), 3:276.
[94] James Mill, "Liberty of the Press," in *Essays on Government, Jurisprudence, Liberty of the Press and Law of Nations*, 1-34 (New York: A. M. Kelley, 1967), 19.
[95] Bruce A. Bimber, *Information and American Democracy: Technology in the Evolution of Political Power* (Cambridge: Cambridge University Press, 2003), 198. For similar arguments, see Michael Schudson, *The Good Citizen: A History of American Civic Life* (New York: Martin Kessler Books, 1998).

administration of [the state]."[96] To effectively take part in deliberation, one must have some understanding of the issues at hand. Even Plato, who advocated a kind of benevolent dictatorship over democracy, stated in his *Laws* that "a citizen has already a calling which will make full demands on him, in view of the constant practice and wide study it involves, in the preservation and enjoyment of the public social order."[97] Even so, it matters little whether the link between access to information and democratic practice is a recent development; access to information is important now.

The Internet, which is often said to level the playing field for the disenfranchised, has instead widened the gap between the information haves and the information have-nots. Herbert Schiller and Bernard Miège state, "The 'information society,' as it now functions, takes for granted, indeed reinforces, a world economy with an international division of labor that apportions benefits to a small number of highly developed nations. These are then redistributed, also unequally, within these privileged economies."[98] Those that have and control information are not individuals, but transnational corporations (TNCs) and nongovernmental organizations (NGOs). Moore argues that "in today's increasingly concentrated media industry, elite control over public opinion is for all intents and purposes total."[99] Moore describes the dangers of media conglomeration,

---

[96] Aristotle, "Politics," in *The Complete Works of Aristotle: The Revised Oxford Translation*, ed. Jonathan Barnes, 1986-2129 (Princeton: Princeton University Press, 1984), 1275b19-20.
[97] Plato, "Laws," in *The Collected Dialogues of Plato, Including the Letters*, ed. Edith Hamilton and Huntington Cairns, 1225-513 (Princeton, NJ: Princeton University Press, 1961), 846d.
[98] Herbert I. Schiller and Bernard Miège, "Communication of Knowledge in an Information Society," in *The Information Society: Evolving Landscapes*, ed. Jacques Berleur, et al., 161-67 (New York: Springer-Verlag, 1990), 163.
[99] Richard K. Moore, "Democracy and Cyberspace," in *Digital Democracy: Discourse and Decision Making in the Information Age*, ed. Barry N. Hague and Brian Loader, 39-59 (London: Routledge, 1999), 46.

suggesting that because of their affiliation with General Electric (GE), NBC would likely not run an exposé on GE's nuclear reactor safety problems or corruption involving GE's government contracts.[100] Where there is corporate or governmental censorship, citizens are unlikely to have all of the necessary information required for competent assessment of issues of public concern. If citizens rely on the news media to provide reporting and commentary on public issues, yet news organizations are increasingly driven by profit and self-preservation rather than reporting important information, how will citizens gather the necessary information with which to make informed decisions?[101] Citizens may turn directly to government officials, but even with laws such as the Freedom of Information Act, it is difficult for common citizens to gain access to information.[102] Thus, government and corporate self-interest places structural limitations on citizen acquisition of information.

A disturbing trend in the information society is the move to an information *economy*. This is not entirely new; Schement points out that the betrayal of Jesus Christ

---

[100] Ibid., 43. Vertical integration and the suppression of potentially damaging information is a recurring theme in the literature discussing media conglomeration. For more on this, see Noam Chomsky, *Media Control: The Spectacular Achievements of Propaganda* (New York: Seven Stories Press, 1997); Edward S. Herman and Noam Chomsky, *Manufacturing Consent: The Political Economy of the Mass Media* (New York: Pantheon Books, 1988); Robert Waterman McChesney, *Corporate Media and the Threat to Democracy* (New York: Seven Stories Press, 1997); Gerald Sussman, *Communication, Technology, and Politics in the Information Age* (Thousand Oaks, CA: Sage Publications, 1997).

[101] For more on the consequences of commercialization of the news media, see McChesney, *Corporate Media and the Threat to Democracy*.

[102] By classifying information, the federal government, especially the executive branch, can avoid scrutiny of their actions. Since the events of September 11, 2001, it seems easier to withhold information in the interest of national security. See "Government Secrecy Continued to Rise in 2004," *Newsletter on Intellectual Freedom* 54, no. 3 (2005): 100-01; Scott Shane, "Since 2001, Sharp Increase in the Number of Documents Classified by the Government," *New York Times*, July 3, 2005.

by Judas Iscariot was essentially a transaction of money for information.[103] Although selling information is not intrinsically wrong, Schiller and Miège point out that "the commercialization of information, in conjunction with the specialization and fragmentation of data that computerization encourages, is deepening what is already an inequitable information order."[104] In an information economy, information is available based on an individual's ability to pay. If citizens are to make informed decisions, information about issues of public concern should be free and easily accessible. Ellul argues that "democracy requires that the people must be correctly informed. If the populace is to make sound decisions, it must have exact and relatively complete information (complicated calculations and experiments are not necessary) regarding the means employed and the dangers that might result. . . . When I say that the public must be informed, I do not have simplistic solutions in mind; the public must be given information that allows free decisions, not ones based solely upon a menu of options served up by technicians."[105]

The public must have access to unfiltered information free of corporate and governmental censorship, even if such information may be difficult to understand. Access to well formatted, usable information should also be available to the public, but it should be provided in addition to the raw data. As information is processed, each party is likely to frame the information to achieve maximum benefit and minimum negative impact for

---

[103] Jorge Reina Schement, "An Etymological Exploration of the Links between Information and Communication," in *Between Communication & Information*, ed. Brent D. Ruben and Jorge Reina Schement, 173-87 (New Brunswick, NJ: Transaction Publishers, 1993), 174-175.
[104] Schiller and Miège, "Communication of Knowledge in an Information Society," 165.
[105] Ellul, "Technology and Democracy," 44.

themselves. Moreover, those who hold information determine what part of the information, if any, is shared with citizens. As filtration of information increases, it is less likely that citizens will have the complete story and less likely that citizens will make well-informed decisions.

In a technologically mediated democracy, information should not flow only in one direction; citizens should also have the ability to create information. But living in an information society does not guarantee equal access to information or the right to disseminate alternate information. Graham Thomas and Sally Wyatt point out that the supposed equalization that the Internet was to bring to individuals and organizations was only in the *potential* for access. To actually create a web site that can compete, both technologically and aesthetically, requires considerable resources.[106] Thus, citizens require considerable resources in skill, money, and bandwidth to create and disseminate information that opposes the official version offered by government or corporate interests. Steven Clift explains that the Internet is a meritocracy and that the right of representation is not assumed. The solution, he argues, is to jump into the fray: "We need to not only state the justification for a standard or open-source solution, but also write and codes solutions that make our technical goals a reality."[107] The solution for representation in the information society is the same, but this cannot be done without knowledge and information.

---

[106] See Graham Thomas and Sally Wyatt, "Access Is Not the Only Problem: Using and Controlling the Internet," in *Technology and in/Equality: Questioning the Information Society*, ed. Sally Wyatt, et al., 21-45 (London: Routledge, 2000), 35.

[107] Steven Clift, "An Internet of Democracy," *Communications of the ACM* 43, no. 11 (2000): 31.

If information is a necessary component of democratic practice, the commodification of information is an alarming development. Even if information is widely available on the Internet, there is also the issue of access to the Internet, which is another form of commoditizing information. Although Schement argues that one component of an information society is widely diffused information technology, this diffusion is unequally distributed. Michael Margolis and David Resnick conclude, "The evidence shows that those who have been powerful in the past—the established organizations, the wealthy, and the privileged—are moving into cyberspace and taking their advantages with them."[108] If the primary means of information distribution becomes the Internet, the digital divide is not simply a problem of access—those without access will be denied full citizenship.

Access to Information Technologies

Norman Solomon argues that "there's nothing inherently democratizing about the Internet."[109] In fact, the Internet can be used to *decrease* information and dialogue. Solomon points out that there was little media attention when the World Bank planned to hold meetings in cyberspace rather than in a physical location in Barcelona Spain: "In a managerial world, disruption must be kept to an absolute minimum. If global corporatization is to achieve its transnational potential, the discourse among power brokers and their favorite thinkers can happen anywhere at once—and nowhere in

---

[108] Michael Margolis and David Resnick, *Politics as Usual: The Cyberspace "Revolution"* (Thousand Oaks, CA: Sage Publications, 2000), 208.
[109] Norman Solomon, "Hiding out in Cyberspace," *The Humanist* 61, no. 4 (2001): 17.

particular. Let the troublemakers try to interfere by doing civil disobedience in cyberspace!"[110] But this is exactly what is happening; people are engaging in online protest. John Clark and Nuno Themudo argue that "the Internet has allowed previously opaque processes of intergovernmental negotiations to become demystified and accessible. Citizens now feel quite well informed and empowered to intervene in these processes. Dot causes provide the opportunity."[111] Even so, Solomon's point remains—the Internet can be used to both increase dialogue and exclude dissidents.

The public view of cyberspace seems contested at best. Moore explains that there are two images of cyberspace: a commercialized version and one that "has to do with sinister hackers, wacko bomb conspirators, and lurking paedophiles. Those of us who use the net daily find such stories ludicrous and unrepresentative, but because we dismiss such stories we may not realize that for much of the general population, that's all they hear about today's internet."[112] The latter image has severe consequences for online freedom of information: "The average Joe Citizen, spoon-fed by the mass media, all too often holds the opinion that the internet is a haven of perverts and terrorists, and thus internet restrictions are not met with the same public outcry that would accompany, for example, newspaper censorship."[113]

---

[110] Ibid.
[111] Clark and Themudo, "The Age of Protest: Internet-Based 'Dot-Causes' and the 'Anti-Globalization' Movement," 117.
[112] Moore, "Democracy and Cyberspace," 48.
[113] Ibid., 42.

For many citizens the Internet is an alien environment. Margolis and Resnick point out that early on, the Internet was not very user-friendly.[114] Even now, with public concern over viruses, hackers, spyware, identity theft, and browser hijacks, the Internet may *still* seem like a dangerous environment. Still, there are those who firmly believe that the structural architecture of the Internet provides liberatory potential. Lewis Friedland argues that "as networks become structurally decentralized, even wider publics gain access to them in ways that lead to an increase in the rate and density of public exchange."[115] Dick Morris takes a slightly different tack on the idea of structure: "Every medium has an essence, an intransitive essence, that it communicates regardless of the content that is being sent out over that medium. . . . If you understand what that essence is as a new medium comes on the political scene, you can exploit it to be far ahead of your rival."[116] Morris goes on to explain what he believes to be the essence of the Internet:

> The essence of the Internet is that it permits you to speak, that it makes a monologue into a dialogue and the essence of the media, the message of the media of the Internet is interactivity and dialogue, and that enforces a discipline on the sender of the communication which is called customisation and responsiveness, and it will totally change the method by which we govern, by which we run for office, by which we lobby those who are in office, and they will all be centred around the fundamental concept that what has for years been a

---

[114] See Margolis and Resnick, *Politics as Usual: The Cyberspace "Revolution,"* 206.
[115] Lewis A Friedland, "Electronic Democracy and the New Citizenship," *Media, Culture & Society* 18, no. 2 (1996): 187.
[116] Dick Morris, "The Future of Political Campaigning: The American Example," *Journal of Public Affairs* 3, no. 1 (2003): 14.

> monologue—sustained by newspapers, sustained by pamphlets, sustained by speeches, sustained by radio, sustained by television—is now a dialogue, and that is indeed a "pluro-logue," if you will.[117]

If Morris's "pluro-logue" is to become a reality, access to the online public forum must extend to all citizens. Citizens must be able to access and comprehend information as well as generate it. Because of the structural constraints of the Internet and the commodification of information, citizens may have access to information (although it may be processed and filtered) but they may not have a reasonable chance of being heard. Steve Jones states, "Perhaps it is the case that the Internet allows us to shout more loudly, but whether our fellows listen, beyond the few individuals who may reply, or the occasional lurker, is questionable, and whether our words will make a difference is even more in doubt."[118]

The Interconnection of Individuals and Institutions in an Information Society

The advent of the information age provides opportunities for change in the ways that individual citizens, governments, and other organizations interact and function. Tim Jordan states that "the one area where cyberspace has undoubtedly brought political change is in the emergence of a global system that restructures the power of the nation-state. Finances flowing across national borders show little regard for the interests of the nation-state they flow through. Information spreading instantly throughout cyberspace

---

[117] Ibid., 15.

[118] Steve Jones, "The Internet and Its Social Landscape," in *Virtual Culture: Identity and Communication in Cybersociety*, ed. Steve Jones, 7-35 (London: Sage Publications, 1997), 30.

evades controls that are more easily put in place on nationally based, centralised broadcast media."[119] Jordan further argues that "cyberspace undermines nation-states to the extent that nation-states can no longer exist in isolation, simply pursuing policies congenial to their national constituencies."[120] Nation states are not the only entities that wield power. Current interpretation of the Fourteenth Amendment grants corporations a kind of personhood status.[121] Although they cannot legally vote, corporations have a voice in American politics through campaign contributions, lobbying, and helping to draft legislation.[122] In an information society, citizens, governments, corporations, and non-governmental organizations are intertwined.

---

[119] Tim Jordan, *Cyberpower: The Culture and Politics of Cyberspace and the Internet* (London: Routledge, 1999), 162.

[120] Ibid.

[121] For more on the idea of corporate personhood, see Natasha N. Aljalian, "Fourteenth Amendment Personhood: Fact or Fiction?" *St. John's Law Review* 73, no. 2 (1999): 495-540; Jan Edwards and Alis Valencia, "Corporate Personhood and the 'Right' to Harm the Environment," *Peace and Freedom* 62, no. 3 (2002): 10; Rita C. Manning, "Corporate Responsibility and Corporate Personhood," *Journal of Business Ethics* 3, no. 1 (1984): 77-84; Robert J. Rafalko, "Corporate Punishment: A Proposal," *Journal of Business Ethics* 8, no. 12 (1989): 917-28; P. Eddy Wilson, "Corporations, Minors, and Other Innocents - a Reply from R. E. Ewin," *Journal of Business Ethics* 13, no. 10 (1994): 761-74. The notion of corporate personhood is problematic in the sense that corporations enjoy many rights of citizens, yet also receive special protections not offered to individuals. Transnational corporations provide a way to examine the networked, decentralized nature of the information age.

[122] This can take place actively or tacitly. Sandra Braman and Stephanie Roberts discuss how Internet Service Provider acceptable use policies are being used to shape media law, even though some policies may not be in harmony with Constitutionally granted protections on privacy and freedom of expression. See Sandra Braman and Stephanie Roberts, "Advantage ISP: Terms of Service as Media Law," *New Media & Society* 5, no. 3 (2003): 422-48. A more active example is Vice President Cheney's energy task force. A Government Accountability Office report states "In developing the *National Energy Policy* report, the NEPDG Principals, Support Group, and participating agency officials and staff met with, solicited input from, or received information and advice from nonfederal energy stakeholders, principally petroleum, coal, nuclear, natural gas, and electricity industry representatives and lobbyists. The extent to which submissions from any of these stakeholders were solicited, influenced policy deliberations, or were incorporated into the final report cannot be determined based on the limited information made available to GAO." See Government Accountability Office, "Energy Task Force: Process Used to Develop the National Energy Policy," (Washington, DC: Government Accountability Office, 2003), 2. The distressing part of this report is that the GAO, a non-partisan group responsible for performing investigations and audits on behalf of Congress, was denied access to information it was clearly entitled to by Vice President Cheney. The courts

Structural changes are shifting the balance of power between the state, the citizenry, and other organizations. In their discussion of datacoupling (the integration of databases), Bekkers and Van Duivenboden found that although the citizen has become more "transparent" it seems that the state has not experienced a similar level of transparency.[123] Transparency of citizen information is troubling in light of the inadequate levels of security afforded this information.[124] Information technologies simultaneously allow for more government secrecy and less privacy for individual citizens. Richard Moore discusses the increasing ability for both governmental and corporate surveillance due to the paper trails created through such actions as filling out forms and the inherent security flaws in the programming of the databases.[125] Philip Howard discusses the problematic use of data mining by governmental officials as well as Political Action Committees (PACs), explaining that "even if some citizens initially gave consent for the use of their political information, most would not have consented to

---

ruled against the GAO, so even now it is not clear who was helping to set the United States energy policy and to what extent private concerns trumped the public good.

[123] Bekkers and Duivenboden, "Democracy and Datacoupling," 222-223.

[124] For example, a laptop was stolen from the University of California Berkeley which contained information on over 98,000 former graduate students and applicants. The laptop was eventually recovered, but the potential for identity theft was a great concern. See Charles Burress, "Berkeley / Cal Issues Alert About Stolen Laptop Computer / It Contains 98,000 Social Security Numbers -- Notifications to Warn of Identity-Theft Risk," *San Francisco Chronicle*, March 29, 2005. On a more financial note, CardSystems, a credit card processing company, improperly kept data which resulted in 40 million credit card numbers being compromised, with the security check code that is supposed to deter fraudulent use. See Eric Dash, "Lost Credit Data Improperly Kept, Company Admits," *New York Times*, June 20, 2005; Neil Sutton, "Security Breach Exposes Holes in Credit Card System," *Computing Canada* 31, no. 10 (2005): 1, 12. But why break in and steal the information when you can simply buy it? ChoicePoint sold access to 145,000 consumer records to thieves who presented themselves as small business owners. See Bill Husted, "Crooks Duped Data Archive Alpharetta Firm Sold Personal Information to Fake Companies," *The Atlanta Journal - Constitution*, February 16, 2005; Tom Zeller, Jr., "Release of Consumers' Data Spurs Choicepoint Inquiries," *New York Times*, March 5, 2005. The media description of the incident as data theft, therefore, is misleading and serves only to remove the blame from the company that sold the information.

[125] See Moore, "Democracy and Cyberspace."

its continuous aggregation and application in unexpected ways."[126] Howard describes some of the loopholes that government officials and special interest groups use to circumvent privacy protections afforded to citizens, explaining that "most of these firms have compiled their digital resources without the explicit or informed consent of the people in the databases, and even though some of the data is from public records, a significant amount of it is *not.* In other words, most of the data is not being used in ways that we would imagine serve a public interest. On the contrary, combining various sources of information paints a highly detailed picture of our private interests."[127]

Martin points out that "in the past, a primary safeguard on privacy has been inefficiency. Government records have been uncollated, uncentralized, erratic, inaccessible, difficult to interpret, and often erroneous. It was expensive to collect and store data. The separate files were not interconnected or cross-referenced. With computers, that is changing."[128] The knowledge that government agencies and corporate interests have of the citizenry is becoming more intimate, but it does not appear that this trend is matched in the other direction. If anything, the government seems to be providing less information, classifying it in the name of national security.[129] Thus, while individuals, government, and institutions are becoming more interconnected, the relationships between them are not becoming more transparent.

---

[126] Philip N. Howard, "Deep Democracy, Thin Citizenship: The Impact of Digital Media in Political Campaign Strategy," *The Annals Of The American Academy Of Political And Social Science* 597, no. 1 (2005): 166.
[127] Ibid.
[128] Martin, *The Wired Society*, 255.
[129] By classifying information, the federal government, especially the executive branch, can avoid scrutiny of their actions. Since the events of September 11, 2001, it seems easier to withhold information in the interest of national security. See "Government Secrecy Continued to Rise in 2004"; Shane, "Since 2001, Sharp Increase in the Number of Documents Classified by the Government."

If the state refuses to become transparent, then citizens should have a similar right to opacity. Yaman Akdeniz argues that although law enforcement agencies often frame anonymity as a way to protect criminal activity, anonymity is an essential component for free speech, allowing for open expression of ideas and such activities as allowing dissidents to speak out concerning human rights abuses in oppressive regimes.[130] Some information is required in order for government agencies to function, but with the explosion of databases containing information about citizens, it seems difficult to strike a balance between having enough information to perform the function required and allowing for individual privacy. James Martin explains that this tension comes from conflicting values held by government agencies and individual citizens: "The problem with 'privacy' is its conflict with other social values, such as competent government, a free press, protection against crime, health care, provision of services, collection of taxes, social and medical research, and the development of community living environments. The authority providing each of these wants to decide what it should know about us and when it should be told. We, on the other hand, resent the intruding official eye."[131]

Although the state has more potential access to information, it is not necessarily in a better position to use this information. Ellul asks, "How can people who are incompetent make important decisions with regard to technique? Here, of course, ordinary citizens are in exactly the same place as the politicians, who are also perfectly incompetent."[132] In their discussion of congressional bureaucracy and specialized offices

---

[130] Yaman Akdeniz, "Anonymity, Democracy, and Cyberspace," *Social Research* 69, no. 1 (2002): 223-37.
[131] James Martin, *The Wired Society* (Englewood Cliffs, NJ: Prentice-Hall, 1978), 250.
[132] Ellul, "Technology and Democracy," 43.

such as the Office of Technology Assessment, Alvin and Heidi Toffler state, "Our elected representatives know less and less about the myriad measures on which they must decide and are compelled to rely more and more on the judgment of others. The representative no longer even represents him or herself."[133] Without an understanding of how technology works, citizens and government officials are ill-equipped to make rational, well-informed decisions concerning its implementation and governance. This can lead to poor policy at best and complete miscarriages of justice at worst.

Dawn Nunziato provides a detailed explanation of unintended consequences of information policy in her discussion of Internet Corporation for Assigned Names and Numbers (ICANN). She argues that ICANN policies restrict freedom of speech, specifically anonymous or critical speech.[134] She provides examples of pro-trademark-holder bias in disputes concerning sites such as vivendiuniversalsucks.com and burlingtondeathfactory.com.[135] She also notes that ICANN's policies make it difficult to appeal through the United States court system because there is a window of only 10 days to lodge a court appeal before the decision is considered final and binding.[136] Most citizens are unaware of these issues, content to surf the web as the struggle for control over cyberspace continues without them.

Citizen ignorance of technological aspects of cyberspace can have lasting consequences. One example of this is the case of "William," who was accused and

---

[133] Toffler and Toffler, *Creating a New Civilization: The Politics of the Third Wave*, 96.
[134] Dawn C Nunziato, "Freedom of Expression, Democratic Norms, and Internet Governance," *Emory Law Journal* 52, no. 1 (2003): 187-279.
[135] Ibid., 208-213.
[136] Ibid., 98n.

convicted by a jury for hacking.[137] What William actually did was perform a port scan on a server, which consists of sending queries to a server to see what ports will allow traffic to pass. Shane Lunceford, a network security professional, explains port scanning in non-technical terms:

> The ports on your server are like having 20 doors on your business. Port scanning is just checking to see if the door opens without walking in. You may actually open the door, but you don't enter. The thing is, these doors are open to the public. Bots and spiders are always checking ports to see just what info you have on your computer or server. If you have something, it is indexed and assumed to be public. That is, if they can actually get in, which they will try to do. Having said that, port scanning is typically the beginning of an attack. There is little use to port scanning besides either tightening security or breaching security. The difference in William's case was that he was only curious to see if the application worked. He pointed it at a place he knew had certain ports open to verify that it picked those up. Unfortunately, his curiosity cost him thousands in supposed damages. I'm sure he would have rather it killed his cat.[138]

Although William did not engage in any unauthorized entrance to any computers, a coincidental server crash later that week led the company that had been port scanned to examine the server logs. When the port scan showed up in the logs, the company assumed that William had hacked them. Despite no proof of unauthorized access,

---

[137] William is an acquaintance of the author's brother. Because it is unlikely that William would like the details of the case published, I refer to him only by his first name to protect his privacy.
[138] Shane Lunceford, phone conversation with author, July 25, 2005.

William was convicted. To put this into perspective, this would be similar to convicting a person of grand theft auto because a witness testified that the suspect had opened a car door, shut the door, and walked away. Because the citizens on the jury were uninformed, they rendered an incorrect verdict that injured the defendant financially and left him with a criminal record. With current legislation that defines hacking as cyberterrorism, the consequences of technological ignorance are now even higher.[139]

Identity and Citizenship in an Information Society

In addition to relational and structural changes enabled by the formation of the information society, there are also possible changes in individual identity. Gregory Stock explains that "biologically, humans have changed little since the beginning of civilization, so *theoretically* we could get along quite well on our own. But socially, people have changed so much that most of us—especially urban dwellers—could not survive in the wilds without modern devices."[140] Not only is society changing, the citizen is changing—in the words of Nicholas Negroponte, we are becoming digital: "It is here. It is now. It is almost genetic in its nature, in that each generation will become more digital than the preceding one."[141] Scholars refer to the rising generation as Generation Y or the Net-Generation and note changes within this generation that may affect citizenship

---

[139] See *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001*, Public Law 107–56, 107th Cong. 1st sess. (October 26, 2001), § 814, 816.
[140] Gregory Stock, *Metaman: The Merging of Humans and Machines into a Global Superorganism* (New York: Simon & Schuster, 1993), 47.
[141] Nicholas Negroponte, *Being Digital* (New York: Knopf, 1995), 231.

and democratic practice: the transcendence of national identity in favor of global allegiances; the ability to embody multiple personas; and the perception of cyberspace as reality.[142]

Sherry Turkle explains that cyberspace allows for a malleability of identity that is hard to perform in the physical world.[143] Leopoldina Fortunati makes a similar argument: "In post-modern society, the social system of differences developed in the modern age is being completely restructured. Many differences, even between men and women, or more specifically, between the world of production and reproduction, have disappeared, or are at least less clear cut. There is a tendency at the social level to fusion, to the formation of hybrids, to the development of similarity. Many of these differences are artificial constructions, the result of historical, social, and cultural determinations."[144] Although this may seem overstated, Turkle describes how individuals construct for themselves alternate personas and that these personas are not viewed as artificial, but as legitimate components of personal identity.[145] Ollivier Dyens argues that "the virtual being is real, but of a different kind of real, one that is both organic and technological.

---

[142] See Barbara Costello, Robert Lenholt, and Judson Stryker, "Using Blackboard in Library Instruction: Addressing the Learning Styles of Generations X and Y," *The Journal of Academic Librarianship* 30, no. 6 (2004): 452-453; Louis Leung, "Impacts of Net-Generation Attributes, Seductive Properties of the Internet, and Gratifications-Obtained on Internet Use," *Telematics and Informatics* 20, no. 2 (2003): 107-29; Louis Leung, "Net-Generation Attributes and Seductive Properties of the Internet as Predictors of Online Activities and Internet Addiction," *CyberPsychology & Behavior* 7, no. 3 (2004): 333-48; Don Tapscott, *Growing up Digital: The Rise of the Net Generation* (New York: McGraw-Hill, 1998); Angela Weiler, "Information-Seeking Behavior in Generation Y Students: Motivation, Critical Thinking, and Learning Theory," *The Journal of Academic Librarianship* 31, no. 1 (2005): 46-53.

[143] See Turkle, *Life on the Screen: Identity in the Age of the Internet.* See esp. chap. 7, "Aspects of the Self."

[144] Leopoldina Fortunati, "The Human Body: Natural and Artificial Technology," in *Machines That Become Us: The Social Context of Personal Communication Technology*, ed. James Everett Katz, 71-87 (New Brunswick, NJ: Transaction Publishers, 2003), 79.

[145] See Turkle, *Life on the Screen: Identity in the Age of the Internet.* See esp. chap. 7, "Aspects of the Self."

This being is a cultural animal, a nonorganic being. The cultural being is in a new stage of evolution."[146]

This shift in consciousness has implications for how individual citizens process information. Barbara Costello, Robert Lenholt, and Judson Stryker describe generation X and Y learners:

> As consumers of information, students expect to find what they need quickly and effortlessly, which is why students turn to the Web for their research needs. In the superficial approach to research, students want only the information they need for their course assignments; they have no interest in learning how information is structured or organized, or in learning the traditional linear research process. As characterized by the Web, knowledge fragmentation leads students to pull pieces of information from a variety of Web sites without an overall context for the subject matter and without knowing the validity of the Web based information obtained in this way. Knowledge fragmentation impedes critical, objective thinking on the part of the student.[147]

McGee argues that the fragmentation of culture is now reflected in discursive practices and that the construction of rhetorical texts is now the work of individuals who piece together fragments of text and context.[148] Costello, Lenholt, and Stryker describe how Generation Y learners perform this behavior, piecing together fragments of evidence to

---

[146] Ollivier Dyens, *Metal and Flesh: The Evolution of Man: Technology Takes Over* (Cambridge, MA: MIT Press, 2001), 33.
[147] Costello, Lenholt, and Stryker, "Using Blackboard in Library Instruction: Addressing the Learning Styles of Generations X and Y," 452-453.
[148] McGee, "Text, Context, and the Fragmentation of Contemporary Culture," 286-288.

accomplish their tasks with little concern for the validity of the information. Costello, Lenholt, and Stryker state that Generation X and Y students "are not concerned with the theoretical, but with the practical; they are only interested in learning about those resources they will have to use in the present to complete their assignments and succeed in class."[149] For Generation X and Y learners, it is not a matter of understanding or knowing, but simply putting together enough pieces to complete the assignment, similar to what Jason Frand refers to as "Nintendo over logic," or learning mainly by trial and error.[150]

In light of the structural changes inherent in an information society, the implications for democratic practice are staggering. Although it is encouraging that such individuals pull information from many fragmentary sources, without the context for the information or concern for its validity, citizens can easily be misled. It is difficult to see how citizens who are not interested in truly understanding the problems with which they are faced can make the kind of informed judgment required to further the public good. Choosing to proceed by trial and error without an understanding of the problem or the context of the problem increases the chances that the solution will have unforeseen consequences. Although there will always be unintended consequences, they can be reduced by carefully considering the consequences of an action *before* embarking on a particular course. Costello, Lenholt, and Stryker suggest that for Generation X and Y, the emphasis is on accomplishing the task with as little research as necessary rather than

---

[149] Costello, Lenholt, and Stryker, "Using Blackboard in Library Instruction: Addressing the Learning Styles of Generations X and Y," 457.

[150] Jason L. Frand, "The Information Age Mindset: Changes in Students and Implications for Higher Education," *Educause Review*, September/October 2000, 17-18.

crafting a solution that will truly solve the problem. With such an approach, one could easily treat symptoms without ever knowing the disease.

Because of the fragmentary nature of identity, it is possible that citizens may unintentionally mislead others by presenting themselves in a way inconsistent with their physical identities. Even as citizens project themselves into a realm of ideas, Dewey cautions that "ideas belong to human beings who have bodies."[151] And bodies still matter, so long as inequalities and prejudices based on attributes of the body exist in the physical world. Dawn Dietrich points out that "women stand to gain little as quasi-disembodied subjects within a network environment *without reference to the material conditions of their subjectivity*."[152]

But this disconnection from the body also presents opportunities for democratic practice and the enactment of citizenship. Saco explains that "the *true digital persona* . . . exploits the bodiless character of electronic space, allowing one to create one's own alternative identity: indeed, a nonidentity vis-à-vis the embodied individual who constructs it inasmuch as the digital persona need bear no resemblance to one's embodied self. Because online encounters are not face-to-face, none of the usual physical traits and the cultural meanings attached to those traits (e.g., gender, race, affluence) need come into play in our online practices unless we choose to identify ourselves in those terms."[153] Of course this assumes that the creator of the identity provides no information concerning

---

[151] Dewey, *The Public and Its Problems*, 8.
[152] Dawn Dietrich, "Refashioning the Techno-Erotic Woman: Gender and Textuality in the Cybercultural Matrix," in *Virtual Culture: Identity and Communication in Cybersociety*, ed. Steve Jones, 169-84 (London: Sage Publications, 1997), 178.
[153] Saco, *Cybering Democracy: Public Space and the Internet*, 120.

traits that may be considered undesirable in the physical world. Even so, by adopting digital personae, citizens are able to come together as anonymous entities. Richard Sennett connects citizenship with the idea of civility, defining civility as "the activity which protects people from each other and yet allows them to enjoy each other's company. Wearing a mask is the essence of civility."[154] Adopting a digital persona as a kind of mask allows for the kind of impersonal interaction championed by Sennett.

By forming bonds with others based on shared ideas rather than physical attributes or nationality, individuals can potentially bracket out their differences and create communities that transcend geographic and national boundaries. Jan Fernback explains that these bonds can become very powerful and take on a kind of reality for the individual:

> People yearning for some new type of communal bonding, a new form of experiencing human contact, or a new form of social existence within an essentially lawless frontier themselves constitute a dissenting voice on the landscape of cultural experience. For some, their experiential lives in cyberspace, their embrace of the collectivist virtual ideology, and their willingness to follow the norms and social expectations that comprise the virtual social contract constitute a rejection of the overly individualistic character of contemporary American social existence. For these members of the collective (including

---

[154] Sennett, *The Fall of Public Man*, 264.

> hackers, civil libertarians, and anarchists), cyberculture and virtual ideology are real constructs from which meaning is derived."[155]

When cyberspace is reality, what of the nation state that exists in the physical world? As with physical identity, the physical conditions of one's citizenship cannot be altered simply because one projects a different citizenship, physical location, or national identity into the digital realm. One's material conditions are still relevant, even in an information society.

Cyberspace *is* a reality, different from physical reality. The online world allows for ways to practice a different kind of citizenship divorced from the constraints of a particular nation state. In "A Declaration of the Independence of Cyberspace," John Perry Barlow addresses the nations of the physical world:

> Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different. . . . Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion. We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge. Our identities may be distributed across many of your jurisdictions. The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able

---

[155] Jan Fernback, "The Individual within the Collective: Virtual Ideology and the Realization of Collective Principles," in *Virtual Culture: Identity and Communication in Cybersociety*, ed. Steve Jones, 36-54 (London: Sage Publications, 1997), 53.

> to build our particular solutions on that basis. But we cannot accept the solutions you are attempting to impose.[156]

Barlow describes some of the difficulties in governing the digital world. The disconnection from the body in the digital world means that governance in the digital world must take a different form than that of the physical world, which often punishes offenders by placing sanctions on the offender's body in the form of incarceration. Thomas explains that in order to try someone for a crime, a virtual presence is not enough and that "what is always needed is a body, a real body, a live body."[157]

This form of self governance is still in its embryonic state, so only time will tell if Barlow's assertions come to fruition. However, the digital world certainly provides opportunities for a new kind of impersonal community based on ideas rather than physical location or nationality. Despite its solitary appearance in the physical world, when individual citizens communicate with each other online they are participating in public discourse. Jan Fernback explains that the urge for this participation may develop from feelings of isolation: "We might be alone at our computers as we type, but we are participating in some form of public life; the form of public life that comes about after the mistrust of our neighbors and our intense desires for privacy force us to re-examine our atomized lives."[158]

But discourse online is not only public discourse. Jon Anderson describes the Internet as "a sphere of creole discourse and creole journeys, an intermediate sphere

---

[156] Barlow, *A Declaration of the Independence of Cyberspace*.
[157] Douglas Thomas, *Hacker Culture* (Minneapolis: University of Minnesota Press, 2002), 182.
[158] Fernback, "The Individual within the Collective: Virtual Ideology and the Realization of Collective Principles," 38.

between more private worlds and those of public rituals; it is part of a continuum between those along which social actors can move."[159] Discourse in the digital realm is a mixture of public life and private life. Fernback states, "Cyberspace is *public* space; at the same time, cyberspace is *private* space where, via e-mail two users can argue politics or fall in love, or several users on a private listserver can strategize a meeting or discuss the finer points of a classroom lecture."[160] The public and the private spheres are combining in ways that may bode well for citizenship. In this sense, the feminist slogan, "the personal is political," is becoming a reality as politics and private lives become intertwined in the lives of individual citizens. Perhaps this intertwining provides a way for citizens to enact the roles of citizen and consumer as the political becomes more recognizably relevant through interactions in the online public sphere. The public and the private need not be compartmentalized any longer.

Protest and Democracy in an Information Society

Touraine argues that "far from being antithetical, social movements and democracy are, in contrast, indissociable," and living in an information society may place constraints on social movement and protest activities.[161] New social movements are a

---

[159] Jon W. Anderson, "New Media, New Publics: Reconfiguring the Public Sphere of Islam," *Social Research* 70, no. 3 (2003): 901.
[160] Fernback, "The Individual within the Collective: Virtual Ideology and the Realization of Collective Principles," 39.
[161] Touraine, *What Is Democracy?* 57.

mixture of private and public concerns, with identity at the forefront.[162] But Parke Burgess explains that all rhetoric incorporates elements of the personal, even when the aim of protest is political: "The strategies and motives of any rhetoric . . . represent an invitation to a life-style, an invitation to adopt a pattern of strategies and motives, verbal and nonverbal, that determine how men and women will function together in culture."[163] In an information society, where the boundaries between the public and the private spheres have become more permeable, it is no longer enough to consider new social movements as the main outlet for "identity politics." In an information society, all politics are potentially identity politics.

Although combining public and private lives into one political whole is possible, it is not inevitable. Ellul explains that political power comes through individual sacrifice: "If citizens are to experience power, there must be both personal devotion and time set aside for political activity. But here we encounter another obstacle technique creates for democracy. Techniques allow the individual many avenues of escape and diversion, such as motoring about the countryside, which then discourage people from spending long evenings of reflection on large and small-scale community projects or long weekends devoted to working in common on the great political problems. . . . The breed [of political activists] has been destroyed by television and the jalopy."[164] Rod Allen and Nod Miller make this point more explicitly: "If people use their time in front of the screen primarily

---

[162] See Pichardo, "New Social Movements: A Critical Review," 411; Scott, *Ideology and the New Social Movements*, 16-17.
[163] Parke G. Burgess, "The Rhetoric of Moral Conflict: Two Critical Dimensions," *Quarterly Journal of Speech* 56, no. 2 (1970): 120.
[164] Ellul, "Technology and Democracy," 42.

to play games such as *Doom* or *Mortal Combat*, to engage in chat room talk about sex or to do tele-shopping, then yet again the promise of enhanced democratic participation through the new medium is hardly likely to be fulfilled."[165] The multitude of choices available to citizens may be a difficult constraint to overcome. But even with other choices such as entertainment vying for time in the public sphere, civic engagement in an information age can extend to choices in entertainment and consumption of goods and services because the dichotomy between citizen and consumer is no longer clear. Citizens may choose to not patronize a particular establishment because of the establishment's treatment of its workers. Individuals may choose to purchase only clothing that is not made in sweatshops. These are economic *and* political decisions that are often enacted by adherents to the anti-globalization and social justice movements. It is no longer a question of individuals participating in public life *or* pursuing private interests—one can do both simultaneously.

In addition to identity constraints, living in an information society places structural constraints on social movement activities. Perhaps the largest structural shift is the rise of the transnational corporation (TNC) and the non-governmental organization (NGO). One example of this shift can be found in the anti-globalization movement's efforts against the World Trade Organization (WTO). Because the WTO is not held accountable by any one nation, strategies that target elected officials in the protestor's country can have, at best, only an indirect effect—especially if the country to which the

---

[165] Rod Allen and Nod Miller, "Panaceas and Promises of Democratic Participation: Reactions to New Channels, from the Wireless to the World Wide Web," in *Technology and in/Equality: Questioning the Information Society*, ed. Sally Wyatt, et al., 46-60 (London: Routledge, 2000), 60.

protestors belong is not very powerful. The anti-globalization movement has adopted different strategies of protest that are not dependent on reaching elected officials, such as creating media events, building coalitions between other social movements such as the labor movement and environmentalists, and using the Internet to recruit and organize adherents.[166] New communication technologies are playing a key role in these strategies. In their study of the anti-globalization movement's protest efforts against the WTO's 1999 meeting in Seattle, Peter Van Aelst and Stefaan Walgrave found that "the fluid, non-hierarchical structure of the Internet and that of the international protest coalition prove to be a good match."[167] Lewis Friedland also notes the importance of network structure: "As networks become structurally decentralized, even wider publics gain access to them in ways that lead to an increase in the rate and density of public exchange."[168]

Cyberspace's potential use for social movements transcends specific protest actions or discourse in real time—it also serves as an online history. Fernback states, "Cyberspace is a repository for collective cultural memory—it is popular culture, it is narratives created by its inhabitants that remind us who we are, it is life as lived and reproduced in pixels and virtual texts. It is sacred and profane, it is workspace and leisure

---

[166] See Kevin Michael DeLuca and Jennifer Peeples, "From Public Sphere to Public Screen: Democracy, Activism, and the 'Violence' of Seattle," *Critical Studies in Media Communication* 19, no. 2 (2002): 125-51; Jeffrey S. Juris, "The New Digital Media and Activist Networking within Anti-Corporate Globalization Movements," *The Annals Of The American Academy Of Political And Social Science* 597, no. 1 (2005): 189-208; Richard Kahn and Douglas Kellner, "New Media and Internet Activism: From the 'Battle of Seattle' to Blogging," *New Media & Society* 6, no. 1 (2004): 87-95; Peter Van Aelst and Stefaan Walgrave, "New Media, New Movements? The Role of the Internet in Shaping the Anti-Globalization Movement," *Information Communication & Society* 5, no. 4 (2002): 465-93.

[167] Van Aelst and Walgrave, "New Media, New Movements? The Role of the Internet in Shaping the Anti-Globalization Movement," 487.

[168] Friedland, "Electronic Democracy and the New Citizenship," 187.

space, it is a battleground and a nirvana, it is real and it is virtual, it is ontological and phenomenological. . . . Cyberspace is essentially a reconceived public sphere for social, political, economic, and cultural interaction."[169] Social movements may not be able to change how they are covered by the news media, but the Internet provides a space to respond and reframe their actions. Lynn Owens and L. Kendall Palmer found that anarchists used their system of websites to engage in damage control when they received unfavorable coverage of their protest actions.[170]

Information technologies allow for new modes of protest. This dissertation focuses on one specific form of technologically mediated protest—hacktivism—and the hacker movement. If new communication technologies are to revolutionize democracy, these technologies must be used in revolutionary ways. Because hackers are creating technology and continually examining and adapting it, they comprise the group most likely to fulfill this requirement. Those who create technology infuse those technologies with particular values; Lessig provides an example of this:

> The architecture of cyberspace is the real protector of speech there; it is the real 'First Amendment in cyberspace,' and this First Amendment is no local ordinance. . . . For over fifty years, the United States has been the exporter of a certain political ideology, at its core a conception of free speech. Many have criticized this conception: some found it too extreme, others not extreme enough. . . . And yet, as if under cover of night, we have now wired these nations with an

---

[169] Fernback, "The Individual within the Collective: Virtual Ideology and the Realization of Collective Principles," 37.
[170] Owens and Palmer, "Making the News: Anarchist Counter-Public Relations on the World Wide Web."

architecture of communication that builds within their borders a far stronger First Amendment than our ideology ever advanced. Nations wake up to find that their telephone lines are tools of free expression, that e-mail carries news of their repression far beyond their borders, that images are no longer the monopoly of state-run television stations but can be transmitted from a simple modem. We have exported to the world, through the architecture of the Internet, a First Amendment in code more extreme than our own First Amendment in law.[171]

[171] Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999), 166-167.

Chapter 3

Building a Hacker Collective Identity

Inquisitiveness and a desire to push the boundaries of what something can do comprise the essence of hacking. Jon Erickson states, "There are some who will still argue that there is a distinct line between hackers and crackers, but I believe that anyone who has the hacker spirit is a hacker, despite what laws he or she may break."[172] To hack is to ask the question, "I wonder if I can make this do something else?" Steven Levy describes the MIT Tech Model Railroad Club as an early hacker group because they modified and incorporated discarded telephone equipment into their existing model railroad systems.[173] This is an excellent example of hacking that does not conform to the vernacular usage of the term.

How a group is defined may have serious consequences and a particular group's self-definition is not the only possible definition. Hackers have been defined by themselves, the mass media, government and law enforcement agencies, and legislation. All of these may have different criteria for inclusion and exclusion. Even within the hacker community, definitions of what it means to be a hacker are contested. Majid Yar points out that "the contested nature of the terms [hacking and hackers] is, however, worth bearing in mind, for a good criminological reason. It shows how hacking, as a form of criminal activity, is actively constructed by governments, law enforcement, the

---

[172] Jon Erickson, *Hacking: The Art of Exploitation* (San Francisco: No Starch Press, 2003), 4.
[173] Stephen Levy, *Hackers: Heroes of the Computer Revolution* (New York: Penguin, 1984), 21-27.

computer security industry, businesses, and media; and how the equation of such activities with 'crime' and 'criminality' is both embraced and challenged by those who engage in them."[174] Questions of definition are important—especially when such definitions carry the possibility of a prison sentence.

There are many myths concerning hackers. When people think of a hacker, they have a particular image in mind. But the myth of the basement dwelling, teenage hacker subsisting on pizza and Jolt cola who does nothing but hack into computer systems all over the world while wearing a black, unwashed T-shirt that reads "Got Root?" is just that—a myth. Like most myths, there is some degree of truth within the myth. But myth is a dangerous thing—on one hand, it allows one to gain some insight into the collective identity of a group. On the other hand, it can be too easy to accept myth at face value and forget the underlying meaning behind the myth. For example, hackers may consume a disproportionate amount of caffeine when compared to the rest of society.[175] It is easy to simply dismiss this as a quirk of a particular subculture but there is utility in the use of caffeine that has a coherent logic within the subculture. When hacking (or coding) there are often stretches where the work must be done over long periods of time with little interruption. Caffeine allows hackers to remain awake during times of protracted hacking when the process cannot wait until the next morning.

---

[174] Majid Yar, "Computer Hacking: Just Another Case of Juvenile Delinquency?" *The Howard Journal of Criminal Justice* 44, no. 4 (2005): 390.

[175] I have not found any study to back this particular claim up. I have only my experience in the computer industry and my conversations with hackers to buttress my claims. However, it is not just me that has clued into the affinity that the computer sector has for caffeine. Jinx (http://www.jinx.com/), a commercial website that caters to the gamer/hacker/geek crowd, has an entire section devoted to caffeinated products.

There is a myth that hackers break into computer systems because they want to intrude on other networks or steal information such as credit card numbers or passwords. There may be other motivations that lead hackers to hack. Some hackers are interested in computer security. Others may simply want to know that they can access a particular network—in other words, it is not the actual utility of accessing a network, but the potential of realizing that utility if necessary.[176] There are also lesser acknowledged professional interests. Many hackers are also computer industry professionals. In other words, the people who build word processing programs, Internet browsers, and computer systems are the same people who are interested in breaking into the code of these programs and systems to examine how they can be made more efficient and more secure. There are hackers who are interested in stealing credit card information or passwords, but this is not the motivation of all hackers. Unfortunately, this is the motivation that has received the most attention.

As a whole, hackers are interested in understanding the program or network at its most intricate level. However, there are also those in the hacker community that are less interested in understanding the code than in recognizing what the code can do for them. Here I refer to the subculture known as "script kiddies." Virtually anyone with a moderate degree of computer literacy and an Internet connection can be a script kiddie. Exploitation scripts are readily available on the Internet. One need only download a script and start trying to run it on servers. This group is looked at with some derision because

---

[176] Anonymous hacker, phone conversation with author, February 20, 2006.

they simply use existing scripts rather than creating their own hacks.[177] However, they are an important group to consider in the question of how democratic practice occurs in an online environment. Many people engaged in hacktivism would likely fall under the banner of script kiddie, even though they may not identify with the term, considering themselves to be hackers.

Script kiddies seem to identify as hackers even though those who consider themselves the "true" hackers would disagree. This identity crisis may keep hackers from creating a coalition based on common ground as they squabble over what it means to be a "real" hacker. In no sense do I wish to diminish the importance of self-definition. Building a shared collective identity is important for any social movement. But other entities, such as the government and the media, have already formulated definitions of "hackers" and "hacking" that have little to do with the supposed split between script kiddies and "real" hackers and these definitions carry severe consequences

Despite the intricacies of hacker identity, some core tenets can be distilled through the hacks and their own writings. *Phrack*, an online hacker journal, and especially the manifesto, "The Conscience of a Hacker," also known as the "Hacker Manifesto," provide hackers with a way of seeing themselves and their place in the world. This is done by reporting on and defining certain exigencies that spurred hackers into creating a shared identity, shaping them into the movement that they have become today. Hackers have become rhetorically constructed as terrorists in government and

---

[177] The term "script kiddie" can be used in multiple ways. Although it is often a term of derision, it can also be used as a term of endearment among hackers. Perhaps this is similar to the use of "dyke" as both a slur and a term of pride within the lesbian community. Zaft, personal communication with author, June 10, 2005.

media discourses. Offensive maneuvers such as Operation Sundevil provided the catalyst that helped move the hacker movement from adolescence into a politically motivated group of hacktivists, cognizant of their place in society and understanding, to some degree, the power that they wield in society as masters of the arcane arts of technology.

The Rhetorical Construction of the Hacker as Terrorist

H. P. Lovecraft wrote, "The oldest and strongest emotion of mankind is fear, and the oldest and strongest kind of fear is fear of the unknown."[178] Entire industries have emerged to protect government, industry, and individuals from the specter of the hacker. The engine driving this industry is fear, specifically fear of those who understand technology and have the ability and means to shape it to their own ends. But are hackers really the ones to fear? What truly makes hackers frightening to government and industry (more so than to individual computer users) is their ability to avoid surveillance and thus undermine the ability of the state and industry to maintain control over the populace. Thus, it is in the interest of the state to eliminate, or at the very least demonize, hackers. What is at stake here is freedom—freedom to gain information, freedom of motion, freedom from surveillance. Michel Foucault explains, "Liberty is a *practice*."[179] By evading the panoptic gaze, hackers are practicing liberty and this liberty makes them a threat to society.

---

[178] Howard Phillips Lovecraft, "Supernatural Horror in Literature," in *Dagon, and Other Macabre Tales*, ed. S. T. Joshi, 365-436 (Sauk City, WI: Arkham House, 1965), 365.
[179] Michel Foucault and James D. Faubion, *Power*, trans. Robert Hurley (New York: New Press, 1994), 354.

Hackers challenge government notions of individual privacy and freedom from surveillance, the role of technology in American society, and the embedded structures of power that allow state and corporate interests to undertake massive campaigns of surveillance on both American citizens and the digitally connected world as a whole. If the system of surveillance is to stand, hackers *must* be defined as terrorists because it is in the interest of the state to maintain more power than the citizenry. If hackers are able to level the playing field and become equally armed in the realm of electronic warfare and surveillance, the state must do what it can to demonize the knowledgeable few and maintain the ignorance of the masses. This demonization of the hacker is necessary to maintain America as a technological / information / panoptic society.[180] The framing of hackers as terrorists or potential terrorists through congressional testimony and news reports has implications not only for hackers, but for all social movements that challenge government and corporate power.

---

[180] I am reluctant to completely subscribe to the idea that the United States currently exists in an information age, but it seems to be moving toward that end of the spectrum. While it is clear that information plays a significant part in American society, it is equally clear that the United States has not completely escaped the age of machines. As it stands now, the chasm between those who have access to information and those who do not is still far too wide and even those who have access to information often lack the media literacy skills to appropriately use this information. Throughout this section, I will use the term "information society" more as shorthand to describe the idea that the United States is heavily reliant upon the information infrastructure and places a high premium on the value of ideas, fiercely protecting them in the name of the public good, even when it is actually in the service of corporate interests. See Chris Sprigman, "The Mouse That Ate the Public Domain: Disney, the Copyright Term Extension Act, and Eldred V. Ashcroft," *FindLaw*, March 5, 2002. http://writ.news.findlaw.com/commentary/20020305 _sprigman.html (accessed September 1, 2005).

The Hacker and the Creation of the National Information Infrastructure

Stephen Segaller describes the formation of the Internet as "one of the twentieth century's most productive accidents," further explaining that the "seeds of the Internet were planted by the U.S. government in the wake of nationwide concern over the Soviet launch of *Sputnik.*"[181] Hackers were an integral part of the construction of this network; Douglas Thomas traces the origins of the computer hacker to the computer programmers of the 1950s and 1960s.[182] For the most part, these programmers worked in universities on projects funded almost exclusively by the government. These programmers were instrumental in the formation of ARPANet, created as a communication system that could be used in the event of a nuclear attack. Neil Randall points out that while ARPANet was a military venture, there are several interpretations of the origins of ARPANet, including a decidedly non-military version that explains ARPANet as a way to develop a network that people wanted anyway. After all, he explains, it was the height of the Cold War and military spending was at an all time high and by framing a project as useful for the military, one could more easily gain funding.[183]

The hackers of today who are considered a threat to national security would not even exist without the military's attempt to use the hackers of yesterday in the interest of national security. Moreover, it was the hackers' desire to push the envelope of what could be done with information and technology that made them useful to the military in the first place. Today's Internet grew out of ARPANet, and hackers had worked on government

---

[181] Stephen Segaller, *Nerds 2.0.1: A Brief History of the Internet* (New York: TV Books, 1998), 29.
[182] Thomas, *Hacker Culture*, 12-14.
[183] Neil Randall, *The Soul of the Internet* (London: Thompson Publishing Inc., 1997), 1-18.

and military projects prior to ARPANet.[184] In this light, the military and the hacker are intertwined, at least in terms of origin.

Information Society / Panoptic Society

Technology has created the possibility of, and, to an extent, the need for, the panoptic surveillance society.[185] The scope of human surveillance is limited by both time and space. Adding computers and networking technology increases the potential for surveillance exponentially. The panopticon works as a tool of surveillance not because individuals are actually under surveillance, but because of the *potential* of being under surveillance.[186] Bogard argues that the reach of the panopticon has increased through technology: "With the proliferation of electronic sensors, codes, and databases, with information availability in "real time," all that happens is that the Panopticon becomes a Superpanopticon . . . a metastasis of the gaze that no longer probes the individual body but instead now "leukemizes" the entire social body."[187]

---

[184] For a history of the transformation from ARPANet to the Internet, see Peter H. Salus, *Casting the Net: From Arpanet to Internet and Beyond* (Reading, MA: Addison-Wesley, 1995).

[185] The original idea of the panopticon was conceived by Jeremy Bentham as a model for a circular prison in which the inmates were constantly under surveillance in a ring surrounding a darkened central watch tower. Thus, the inmates could always be seen while the guards were never seen. See Jeremy Bentham, *Panopticon; or, the Inspection-House: Containing the Idea of a New Principle of Construction Applicable to Any Sort of Establishment, in Which Persons of Any Description Are to Be Kept under Inspection: And in Particular to Penitentiary-Houses, Prisons, Houses of Industry ... And Schools: With a Plan of Management Adapted to the Principle: In a Series of Letters, Written in the Year 1787* (London: T. Payne, 1791). For a critical discussion of Bentham's panopticon, see Michel Foucault, *Discipline and Punish: The Birth of the Prison*, trans. Alan Sheridan, 2nd Vintage Books ed. (New York: Vintage Books, 1995), 195-228.

[186] See Greg Elmer, "A Diagram of Panoptic Surveillance," *New Media & Society* 5, no. 2 (2003):232-233.

[187] William Bogard, *The Simulation of Surveillance: Hypercontrol in Telematic Societies* (New York: Cambridge University Press, 1996), 71. Bogard parenthetically cites Mark Poster, *The Mode of Information: Poststructuralism and Social Context* (Chicago: University of Chicago Press), 85ff.

Both the state and industry have a heavy reliance on information. America is shifting from an industrial economy to an information economy; information is now the good itself rather than the means of producing the good.[188] The focus on information is woven into every aspect of American society. Our lives are a patchwork of PIN numbers, Social Security numbers, computer passwords, credit bureaus, and official documents. Forging a passport and opening a few credit cards in someone else's name is referred to as "identity theft." Are we no more than the sum of our records? Perhaps not to friends and family, but in a bureaucracy, we *are* the sum of our records. In this situation, it is one's *constructed/official*, identity that has been stolen. Once it has been formed, the individual has little control over his or her constructed identity because in bureaucratic relationships others construct this identity. This constructed identity is important not only to the individual, but to the efficient operation of industry and the State.

Profit is one reason for corporate surveillance. The more a salesman knows about a customer, the easier it is to pitch a particular product to that customer. William Bogard describes the staggering amount of records maintained by government and business organizations, stating that these records form a massive decentralized database.[189] Corporate interests then use this information to tailor products to the consumer, which, advocates argue, benefits the consumer. But with this stockpiling of information comes the possibility that these databases may be compromised, which is troubling in light of

---

[188] See Bell, *The Coming of Post-Industrial Society: A Venture in Social Forecasting;* Castells, *The Rise of the Network Society*; Schement and Curtis, *Tendencies and Tensions of the Information Age: The Production and Distribution of Information in the United States*.

[189] Bogard, *The Simulation of Surveillance: Hypercontrol in Telematic Societies*, 70.

the inadequate level of security afforded such information.[190] When these databases are breached, information becomes exposed—information that the individual may not have even known that the company had. Unfortunately, some industry leaders seem to ignore privacy concerns. Scott McNealy of Sun Microsystems bluntly stated, "You have zero privacy anyway. Get over it."[191] In this climate, individual privacy is experiencing a full-frontal assault through the recent upsurge in "spyware" programs that may include not only tracking programs, but also keyloggers.[192] Privacy erosion and personal data collection can also take place outside of the digital domain through such programs as reward / loyalty programs that require you to register a credit card to acquire points toward airline frequent flyer mileage or products. These forms of surveillance have become commonplace. The information found in credit bureaus, medical history, and

---

[190] For example, a laptop was stolen from the University of California Berkeley which contained information on over 98,000 former graduate students and applicants. The laptop was eventually recovered, but the potential for identity theft was a great concern. See Burress, "Berkeley / Cal Issues Alert About Stolen Laptop Computer / It Contains 98,000 Social Security Numbers -- Notifications to Warn of Identity-Theft Risk." On a more financial note, CardSystems, a credit card processing company, improperly kept data which resulted in 40 million credit card numbers being compromised, with the security check code that is supposed to deter fraudulent use. See Dash, "Lost Credit Data Improperly Kept, Company Admits"; Sutton, "Security Breach Exposes Holes in Credit Card System." But why break in and steal the information when you can simply buy it? ChoicePoint sold access to 145,000 consumer records to thieves who presented themselves as small business owners. See Husted, "Crooks Duped Data Archive Alpharetta Firm Sold Personal Information to Fake Companies"; Zeller, Jr., "Release of Consumers' Data Spurs Choicepoint Inquiries." The media description of the incident as data theft, therefore, is misleading and serves only to remove the blame from the company that sold the information.

[191] Edward Yourdon, *Byte Wars: The Impact of September 11 on Information Technology* (Upper Saddle River, NJ: Prentice Hall PTR, 2002), 71.

[192] Spyware is often bundled with other programs. For example, a person could download a program that displays current weather information on their desktop, but included in the installation of the program are several other programs that the user has not chosen to install. These "hidden" programs may track the user's Internet surfing or gather other data about the user. This information is then transmitted to a server and retrieved by the company or person that manages the program. Often, the end user does not realize that his or her computer is infected with spyware. Keyloggers are programs that have the ability to record every keystroke that the user makes, which can reveal such things as passwords and credit card numbers. Tracking programs gather a detailed history of the user's Internet surfing, recording, for example, sites that the user has visited and for how long.

other databases that, taken together, comprise one's official identity can be used to target customers more efficiently and sold to other corporate interests. In some circumstances, government and law enforcement officials can demand access to this information.

Although corporate surveillance is a vexing concern, Jay Stanley and Barry Steinhardt explain that "only the government has the power to take away liberty—as has been demonstrated starkly by the post-September 11 detention of suspects without trial as 'enemy combatants.'"[193] This statement illustrates some of the logic behind the demonization of deviant groups. If the government can define hackers as terrorists, they no longer have the rights of citizens, but rather, the meager protection afforded to enemy combatants. To successfully define hackers as terrorists, the government must also convince citizens that this definition of hackers is accurate.

Although hackers may not appear to be "enemy combatants," they do pose a real threat to governmental control. As architects and masters of the information infrastructure, hackers are often able to undermine the panoptic system of control by understanding when they are actually under surveillance. Thomas relates the story of Kevin Poulsen, who, after discovering that he was under investigation, "hacked into the FBI's systems and discovered a maze of wiretaps and electronic surveillance programs that were monitoring everything from the restaurant across the street from him to (allegedly) Ferdinand Marcos."[194] Poulsen was eventually apprehended after someone recognized him from a profile on *Unsolved Mysteries*. Thomas argues that "Poulsen's

---

[193] Jay Stanley and Barry Steinhardt, "Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society," *American Civil Liberties Union*, http://www.aclu.org/FilesPDFs/aclu_report_bigger_monster_weaker_chains.pdf (accessed April 18, 2006), 7.
[194] Thomas, *Hacker Culture*, 214.

discovery, and therefore his threat, was the ability to know, at any given moment, who was and was not being watched."[195]

Thomas explains that another way hackers evade the panoptic gaze is by disconnecting themselves from the body: "The virtual presence of the hacker is not enough to constitute a crime—what is always needed is a body, a real body, a live body."[196] Those who can free themselves from the body and escape into the digital domain are threatening to the offline/analog society. Yvonne Jewkes and Keith Sharp state that the Internet "can liberate its users from the usual constraints of corporality."[197] A number or a digital presence is more difficult to trace than a physical body. As a digital presence, one can enter into places impossible to access with the physical body.

But panoptic control is not always used as a means for imposing sanctions. Elmer points out that "the panoptic diagram, in other words, only disciplines consumers if they actively seek out the unfamiliar, the different, the previously unseen, purchased, or browsed."[198] The panoptic gaze can actually enable consumers to receive more of what they desire—so long as that desire conforms to pre-determined norms, determined by corporate and state interests. Once these desires become transgressive or deviate from the norm, punishment is likely, whether direct (law enforcement officials may come to one's door if he or she requests illegal information or material) or indirect (the material or information desired is more difficult or impossible to find, or becomes prohibitively

---

[195] Ibid.
[196] Ibid., 182.
[197] Yvonne Jewkes and Keith Sharp, "Crime, Deviance and the Disembodied Self: Transcending the Dangers of Corporeality," in *Dot.Cons*, ed. Yvonne Jewkes, 1-14 (Portland, OR: Willan Publishing, 2002), 3.
[198] Elmer, "A Diagram of Panoptic Surveillance," 245.

expensive). Lawrence Lessig makes the link between cost and access more explicit: "A regulation need not be absolutely effective to be sufficiently effective. It need not raise the cost of the prohibited activity to infinity in order to reduce the level of that activity quite substantially. If regulation increases the cost of access to this kind of information, it will reduce access to this information, even if it doesn't reduce it to zero."[199] Although Lessig is discussing material such as sexually explicit content, the principle holds true for any information or material that a person wishes to acquire.

Although some scholars describe the panoptic potential of networks such as the Internet,[200] others argue that networks have the potential to serve as sites of resistance.[201] But if one has little or no access to networks, how can he or she resist? Even if there is potential for liberation through networks, this potential will be squandered for much of the population. Because hackers may gain access to many networks, they are one of the few groups able to resist the panoptic gaze and realize the liberatory potential of networks.

Hackers have found a way to watch back, but this is not only an attribute of hackers. Green argues that "our modern society is, by definition, obsessed with surveillance and (covert) knowledge of the social realm."[202] He concludes that there is a "move away from the image of a central eye to a conception of decentred surveillance,

---

[199] Lawrence Lessig, "The Zones of Cyberspace," *Stanford Law Review* 48, no. 5 (1996): 1405.
[200] See John Edward Campbell and Matt Carlson, "Panopticon.Com: Online Surveillance and the Commodification of Privacy," *Journal of Broadcasting & Electronic Media* 46, no. 4 (2002): 586-606.
[201] See Stephen Green, "A Plague on the Panopticon: Surveillance and Power in the Global Information Economy," *Information Communication & Society* 2, no. 1 (1999): 26-44.
[202] Ibid., 37.

consisting of multiple glances from different agents, often operating informally."[203] Rather than existing as a system of control wielded by the state, surveillance is also increasingly used by corporations, protestors, and private citizens. The panoptic society is in flux; the gaze is everywhere.

From Nerd to Nemesis: Constructing the Hacker as Terrorist

The hacker has been considered a threat for quite some time, but the nature of the threat has evolved. In 1989, the Air Force Satellite Control Network System Program Office for Sustaining Engineering issued a pamphlet titled *The Hacker Threat*, in which hackers are viewed more as a nuisance than a terrorist threat, and noted that hackers often use low-tech means to gain access to systems such as searching trash cans for printouts—methods that are still used today.[204] The way into a computer system is often not through technology but through people. Why break in to a computer system when one can simply call someone who has access to the network and ask for his or her login and password?[205]

Some argue that hacking is merely theft or espionage under a different name and through a (sometimes) different medium. Winn Schwartau bluntly states, "Graffiti on

---

[203] Ibid., 38.

[204] Air Force Satellite Control Network System Program Office for Sustaining Engineering, "The Hacker Threat," (Washington, DC: Air Force Satellite Control Network System Program Office for Sustaining Engineering, 1989), 9.

[205] For more on social engineering, see Hackers of Planet Earth, "Social Engineering," in *Information Warfare: Cyberterrorism--Protecting Your Personal Security in the Electronic Age*, ed. Winn Schwartau, 360-66 (New York: Thunder's Mouth Press, 1996); Sverre H. Huseby, *Innocent Code: A Security Wake-up Call for Web Programmers* (New York: John Wiley & Sons, 2004), 105-106; Kevin D. Mitnick and William L. Simon, *The Art of Deception: Controlling the Human Element of Security* (Indianapolis, IN: Wiley, 2002).

billboards, graffiti on web sites, same difference, different medium."[206] But Marshall McLuhan reminds us that the medium matters.[207] The widespread fear of hackers illustrates some of the ways that society views technology and information, and the medium is a component of this view.

The view of hackers today has shifted—hackers are no longer seen as simply a nuisance; they are now potential terrorists with the ability to destroy computerized systems from the relative anonymity of the ether. Gone is the explanation that the user can be partially at fault for computer system insecurity. With the shift to an information economy comes the possibility that information can be used as a weapon. Marshall McLuhan, Quentin Fiore, and Jerome Agel state that "real total war has become information war."[208] The military has become increasingly dependent on electronic systems and cryptography plays a large role in military operations.[209] This helps to explain the federal government's attempts to suppress cryptographic programs for individual users, such as PGP (Pretty Good Privacy), and bans on the exportation of software that contains encryption components to certain nations.

The rhetorical construction of the hacker as terrorist begins with definitions of the term "terrorist." Ayn Embar-Seddon states that "a terrorist is an individual who employs

---

[206] Winn Schwartau, *Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Destruction* (New York: Thunder's Mouth Press, 2000), 25.
[207] See Marshall McLuhan, *Understanding Media: The Extensions of Man*, 1st MIT Press ed. (Cambridge, MA: MIT Press, 1994).
[208] Marshall McLuhan, Quentin Fiore, and Jerome Agel, *The Medium Is the Massage: An Inventory of Effects* (San Francisco, CA: HardWired, 1996), 138.
[209] For discussion on the military uses of electronic warfare, see D. Curtis Schleher, *Electronic Warfare in the Information Age* (Boston: Artech House, 1999); Sergei A. Vakin, Lev N. Shustov, and Robert H. Dunwell, *Fundamentals of Electronic Warfare* (Boston: Artech House, 2001). For an excellent overview of the role cryptography has played in past wars, see Don E. Gordon, *Electronic Warfare: Element of Strategy and Multiplier of Combat Power* (New York: Pergamon Press, 1981), 14-25.

terrroristic means to achieve political and social ends. A cyberterrorist is a terrorist who uses hacking skills to achieve terroristic ends. Their motivation is the normal terrorist motivation of political change, with a willingness to resort to violence to bring about that change."[210] This definition seems too simplistic—essentially, a terrorist is one who does things like a terrorist. In the wake of the events of September 11, 2001, government officials seem quick to place many offenses under the umbrella of terrorism. One of the concerns that the American Civil Liberties Union expressed concerning the USA PATRIOT Act is "an overly broad definition of 'terrorism' which includes activities that no reasonable person would consider terrorist activities."[211] Social movements sometimes operate outside of the law in order to enact change and may even resort to violence. Franklyn Haiman explains, "It would seem that even the 'rhetoric of the riot,' mindless and indiscriminate as it may be, has its positive function in contemporary America."[212]

The main difference between a criminal act and a terrorist act seems to be the nature of the threat and what is threatened. A common thug threatens an individual; a terrorist threatens society. Hackers threaten organizations, corporations, nation states, and societal institutions. Hacking may be viewed as a terrorist act because it undermines the social structure and the potential for governmental surveillance and control of the citizenry. If all citizens understood how to evade surveillance, it is possible that

---

[210] Ayn Embar-Seddon, "Cyberterrorism: Are We under Siege?" *The American Behavioral Scientist* 45, no. 6 (2002): 1037.

[211] American Civil Liberties Union, "Despite Significant Improvements, ACLU Says House Bill Fails to Protect Liberty," *American Civil Liberties Union*, October 4, 2001. http://www.aclu.org/NationalSecurity/NationalSecurity.cfm?ID=9782&c=24., para 3 (accessed December 13, 2003).

[212] Franklyn S. Haiman, "The Rhetoric of the Streets: Some Legal and Ethical Considerations," *Quarterly Journal of Speech* 53 (1967): 105.

governments would have to abandon the current illusion of freedom in favor of more direct and immediate control mechanisms.

The idea that hackers threaten established systems of control is illustrated in an exchange between Attorney General John Ashcroft and Representative (NC) Howard Coble in a hearing before the House Committee on the Judiciary to discuss the proposed Anti-Terrorism Act of 2001:

> Attorney General ASHCROFT. Well, I thank the Congressman. First, to the question as to whether computer crimes could rise to the level of or could be categorized as terrorist acts, when you think about the utilization of computers in terms of air traffic control, you can imagine the chaos that could come from the disruption of that system if we had an assault launched through a computer virus or some other infection in the computer infrastructure, not to mention other very serious controls in our culture that relate to other infrastructure, whether it be power grids, power generation supplies and the like.
>
> Mr. COBLE. Yeah. I wanted that on the record, General, because some folks might think that was too far-reached. I just wanted it on the record.[213]

Ashcroft refers to "very serious controls in our culture that relate to other infrastructure, whether it be power grids, power generation supplies and the like." Computer infrastructure is important not only because Americans rely on it to automate processes that the average person no longer understands, but also because it is a mechanism for control in our culture. Ashcroft ties computer infrastructure to other

---

[213] House Committee on the Judiciary, *Administration's Draft Anti-Terrorism Act of 2001: Hearing before the House Committee on the Judiciary*, 107th Cong., 1, 2001, 30-31.

infrastructure, arguing that an attack on the computer infrastructure is also an attack on other infrastructure, such as power grids and power supply. Implicit in this argument is the assertion that an attack on computer infrastructure is an attack on governmental power and control. Without the computer infrastructure, the power grid—both physical and governmental—is rendered useless. The National Commission on Terrorism states, "Cyber attacks are often considered in the same context with CBRN [chemical, biological, radiological, or nuclear threat]."[214] Following this logic, hackers have the same potential for societal disruption as a nuclear bomb.

This hyperbole filters down from the government through the news media to crystallize fear of the hacker into the public mind.[215] Vegh describes the consequences of media and government portrayals of the hacker:

> [Anti-hacking legislation] also protects the government from any other political dissent, or at least gives them the power to monitor their citizens, as well as it protects businesses from loss revenue from "copyleft," "peer-to-peer," and "open source" initiatives. Perhaps it is only sensationalist reporting by newspapers to sell more copies. Yet, it influences public opinion, creates a negative image of hacking, online political activism, free software and other counter-corporate-cultural movements, blurs the boundaries of cyberactivism and cyberterrorism,

---

[214] National Commission on Terrorism, "Countering the Changing Threat of International Terrorism," *National Commission on Terrorism*, August 2, 2000. http://www.gpo.gov/nct/nct3.pdf., 5 (accessed February 21, 2006).

[215] For some examples of media sensationalism, see Gerald L. Kovacich, "Hackers: Freedom Fighters of the 21st Century," *Computers & Security* 18, no. 7 (1999): 573-76; Paul A. Taylor, *Hackers: Crime in the Digital Sublime* (London: Routledge, 1999), 176-79; Sandor Vegh, "Hacktivists or Cyberterrorists? The Changing Media Discourse on Hacking," *First Monday* 7, no. 10 (2002), http://www.firstmonday.org/issues/issue7_10/vegh/index.html.

> and consequently prompts unwarranted restrictive legislation, induces misguided policy-making, and causes the curtailment of civil liberties.[216]

Vegh paints a bleak picture of how the portrayal of hackers affects everyone in the form of misguided policy making and curtailment of civil liberties. In the mass media, it is generally taken for granted that hackers are criminals. In news reports, hackers are bent on stealing identities and destroying power grids, finance systems, air traffic control systems, and society as a whole. The print media frames hackers through two major themes, disruption and the ease with which hackers can wreak havoc.

The lead paragraph in an article in *American Banker* concludes with a quote from testimony before the House Financial Services Committee: "[Treasury Assistant Secretary for Financial Institutions Wayne Abernathy] said these assaults [on banks] have progressed 'from computer hackers and pranksters into theft and now, we believe, on to schemes to disrupt the operations of our financial systems.'"[217] Disruption is a recurring theme in articles discussing hacking and terrorism. Tom Ridge is quoted in the St. Louis *Post Dispatch*: "'Terrorists know that a few lines of code could ultimately wreak as much havoc' as a physical attack, Ridge told about 350 industry executives at the National Cyber Security Summit. 'The enemies of freedom use the same techniques as hackers do . . . and we must be as diligent and determined as the hackers.'"[218] Ridge subtly conflates

---

[216] Vegh, "Hacktivists or Cyberterrorists? The Changing Media Discourse on Hacking," conclusion, para. 2.
[217] Rob Blackwell, "Treasury Exec: Banks Face New Cyber Enemies," *American Banker*, September 9, 2004, 3.
[218] The Associated Press, "Ridge Seeks Tech Companies' Support," *St. Louis Post - Dispatch*, December 4, 2003.

hackers and the "enemies of freedom." Moreover, he touches on the other recurring theme concerning hackers—that a few lines of code can bring down society as we know it.

In an opinion editorial in the *Washington Post*, Valery E. Yarynich, a retired army colonel and professor at the Russian Academy for Military Sciences, writes: "Could a U.S. Minuteman missile be launched without authorization? How do we defend the cable, radio and satellite communications channels on both sides from interception that could lead to the cracking of key launch codes? Have we adequately isolated control of nuclear weapons from both military and civilian computer networks, so that hackers cannot penetrate them? There already have been cases in which military networks were compromised."[219] Yarynich describes what hackers have always known—networks are intrinsically insecure. The American public seem to hold a tacit belief that the networks that control nuclear weapons and other military systems are secure but Yarynich explains that we have no way of knowing because individual nation states jealously guard the architecture of these systems.[220] While there is some logic in this, it matters little if one's own architecture is secure if others' are not.

The "12-year-old hacker problem" is another recurring theme of media coverage of hackers. For example, in a *Houston Chronicle* article, James Farnan, deputy assistant director of the FBI's cyber division, states, "Using a simple Internet search, a 12-year-old

---

[219] Valery E. Yarynich, "The Ultimate Terrorism," *The Washington Post*, April 30, 2004.
[220] Ibid.

could locate a variety of hacker tools, then download and implement them."[221] This is not so far fetched. *The Washington Post* reports that "in 1998, a 12-year-old hacker, exploring on a lark, broke into the computer system that runs Arizona's Roosevelt Dam. He did not know or care, but federal authorities said he had complete command of the SCADA system controlling the dam's massive floodgates."[222]

The print media sometimes agree with the hacker-as-terrorist conflation but this is not the case for all journalists. Some news stories explain that there are other motivations to hack that, while criminal, stop far short of terrorism. For example, in an article about cyberattacks on power suppliers, Charles Piller reports: **"**Although a concentration of attacks come from countries identified with terrorist groups, [Tim Belcher, former cyber-security consultant for the Defense Department] cautioned that many such countries are major energy producers—suggesting that the hacks may be the product of more mundane industrial espionage, rather than terrorism. Similarly, Hong Kong—a key financial center—is a hotbed for cyber attacks on the financial services industry, he said."[223] Even so, this would still be defined as terrorism under the USA PATRIOT Act, even if terrorism is not the result or the desired outcome but rather financial gain or corporate espionage.[224]

---

[221] David Ho, "Ex-Convict Tells Lawmakers Hackers Seek 'Weakest Link,'" *Houston Chronicle,* April 4, 2003.
[222] Barton Gellman, "Cyber-Attacks by Al Qaeda Feared; Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say," *The Washington Post*, June 27, 2002.
[223] Charles Piller, "Hackers Target Energy Industry; Computers: Attacks at Power Companies Are up Substantially. Some Experts Blame Industrial Spying and Mischief, Others Fear Terrorism," *Los Angeles Times*, July 8, 2002.
[224] See *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001*, § 814, 816.

Judith Miller reports in the *New York Times* that Richard A. Clarke, former National Security Advisor "feared that civil rights might be eroding in the struggle against terrorism. 'When we sacrifice our civil liberties and privacy rights, the terrorists win because they have gotten us to change the nature of our country,' he said. Despite having fought terrorism for more than 11 years, he said, 'I have never seen one reason to infringe on privacy or civil liberties.'"[225] But with legislation such as the USA PATRIOT Act, the definition of the term "terrorist," and the extent to which the government will go to catch them, is shifting. For example, the FBI's "Carnivore" device can retrieve not only the email of suspected criminals but *all* traffic that travels through a particular Internet Service Provider (ISP).[226] However, the FBI will not allow outside institutions or individuals, or even the ISP on whose network the FBI would be installing it, to examine the device.[227]

Although the plight of hackers may seem inconsequential to most law-abiding citizens, Vegh points out that the demonization of hackers has implications for all groups that engage in electronic activism: "The simple injection of colorful terminology, such as cybervandalism, cyberterrorism, or malicious hackers, disregards the motives and goals

---

[225] Judith Miller, "Departing Security Official Issues Warning," *New York Times*, February 2, 2003.

[226] See Wayne Madsen, "Carnivore Documents Reveal Enhanced Tapping Abilities," *Network Security* 2001, no. 1 (2001): 5.

[227] For more on Carnivore, see Talitha Nabbali and Mark Perry, "Going for the Throat: Carnivore in an Echelon World -- Part I," *Computer Law & Security Report* 19, no. 6 (2003): 456-67; Talitha Nabbali and Mark Perry, "Going for the Throat: Carnivore in an Echelon World - Part II," *Computer Law & Security Report* 20, no. 2 (2004): 84-97. The details of the Carnivore system are now moot because the FBI has recently discontinued use of Carnivore in favor of commercially available surveillance technology, which is even more disconcerting. See Kevin Poulsen, "FBI Retires Its Carnivore," *SecurityFocus*, January 14, 2005. http://www.securityfocus.com/news/10307 (accessed February 22, 2006). Even so, the secrecy which surrounded the project and the willingness to consider massive surveillance as an acceptable means of law enforcement is illustrative of the current atmosphere in law enforcement.

of online activism and puts those socially or politically progressive but marginalized voices whose main chance to be heard is through the Internet even more to the peripheries."[228] Hackers have been dehumanized, demonized, disembodied, feared, and misunderstood. The hacker is surrounded by myth; sometimes they are depicted as having almost superhuman powers over technology. Maura Conway explains that "the US Department of Justice labeled Kevin Mitnick, probably the world's most famous computer hacker, a 'computer terrorist.' On his arraignment, Mitnick was denied access not only to computers, but also to a phone, because the judge believed that, with a phone and a whistle, Mitnick could set off a nuclear attack."[229] Understanding how hackers actually operate would probably lessen irrational fear of the unknown and perhaps help government and industry to create more secure networks. Mary Ann Davidson, Director of Security Product Management for Oracle Corporation, testified that "hackers, 98 percent of whom really just want bragging rights when they break into your system, they don't intend to use the information maliciously. It's important for companies to use that type of thought processes to defend their own systems, very much like the Department of Defense conducts war games."[230]

---

[228] Vegh, "Hacktivists or Cyberterrorists? The Changing Media Discourse on Hacking," para. 7.
[229] Maura Conway, "Hackers as Terrorists? Why It Doesn't Compute," *Computer Fraud & Security* 2003, no. 12 (2003): 13.
[230] Subcommittee on Commerce, Trade, and Consumer Protection of the Committee on Energy and Commerce, *Cyber Security: Private-Sector Efforts Addressing Cyber Threats*, 107th Cong., 1, November 15, 2001, 31-32.

The Consequences of Constructing the Hacker as Terrorist

Debora Halbert claims that American society is growing increasingly dependent on technology.[231] Tom Ridge, as director of the Department of Homeland Security, revealed the consequences of this dependence: "Our 21st century global economy and the 21st century technologies on which it relies are vulnerable to new threats of cyber terrorism."[232] Dependence on technology coupled with a lack of understanding of this technology fuel fear of the hacker. Langdon Winner refers to the way that people seem to willingly cede power to technology as "technological somnambulism," going through life refusing to critically assess technology.[233] In this sense, technology wields power over society; it stands to reason that those with power over technology may wield power over society through technology.

Demystifying technology is the first step toward diminishing the fear of hackers in the eyes of the general public. There are criminal hackers who are terrorists and one should not have a cavalier attitude toward network security. Dangerous hackers exist, and a healthy level of skepticism online and an understanding of tactics used by hackers can protect the average computer user from having his or her system compromised. But an understanding of risk is far different from the paralyzing fear generated by an over-hyped portrait of hackers. The vast majority of the population will never have their personal

---

[231] Debora Halbert, "Discourses of Danger and the Computer Hacker," *Information Society* 13, no. 4 (1997): 368.
[232] House Select Committee on Homeland Security, *H.R. 5005, the Homeland Security Act of 2002, Days 1 and 2: Hearing before the House Select Committee on Homeland Security*, 107th Cong., 2, July 15-16, 2002, 8.
[233] Langdon Winner, "Technologies as Forms of Life," in *Technology and Values*, ed. K. S. Shrader-Frechette and Laura Westra, 55-69 (Lanham, MD: Rowman & Littlefield, 1997), 61.

computers compromised by hackers because most people are just not that interesting. Yet many people still buy into the hype—literally. For $49.99, one can purchase Norton Personal Firewall 2006, "your primary line of defense against hackers, automatically locking out intruders and protecting your identity and data while you're on the Internet."[234] Firewalls are important, but the real risk lies not with a particular individual's computer (unless that individual is also a common target for paparazzi photographers and tabloid writers) but rather with corporate and government databases that compile millions of individual records with Social Security numbers, credit bureaus, and other personal identifying information.[235]

It is easy to fear hackers when the arguments concerning them are so confusing and riddled with contradictions. Computer networks are so insecure that a 12-year-old could take them down with tools readily available on the Internet, yet most Americans believe that this technology is beyond their understanding. Cyberattacks that can easily be explained as white collar crime are framed as terrorist acts. Jacques Ellul explains that there is often a disconnect between what people believe and how they behave, arguing

---

[234] Symantec Corporation, "Norton Personal Firewall: Product Overview," 2006, http://www.symantec.com/home_homeoffice/products/internet_security/npf2006/index.html (accessed March 10, 2006).

[235] For example, a laptop was stolen from the University of California Berkeley which contained information on over 98,000 former graduate students and applicants. The laptop was eventually recovered, but the potential for identity theft was a great concern. See Burress, "Berkeley / Cal Issues Alert About Stolen Laptop Computer / It Contains 98,000 Social Security Numbers -- Notifications to Warn of Identity-Theft Risk." On a more financial note, CardSystems, a credit card processing company, improperly kept data which resulted in 40 million credit card numbers being compromised, with the security check code that is supposed to deter fraudulent use. See Dash, "Lost Credit Data Improperly Kept, Company Admits"; Sutton, "Security Breach Exposes Holes in Credit Card System." But why break in and steal the information when you can simply buy it? ChoicePoint sold access to 145,000 consumer records to thieves who presented themselves as small business owners. See Husted, "Crooks Duped Data Archive Alpharetta Firm Sold Personal Information to Fake Companies"; Zeller, Jr., "Release of Consumers' Data Spurs Choicepoint Inquiries." The media description of the incident as data theft, therefore, is misleading and serves only to remove the blame from the company that sold the information.

that the propagandist exploits this disconnect.[236] In American society, the dissonance between people's lived experiences online and the fantasy construction of what hackers are capable of is smoothed over by the demonization of the hacker. Hackers are not like normal people—hackers are "enemies of freedom" with skills far surpassing the abilities of the average person. The unquestioned assumption of malevolent intent is problematic. This seems to illustrate what George Gerbner et al. refer to as the "mean world syndrome."[237] Gerbner and his colleagues found that heavy viewers of television were more likely to view the world as a dangerous place. In the case of television, law enforcement agencies, not the television show producers, were the beneficiaries of this fear. In the case of cyberspace, it seems that the federal government, mass media, and the computer security industry are hyping the danger of the Internet—the groups who would most benefit from this fear.[238] Much as the fictional television world differs from the much less violent reality of life, cyberspace is not as dangerous as it is portrayed.

Society is changing and with this change often comes fear of the unknown and unexpected. As society evolves, technology is a part of that evolution; technology shapes society and society shapes technology. But real individuals and entities are involved in this process and technology reflects their desires. An elevator is a manifestation of a

---

[236] Jacques Ellul, *Propaganda: The Formation of Men's Attitudes*, trans. Konrad Kellen and Jean Lerner (New York: Knopf, 1965).

[237] George Gerbner et al., "Growing up with Television: Cultivation Processes," in *Media Effects: Advances in Theory and Research*, ed. Jennings Bryant and Dolf Zillmann, 43-68 (Mahwah, NJ: Lawrence Erlbaum Associates, 2002), 52.

[238] Although the government and computer security industry may seem obvious beneficiaries, it is easy to forget that the news media and the Internet industry are deeply entwined. Thus, to demonize hackers, who pose a threat to the media's monopoly on information dispersal, is in the best interest of the mass media. For more on the vertical integration of media, see McChesney, *Corporate Media and the Threat to Democracy*; Sussman, *Communication, Technology, and Politics in the Information Age*.

desire to not climb stairs. It is also a manifestation that individuals in society wish to maximize the amount of living and working space by going up instead of out, which in turn reflects the value of land. Values and norms can be extrapolated by examining a particular device or idea.[239] As technologies are created, society adapts to them and alters values based on the new environment.

But adaptation to technology comes at a price. Attorney General John Ashcroft described just how vulnerable the United States had become as a result of technological dependence: "As our economy and infrastructure become more dependent on computers, our potential vulnerability to terrorist attacks against our cyber systems grows. The United States relies increasingly upon information technologies and the Internet to conduct business, manage industrial and governmental activities, engage in personal communications, and perform scientific research. These technologies have resulted in enormous gains in efficiency, productivity, and communications and have spurred tremendous growth in the U.S. economy. They have also become essential to our society's ability to function."[240] The last sentence ties the previous elements of Ashcroft's testimony together. Whether current communications infrastructure is necessary to function as a society depends on the nature of the society one wishes to belong to. Hackers occupy a role in the dialectic between technology and society by making this tacit relationship explicit. They understand the danger of relying upon

---

[239] For more on the social construction of technological systems, see Wiebe E. Bijker, Thomas Parke Hughes, and T. J. Pinch, eds., *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (Cambridge, MA: MIT Press, 1987).

[240] House Select Committee on Homeland Security, *Transforming the Federal Government to Protect America from Terrorism: Hearing before the House Select Committee on Homeland Security*, 107th Cong., 2, July 11, 2002, 57-58.

technology. Thomas explains, "Hackers realize that at some level, *all* machines are insecure."[241] This reflective view of technology allows hackers to transcend the technological somnambulism experienced by much of society and recognize that technology need not even appear deterministic. What makes hackers dangerous to society is their willingness and ability to act on this knowledge.

David Gunkel argues that hacking is an intrinsic part of the technological system: "Hacking, like a parasite, takes place in and by occupying and feeding off a host that always and already has made a place for it to take place. It is for this reason that, despite the valiant efforts of law enforcement, hacking cannot be stopped or even hindered by cracking down on and punishing individual hackers."[242] So long as there is a frontier, hackers will explore it. Hackers remind us that technology is ultimately human-driven. It is not something that is "out there" in a black box; technology can be understood.

Rather than trying to demonize the hacker or legislate them out of existence, a more fruitful option for society may be education. This education should be twofold—education about technological systems and education about systems of surveillance. If individuals begin to understand the capabilities and limitations of the technological infrastructure, there may be less irrational fear of hackers and less desire to cede power to government or technology. Understanding systems of surveillance and means of evading them may likewise prove liberating. We already live in an Orwellian society but hackers

---

[241] Thomas, *Hacker Culture*, 88.
[242] David J. Gunkel, *Hacking Cyberspace* (Boulder, CO: Westview Press, 2001), 9.

demonstrate that this need not be the case.[243] Not only can one evade observation, he or she can also watch back. Learning the art of the hacker may undermine the panoptic society but so long as the hacker remains an "enemy of freedom" and a terrorist, the structures of control will remain firmly in place for much of the population.

The urge to conflate "hacker" and "terrorist" is an urge to oversimplify complex social institutions and to find a scapegoat for the limitations of these institutions. It is far easier to demonize hackers who take advantage of intrinsically insecure software than to find ways to make software insecure. Creating a rhetorical construction of hackers as terrorists allows our society to remain in a state of technological somnambulism, ignoring the flaws in our technological system. In the tale of the emperor's new clothes, it is childhood innocence that allows the child to see through the façade of adult pride and recognize that the emperor is naked. Even though the people began to realize that the clothing was just an illusion, the emperor still could not admit it.[244] Hackers fulfill a similar role in society by demonstrating that the technological systems that we have constructed are insecure. By demonizing the hacker, the leaders of our nation can ignore the more complex problems of technological reliance. But eventually, like the

---

[243] This may seem to be a strong claim but there are many means of surveillance in American society such as the widespread use of video cameras in private and public establishments, fingerprinting and the issuance of a unique identifier (Social Security number), and the digital "paper trail" that one leaves behind in almost every commercial interaction. Online presences are recorded and archived; even such mundane things as personal email and chat sessions can be tracked and captured. An ongoing theme in this section is the potential for surveillance in the databases that compile our private and public lives. Information such as credit card transactions, medical data, and public records can be found in databases. Datamining has become a powerful tool both for commercial and political enterprises. I have mentioned the commercial risks of datamining; for more on the political uses of datamining, see Howard, Philip N. "Deep Democracy, Thin Citizenship: The Impact of Digital Media in Political Campaign Strategy." *The Annals of The American Academy Of Political And Social Science* 597, no. 1 (2005): 153-70.

[244] Hans Christian Andersen, "The Emperor's New Suit," in *The Complete Hans Christian Andersen Fairy Tales*, ed. Hans Christian Andersen and Lily Owens, 438-41 (New York: Chatham River Press, 1984).

townspeople who realized that the emperor was naked, our society, as well as our leaders, must recognize that the technological system is digitally naked. Holding on to the rhetorical construction of the hacker as terrorist only allows us to delay that moment of painful realization.

The Creation of a Hacker Movement

There was a time when hackers and government peacefully coexisted. Levy describes the important role that hackers played in government and corporate information technology projects through the 1950s and 60s.[245] Hackers were useful to government and industry for the same reasons that they are now perceived as a threat—hackers are inquisitive, driven by internal rather than external motivations, and refuse to accept boundaries concerning what can and can not be done. Since the early 1980s, the media has expressed a growing sense of unease concerning hackers. Headlines such as "Raising Security Consciousness; A Monthly Guide for Managers that Helps Protect Corporate Data from Assaults by the Hackers," and "The World of Data Confronts the Joy of Hacking," which begins, "The recent electronic escapades of a group of Milwaukee youths have brought national attention to the growing problem of computer security," demonstrate the early concerns over hackers in the media.[246] Eric Raymond explains that "it was also around this time [1984] that serious cracking episodes were first covered in

---

[245] Levy, *Hackers: Heroes of the Computer Revolution*.

[246] Erik Sandberg-Diment, "Raising Security Consciousness," *New York Times*, July 28, 1985; "The World of Data Confronts the Joy of Hacking," *New York Times*, August 28, 1983.

the mainstream press—and journalists began to misapply the term 'hacker' to refer to computer vandals, an abuse which sadly continues to this day."[247]

"Hacker" is a contested term with many shades of difference. Legislation such as the USA PATRIOT Act defines hackers as terrorists. Popular movies portray hackers in conflicting ways; *The Matrix* portrays hackers as saviors of humanity while *The Net* portrays hackers as murderous criminals able to erase and replace another's identity. Popular press and network security journals describe hackers as a threat. Even within the hacker community there are different opinions concerning what constitutes a "true" hacker. Even if hackers were able to agree on a definition, theirs would be only one of many competing definitions; socially constructed views of hackers have considerable weight. The days when the term "hacker" and "elite programmer" were synonymous are long gone, and rightfully so. The mosaic of definitions surrounding hackers reflects the complexity of hacker identity. Hackers are much more than artisan programmers who write elegant code. Hackers exist in the liminal space between the fears and dreams of how technology is shaping society. Rather than accept technology at face value, hackers learn to understand it and shape it to fulfill their own ends. The differences in how hackers are defined reflect different societal views concerning those who control and shape technology.

Other scholars have traced the history of more mainstream hackers.[248] This section provides a kind of alternate rhetorical history of the more subversive element of

---

[247] Eric S. Raymond, *The Cathedral & the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary* (Cambridge, MA: O'Reilly, 1999), 19.

[248] See Levy, *Hackers: Heroes of the Computer Revolution*; Segaller, *Nerds 2.0.1: A Brief History of the Internet*.

the hacker movement through analysis of their own texts, specifically *Phrack*, but also drawing on other hacker texts such as *2600*. These texts demonstrate how the hacker underground evolved from a loose collective to a social movement with a collective identity (albeit contested and constantly in flux) and political motivations. Two defining moments helped this to take place: Operation Sundevil and the arrest of Kevin Mitnick.

In the Beginning There Was *Phrack*

Phrack is one of the most respected online hacking journals. It began November 17, 1985, on the Metal Shop Bulletin Board System (BBS) run by Taran King. *Phrack* is made up of "philes," or text files, which may cover anything from making methamphetamines to highly technical schematics of phone or computer equipment. *Phrack* was not the only group of phile writers—the longest running group of phile writers is Cult of the Dead Cow. The very first phile in *Phrack* states:

> 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 sponsering Phrack Inc., please leave feedback to me, Taran King stating you'd like your BBS in the credits. Later on.[249]

With this simple introduction began one of the most well-known and influential online sources for hacker information and indoctrination and the beginning of the adolescent phase of the hacker movement. The preferred topics include "telcom (phreaking/hacking), anarchy (guns and death & destruction) or kracking," which taps into the current of rebellious male adolescence.[250]

In the first issue of *Phrack*, there is already tension between the serious, technical information and the urge to learn about other illicit information—alongside technical documentation there are philes describing lock picking techniques and the construction of acetylene balloon bombs. In issue two, mingled with an in depth overview of MCI Communications Corporation, which includes such data as subscriber figures and descriptions of various services that they offer, are instructions for how to make homemade guns and blowguns. Issue four contains a phile guiding the reader through the process of making methamphetamines. *Phrack* was living up to its mission statement and seemed geared toward mischievous adolescent males.

---

[249] Taran King, "Introduction," *Phrack* 1, no. 1 (November 17, 1985): phile 1. In all of these philes, I have left spelling as found in the original. Because several of these philes have many spelling and grammatical errors, I have omitted the traditional use of [*sic*] in order to ease readability.

[250] It is important to note that these files indicate an interest in these topics rather than a disposition to actually enact them. When researching the commonly held belief that adolescent males like things like fire and explosives, I was surprised to find that there was little research on *interest* in these topics. Most of the psychological and sociological literature dealt with adolescents that actually displayed seriously antisocial behavior, and rightfully so. Thus, although it seems intuitive, it is difficult to find scholarly literature concerning those who may harbor antisocial feelings or fantasies rather than display them, or those who are simply interested in information deemed dangerous or inappropriate.

But early on in *Phrack*, one can see the beginnings of the end of adolescence and recognition of the sociopolitical world in which hackers existed. An article by The Mentor on crashing DEC-10 computers begins "Occasionally there will be a time when destruction is necessary. Whether it is revenge against a tyrannical system operator or against a particular company, sometimes it is desirable to strike at the heart of a company . . . their computer."[251] In the same volume, an article concerning telephone regulatory changes ends with the following postscript: "The above text was written primarily for people in marketing telephone technologies. In the interest of the phreaking world, I hope that you can focus on the business side of telecommunications which may be in your future."[252] Even in the beginning, some hackers and phreakers understood the larger implications of their actions. They seemed to recognize that these telecommunication systems were embedded within societal systems in which they may, to some degree, fight against and/or become assimilated into. Levy describes hacker after hacker who eventually used his or her skills to work in corporate and government empires. Thus, even in the beginning, there are clues that hackers understood that adolescence would one day fade away.

According to some scholars, the politicization of the hacker is a relatively new phenomenon. Thomas states that hackers had more limited political agendas in the 1970s and 1980s and that at that time most attacks were directed at the phone company. After the breakup of the phone monopoly, this changed: "More recently, in the wake of the

---

[251] The Mentor, "Crashing Dec-10's," *Phrack* 1, no. 4 (March 13, 1986): phile 6.
[252] Leslie Albin and Jester Sluggo, "Centrex Renaissance: 'The Regulations,'" *Phrack* 1, no. 4 (March 13, 1986): phile 7.

AT&T break up, with the rise of the Internet, and with the increasing globalization of technology, hackers have begun to engage in more concerted political action, at both local and political levels."[253] Although not the only causes of the rise in political hacking, or hacktivism, these events may have played a significant part. Thomas identifies Cult of the Dead Cow (cDc) as "the first hacker group dedicated to a kind of political action based on principles of civil disobedience and visibility, and . . . the first group to connect hacker identity with the notion of political action."[254] There are problems with this account of the politicization of the hacker. Political uses of hacking and phreaking can easily be traced back to the early 1970s when the Youth International Party Line (YIPL) advocated ripping off the phone company as a way to avoid paying the War Tax levied on phone bills and providing schematics for blue boxes.[255] Other hacker groups, such as 2600 have also had a political slant from early on. The first issue of *2600* (published in 1984 by Emmanuel Goldstein) includes a list of phone numbers for the White House.[256]

Because unauthorized hacking (which was the main means of access for many early hackers who could not afford the prohibitively expensive computer equipment) has always existed in the nebulous grey area of legality at best (before the law caught up with the possibility of hacking), the act of hacking itself should be considered a political act. With this action comes ideology, which can be seen in their justifications and slogans. Within the slogan "information wants to be free," lies an ideology opposed to the notion

---

[253] Thomas, *Hacker Culture*, 89.
[254] Ibid., 96.
[255] See Al Bell, "Blue Box Is Linked to Phone Call Fraud," *Youth International Party Line*, July, 1971; "Remember the Blue Box?" *Youth International Party Line*, October, 1971. Blue boxes created tones that allowed individuals to use pay phones without paying.
[256] "White House Phone Directory," *2600*, January, 1984.

of commodified, proprietary information. Dan Verton writes, "Hackers look at themselves as Internet-age Robin Hoods, stealing from the information rich to give to the information- and connectivity- starved poor. Their aim is to open up and expose information held closely by corporate America and government and expose the truth. The world's knowledge belongs to the world, not a select few with the money and political influence to claim ownership of it. The freedom of information and knowledge is another core belief of the hacker community."[257]

Even today, in an age of supposedly inexpensive computer equipment and widespread information, there are still many barriers to understanding the internal workings of computer systems. Cost is still a barrier. To understand basic equipment functionality is relatively inexpensive, but to develop more sophisticated hacking techniques requires equipment that would be financially out of reach for most users. There are also barriers erected by legislation and corporate interests. For example, Microsoft Windows is the operating system of choice for a vast majority of computer users. However, it is difficult to understand exactly how it works on a technical level because Microsoft jealously guards the source code. Also, in order to install the program in the first place to examine it, one must agree to the End User License Agreement (EULA), in which the user agrees to not reverse engineer the product. These agreements also apply to Internet connection. Sandra Braman and Stephanie Roberts argue that Internet Service Providers' (ISP) Acceptable Use Policy and Terms of Service agreements are becoming a kind of de-facto law because governments worldwide are

---

[257] Dan Verton, *The Hacker Diaries: Confessions of Teenage Hackers* (New York: McGraw-Hill/Osborne, 2002), 191.

demanding more of ISPs, placing them into a regulatory role, yet allowing ISP regulations that may not be Constitutional.[258] It seems that government agencies that should be regulating these agreements and policies have abdicated their role to the software manufacturers and the ISPs and are allowing them to set precedent. In general, legislation concerning the Internet seems to favor established corporate interests. Dawn Nunziato provides a detailed explanation of overlooked unintended consequences of information policy in her discussion of the Internet Corporation For Assigned Names and Numbers (ICANN). She argues that ICANN policies restrict freedom of speech, specifically anonymous and/or critical speech.[259] Some examples she gives are the pro-trademark-holder bias in disputes concerning sites such as vivendiuniversalsucks.com and burlingtondeathfactory.com.[260] She also notes that ICANN's policies make it difficult to appeal to the U.S. Court system because there is only a window of 10 days to lodge a court appeal before the decision is considered final and binding.[261] In short, physical and legal barriers exist that impede attempts by both average users and experts to gain control over technology. Franklyn Haiman explains that "perhaps the best one can do is to avoid the blithe assumption that the channels of rational communication are open to any and all who wish to use them."[262]

Hackers have long understood the power that comes with understanding technology. Gareth Branwyn put it this way: "One of the first 'a-ha's' I had about

---

[258] Braman and Roberts, "Advantage ISP: Terms of Service as Media Law."
[259] Nunziato, "Freedom of Expression, Democratic Norms, and Internet Governance."
[260] Ibid., 208-213.
[261] Ibid., 98n.
[262] Haiman, "The Rhetoric of the Streets: Some Legal and Ethical Considerations," 114.

computer terrorism in the late '80s was that the possibilities for insurrection and for a parity of power not based on brute force had changed radically with the advent of computer networks and our society's almost complete reliance on them. There was now at least the possibility that groups or individual hackers could seriously compromise the U.S. military and/or civilian electronic infrastructure."[263] Michael Synergy, a hacker, echoes this point: "Anyone who was around in the Sixties is aware of the concept that all political power comes from the barrel of a gun and the power to control is the power to destroy. . . . Now, with information tools, people like me have the capability and the access—because of the way the system is structured—to shut everything down—not just locally, but globally. And, it's getting worse every day."[264] But it is not only hackers that have the power to engage in digital resistance. In a sense, hackers serve as Promethean figures, bringing the ability to utilize the tools of the hacker to the general population by releasing exploits and packaging hacking tools with easy to use interfaces.[265] This has helped to spawn a new subset of hackers—script kiddies—who are not necessarily interested in the inner workings of the machines, but rather in what these exploits and scripts can accomplish. Although hackers tend to view script kiddies with derision, hackers have made it possible for them to exist. However, script kiddies are often the ones who attempt to transform technical knowledge into political action.

---

[263] Gareth Branwyn, introduction to *Secrets of a Super Hacker* by The Knightmare (Port Townsend, WA: Loompanics Unlimited, 1994), iii.
[264] A. J. S. Rayl, "Secrets of the Cyberculture," *Omni*, November 1992, 67.
[265] For example, to participate in the electrohippies denial of service attack on the World Trade Organization's website during the 1999 WTO meeting in Seattle, one needed only to access a website.

Social movements that can wield power in the virtual realm can also wield power in the physical realm. Diana Saco argues that the virtual and the physical have become intertwined: "Perhaps because computers today are so thoroughly wired into society, changes in cyberspace have repercussions for the physiocentric social spaces of which the virtual is already a part. Hacking cyberspace, in this respect, is ultimately about hacking society."[266] Hyun Soon Park demonstrates this principle in his examination of the Electronic Frontier Foundation's (EFF) campaign against the Communications Decency Act (CDA) in 1996, arguing that "grassroots campaign web sites can facilitate frame extension and frame transformation processes taking place in a timely, appropriate and effective manner. Through sending out electronically published newsletters and press release kits on a regular basis, they can galvanize interest, and motivate and retain participation among potential adherents."[267]

Phrack's mission was to bring technical information to the hacker/phreaker collective. There were other phile writers in the BBS world, such as Cult of the Dead Cow, but *Phrack* seemed to have a clear, unwavering vision. Where Cult of the Dead Cow is a mixture of technical information and (sometimes rather perverse) literary musings,[268] *Phrack* stuck mainly to the practical aspects of technology. Important developments could be found in the pages of Phrack World News, and through their

---

[266] Saco, *Cybering Democracy: Public Space and the Internet*, 197.

[267] Hyun Soon Park, "Case Study: Public Consensus Building on the Internet," *CyberPsychology & Behavior* 5, no. 3 (2002): 237.

[268] For example, one text file details the torture, anal rape, and killing of a lab rabbit by two men. See Tippy Turtle, "Ted and Dave's Animal Fun: Session I: Bunny Lust," *Cult of the Dead Cow*, 1987, http://www .cultdeadcow.com/cDc_files/cDc-0018.php (accessed March 22, 2006). However, not all of the files in Cult of the Dead Cow follow such a pattern. A recently published file is a detailed philosophical consideration of the nature of love. See Trammel, "Modern Love," *Cult of the Dead Cow*, February 14, 2006, http://www.cultdeadcow.com/cDc_files/cDc-0403.php (accessed March 22, 2006).

reporting, a hacker identity began to take shape. *Phrack* was a place not only for information, but also for indoctrination.

Operation Sundevil and the Galvanization of the Hacker Movement

Hackers may have begun forming as a social movement before Operation Sundevil, but this event provided the catalyst for hackers to recognize the need for solidarity and organization. That hackers may be busted by the authorities was already understood within the hacker community; in the second issue of *Phrack*, Phreak World News reports three different instances of phreakers and hackers being busted for various offenses. But Operation Sundevil was an unprecedented wide-scale assault on hackers, and as such, it seemed to take hackers largely by surprise. According to Bruce Sterling, "Of the various antihacker activities of 1990, Operation Sundevil had by far the highest public profile. The sweeping, nationwide computer seizures of May 8, 1990, were unprecedented in scope and highly, if rather selectively, publicized."[269]

Sterling states that "Sundevil's motives can only be described as political. It was a public relations effort, meant to pass certain messages, meant to make certain situations clear: both in the mind of the general public and in the minds of various constituencies of the electronic community. First—and this motivation was vital—a 'message' would be sent from law enforcement to the digital underground."[270] This message was received loud and clear by the hacker community. The opening lines of the May 28, 1990, edition

[269] Bruce Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier* (New York: Bantam Books, 1992), 153.
[270] Ibid., 161.

of Phrack World News begin: “May 9th and 10th brought on two days [that] would be marked in every hackers history book. The reason we assume these days will be important to many, is that maybe it’s time we opened are eyes and saw the witch hunt currently in progress.”[271] The introduction concludes, “Yes, we are the witches, and we are being hunted.”[272]

This should not have come as such a surprise to the hacker community; hackers had already encountered similar operations by law enforcement agencies. The July 28, 1987, edition of *Phrack* begins with this introduction by Knight Lightning: “Hi and welcome to the final regular issue of Phrack Newsletter. Most of you already know about the nationwide arrest of many of the phreak/hack world’s most knowledgeable members. I may receive a visit from the authorities as well and because of this and other events, I am going to leave the modem world.”[273] Even so, his decision to reprint “The Conscience of a Hacker”—also known as the “hacker manifesto”—with its unapologetic conclusion “you may stop this individual, but you can't stop us all,” demonstrates a sense of defiance. Shortly thereafter (August 7, 1987), the editorship changed hands with the following message: “So, did you miss us? Yes, Phrack is back! Phrack Magazine’s beloved founders, Taran King and Knight Lightning, have gone off to college, and the recent busts (summarized completely in this month’s Phrack World News) have made it difficult to keep the magazine going. TK and KL have put the editorship of Phrack in the

---

[271] Phreak_Accident, “Phrack World News,” *Phrack* 3, no. 31 (May 28, 1990): phile 8.
[272] Ibid.
[273] Knight Lightning, “Introduction,” *Phrack* 2, no. 14 (July 28, 1987): phile 1.

hands of Elric of Imrryr and Sir Francis Drake. SFD is primarily responsible for PWN. As of yet we have no 'Official Phrack BBS.'"[274]

By 1990, when Operation Sundevil took place, the days of hoping for a slap on the wrist when caught had long been over and the hacker community knew it. In 1988, Phrack World News had reprinted an article called "Illegal Hacker Crackdown" from the California Computer News that detailed the first adult conviction for hacking.[275] *Phrack* had also moved from simply reporting busts to explaining what to do when the reader is actually involved in a bust. The April 25, 1989 edition of *Phrack* features an article called "Getting Caught- Legal Procedures" by Disk Jockey that provides an overview of the legal process from informing the phone company to sentencing at the trial.[276] The first explicit phile dedicated to legal issues is "The Laws Governing Credit Card Fraud," published in 1987.[277] Later philes such as "Can You Find Out If Your Telephone Is Tapped?"[278] "Big Brother Online,"[279] and "Hacking: What's Legal And What's Not,"[280] demonstrate that by the time Operation Sundevil occurred, hackers had already abandoned the belief that they could simply hide in the relative anonymity of the ether.

The law enforcement community had issued a wakeup call not only to the hacker community, but also to the general public. There had already been media coverage of the potential threat that hackers represented to the general public. This was now brought back

---

[274] Shooting Shark, "Phrack XV Intro," *Phrack* 2, no. 15 (August 7, 1987): file 1.
[275] The Smuggler, "Phrack World News," *Phrack* 2, no. 17 (February 1, 1988): file 11.
[276] The Disk Jockey, "Getting Caught - Legal Procedures," *Phrack* 3, no. 26 (March 24, 1989): file 3.
[277] Tom Brokaw, "The Laws Governing Credit Card Fraud," *Phrack*, no. 16 (September 19, 1987): file 5.
[278] Fred P. Graham and VaxCat, "Can You Find out If Your Telephone Is Tapped? 'It Depends on Who You Ask,'" *Phrack* 2, no. 23 (December 30, 1988): file 9.
[279] Thumpr Of ChicagoLand, "Big Brother Online," *Phrack* 2, no. 23 (June 6, 1988): file 10.
[280] Hatchet Molly, "Hacking: What's Legal and What's Not," *Phrack* 3, no. 25 (March 8, 1989): file 8.

into the public eye in a dramatic way, but only for those who read reports of the raid. The raid made the front page of *USA Today*,[281] but other outlets did not see this event as front page news and it was not even mentioned in the *New York Times*.[282] Thus, Operation Sundevil may have been newsworthy but it did not seem to be particularly noteworthy at the time. Maxwell McCombs and Donald Shaw argue that the mass media, especially the news media, set the agenda of what is important in political campaigns.[283] By relegating coverage of Operation Sundevil to the interior of the newspaper, the news media sent a clear message to the reader—this was not something with which they should be terribly concerned. Thus, although Operation Sundevil is largely credited for raising the consciousness of the public mind concerning the hacker threat, a brief evaluation of the news coverage suggests that Operation Sundevil may not have been the watershed event that fostered this shift.

On the other hand, the change in relationship between industry and the law enforcement community was unmistakable. Sterling writes, "Sundevil was greeted with joy by the security officers of the electronic business community. After years of high-tech harassment and spiraling revenue losses, their complaints of rampant outlawry were being taken seriously by law enforcement."[284] From that point, the aggressive stance against hackers has only intensified.

---

[281] Debbie Howlett, "Hackers Run up $50 Million Phone Bill," *USA Today*, May 10, 1990.
[282] See "Computer Hacker Ring with a Bay Area Link," *San Francisco Chronicle*, May 9, 1990; "Lawmen Seek Hackers - Raids in 15 Cities," *San Francisco Chronicle*, May 10, 1990; Tom Schmitz and Rory J. O'Connor, "Fed Program Pulls the Plug on Hackers," *Houston Chronicle*, May 13, 1990.
[283] See Maxwell E. McCombs and Donald L. Shaw, "The Agenda-Setting Function of Mass Media," *Public Opinion Quarterly* 36, no. 2 (1972): 176-87.
[284] Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, 163.

The scars from Operation Sundevil are still visible within the hacker community. In a phile commemorating the fifteenth anniversary of Operation Sundevil, Dark Sorcerer spends much of the early part of the essay attacking an informant called "The Dictator." Dark Sorcerer reinforces the value of loyalty in the hacker community: "I reserve a special hatred for snitches and narcs of all types. In my view, there is no lower creature in the world than the professional snitch. Law enforcement personnel are simply doing their job: they might be clueless, on a power trip, or what have you, but you can't fault law enforcement for doing what they do – if you throw bananas in a cage of orangutans, for example, you simply don't expect them to do anything but grab them and shove them in their mouths. Likewise, if you are on the "other side", you should at least know who your enemies are."[285] Dark Sorcerer concludes the attack with a comparison to Christ's betrayal by Judas Iscariot: "Enjoy your 30 pieces of silver, and don't be surprised if you're born in Haiti during your next life."[286]

The loyalty that Dark Sorcerer values marks a shift away from individual skill as the measure of one's worth in hacker culture. Hacker culture celebrated rugged individualism rather than loyalty. But times had changed, the stakes had been raised, and hackers were under attack. Operation Sundevil provided the catalyst that helped bring hackers together into an organized movement. Law enforcement, government officials, and industry were all united against hackers; hackers needed to also become united.

---

[285] Dark Sorcerer, "Operation Sundevil... 15 Years Later," *Cult of the Dead Cow*, May 9, 2005, http://www.cultdeadcow.com/archives/2005/05/operation_sundevil_1.php3 (accessed March 21, 2006).
[286] Ibid.

Kevin Mitnick and the Myth of the Superhacker

Operation Sundevil provided the impetus for hacker organization but the capture and imprisonment of Kevin Mitnick provided the opportunity to define exactly what it meant to be a hacker. Mitnick was a figure who both galvanized and polarized hackers. He had been arrested on multiple occasions for computer crime and few hackers argued that he was innocent. But hackers protested that the caution with which Mitnick was held was unreasonable and served more to instill within the general public a sense of fear and awe of the hacker. Although his crimes were rather pedestrian and far from threatening to the general public, the image of Mitnick created by the prosecution and the media is one of a dangerous "darkside hacker" with almost superhuman powers. Mitnick's legal issues and fugitive status would be played out not only on the front page of the *New York Times*, but also in the text files of Phrack World News.

Even some members of the law enforcement community noted that Mitnick was treated unfairly and served more as a scapegoat than as an example of a real threat. Gerald Kovacich, a veteran law enforcement and information security professional, states:

> I hate to bring up old news, but the Mitnick case was an example of the criminal justice system gone awry, with the FBI agents and prosecutors more interested in forthcoming fame and fortune than justice. Mitnick may have been a pain in the ass, but he was no Capone, although he was treated as if he was that dangerous. Yes, in what he could have done if he wanted to but not what he actually did. He was an embarrassment to the government agencies with their political and public

> relations egos being damaged while he was on the [loose] - like so many other hackers now being investigated charged by our nation-states. These employees of the nation-state with their high tech and millions of dollars couldn't even find the guy, so when he was found - not by the FBI by the way - it was get even time. This is mentioned only as an example of what millions of federal dollars can not accomplish and also what power the federal government can bring to bear on an individual. It is only the beginning if one looks at the trends."[287]

Kovacich makes some startling claims, describing vindictive federal agencies interested more in revenge and self-interest than justice. Now that hackers have been lumped into the category of "cyberterrorist," the stakes are now higher. Kovacich also illustrates the extreme power differential between the hacker and the federal government, but demonstrates that even with this power differential, there is still a possibility of evading the law.

Kovacich's suggestion that revenge was a motivation for the treatment of Mitnick overlooks the genuine fear of Mitnick within the federal law enforcement community. After all, this was a person who, according to John Markoff's front page coverage of Mitnick in the *New York Times*, used to break into North American Aerospace Defense Command (NORAD) as a teenager.[288] In one portion of Phrack World News, Kenneth Siani, a security specialist had this to say about Kevin Mitnick's arrest:

---

[287] Kovacich, "Hackers: Freedom Fighters of the 21st Century," 573-574.
[288] John Markoff, "Cyberspace's Most Wanted: Hacker Eludes F.B.I. Pursuit," *New York Times*, July 4, 1994.

> Unfortunately he is thought of as some kind of a "SUPER HACKER." The head of Los Angeles Police Dept's Computer Crime Unit is quoted as saying, "Mitnick is several levels above what you would characterize as a computer hacker." No disrespect intended, but a statement like this from the head of a computer crime unit indicates his ignorance on the ability of hackers and phone phreaks. Sure he did things like access and perhaps even altered Police Department criminal records, credit records at TRW Corp, and Pacific Telephone, disconnecting phones of people he didn't like etc. But what is not understood by most people outside of the hack/phreak world is that these things are VERY EASY TO DO AND ARE DONE ALL THE TIME."[289]

Siani's argument both redeems Mitnick from his demonization by placing him on a level of the average, above novice hacker, while simultaneously raising questions of what the advanced hackers are capable of. But his description also casts aspersions on Mitnick's skill, which defines what it means to be a hacker.

Siani explains why Mitnick was perceived as such an advanced hacker: "The only thing special about Kevin Mitnick is that he is not a 'novice' hacker like most of the thirteen year old kids that get busted for hacking/phreaking. It has been a number of years since an 'advanced' hacker has been arrested. Not since the days of the Inner Circle gang have law enforcement authorities had to deal with a hacker working at this level of ability. As a general rule, advanced hackers do not get caught because of [their] activity but rather it is almost always others that turn them in. It is therefore easy to understand

---

[289] Kenneth Siani, "Kenneth Siani Speaks out About Kevin Mitnick," *Phrack* 3, no. 27 (June 20, 1989): file 10.

why his abilities are perceived as being extraordinary when in fact they are not."[290] In this, we see a discussion of what it means to be an elite hacker. I have spoken to hackers who state that the main problem with Mitnick is that he got caught. Many of the old guard of the hacker underground had been arrested or raided, yet they were generally not ridiculed by the hacker community. Here we see a shift to the belief that hackers still hold today: a real hacker can cover his or her tracks well enough to evade detection and capture. Perhaps this is one reason for Siani's disparaging remarks concerning Mitnick's skills—the collective identity had shifted and what was once a peril of hacking had become an unpardonable sin.

An interview with Agent Steal, an FBI informant, also criticizes Mitnick's skill. When asked about Mitnick in an interview, Steal replied: "I had never met him before I was busted. When I went to work for the bureau I contacted him. He was still up to his old tricks so we opened a case on him and Roscoe. It's a long story but they wound up getting busted again. Mitnick got tipped off right before they were going to pick him up. So he's on the run again. Roscoe wasn't so lucky. This will be Mitnick's fifth time to get busted. What a loser. Everyone thinks he is some great hacker. I out smarted him and busted him. [Kevin] Poulson blows him away as well."[291]

---

[290] Ibid.

[291] Mike Bowden (Agenta Aka Agent 005), "An Interview with Agent Steal," *Phrack* 4, no. 44 (November 17, 1993): file 16.

Many issues of Phrack World News did little more than reprint mainstream news coverage of Mitnick with little additional comment.[292] However, once Mitnick was caught, *Phrack* provided reprints and excerpts of mainstream news stories and headlines about Mitnick with the following commentary: "Just a sampling of the scores of Mitnick articles that inundated the news media within hours of his arrest in North Carolina. JUMP ON THE MITNICK BANDWAGON! GET THEM COLUMN INCHES! WOO WOO!"[293] For the news media, the Mitnick case was the ideal hacker story. He had been captured after a nationwide manhunt. This kind of journalism that made sense; tracing someone though server hops is boring for readers but a man on the run is interesting. This was a far different kind of bust than what took place during Operation Sundevil where many of the hackers had been raided in their parent's homes, much to their surprise. Mitnick was a fugitive on the FBI's most wanted list and he was caught with the help of a journalist. But other elements made the Mitnick case attractive from a journalistic perspective. Mitnick fit the hacker stereotype: geeky, glasses, overweight, a bit petty at times. He was also an identified computer criminal. In other words, he was not like the average reader. Many of the individuals busted in Operation Sundevil were typical white kids from the suburbs who had not previously gotten into trouble—they could be anybody. Mitnick was someone who could be safely viewed as "other" by both the journalists and by the readers.

---

[292] For some examples, see Knight Lightning, "Phrack World News," *Phrack* 2, no. 23 (January 25, 1989): file 11; Knight Lightning and Taran King, "Phrack World News," *Phrack* 2, no. 22 (December 23, 1988): file 9; Disorder, "Phrack World News," *Phrack* 8, no. 53 (July 8, 1998): article 14.
[293] Datastream Cowboy, "Phrack World News," *Phrack* 6, no. 47 (April 15, 1995): file 22.

Hackers are skeptical of the supposed facts of the Mitnick case as reported by Markoff. A *Phrack* editorial lays out an argument that casts doubt upon the entire case. The editorial establishes ties between Mitnick and Shimomura and illuminates the prior relationship between Markoff and Mitnick: "I guess Markoff has had a hard on for Mitnick for ages. Word always was that Mitnick didn't really like the treatment he got in Markoff's book 'Cyberpunk' and had been kinda screwing with him for several years. (Gee, self-proclaimed techie-journalist writes something untrue about computer hackers and gets harassed…who would have thought.)"[294] After outlining the reasons why the charges against Mitnick seemed overstated, the editors suggest that Mitnick's arrest was little more than a get rich quick scheme for Markoff and Shimomura:

> Less than a month after the whole bust went down, Markoff and Tsutomo signed with Miramax Films to produce a film and multimedia project based on their hunt for Mitnick. The deal reportedly went for $750,000. That is a fuckload of money. Markoff also gets to do a book, which in turn will become the screenplay for the movie. (Tsutomo commented that he went with Miramax "based on their track record." Whatever the fuck that means.) Less than a month and they are signed. Looks to me like our duo planned for all this.
>
> "Hey Tsutomo, you know, if you went after this joker, I could write a book about your exploits! We stand to make a pretty penny. It would be bigger than the Cuckoo's egg!"

---

[294] Phrack Staff, "Phrack Editorial," *Phrack* 6, no. 47 (April 15, 1995): file 2a.

> "You know John, that's a damn good idea. Let me see what I can find. Call your agent now, and let's get the ball rolling."
>
> "I'll call him right now, but first let me write this little story to recapture the interest of the public in the whole Mitnick saga. Once that runs, they publishers are sure to bite."
>
> Meanwhile Mitnick becomes the fall guy for the world's ills, and two guys methodically formulate a plot to get rich. It worked! Way to go, guys.[295]

Arguments that Markoff had motives other than journalistic inquiry have been largely ignored by the popular media. Even when the *New York Times* was hacked in protest of Markoff's reporting and the hackers explicitly pointed out that Markoff had greatly profited from Mitnick's arrest, this point was glossed over in the reporting of the hack.[296]

Within the hacker community, not all thought that Mitnick's arrest was a bad thing. Debate concerning Kevin Mitnick extended beyond the pages of *Phrack,* taking place also on the pages of defaced websites. The day after the *New York Times* hack, a group calling themselves H4G1S hacked Slashdot's website with the following message: "Fuck Kevin Mitnick! People like Eric Corley have dedicated their whole miserable lives to help 'free' guilty Kevin Mitnick. The truth of the matter is Eric Corley is a 'profiteering glutton', using Kevin Mitnick's misfortune for his own personal benefit and profit."[297] The archive containing the hack points out that "the authenticity of this hack is in question as the group allegedly taking responsibility (H4G1S) has hacked pages in the

---

[295] Ibid.

[296] This hack will be discussed in further detail in the next chapter.

[297] H4G1S, "RoTSHB," *2600*, September 14, 1998, http://www.2600.com/hackedphiles/slashdot/hacked/ (accessed March 27, 2006).

past with pro-Mitnick sentiments and links to 2600, most notably the NASA hack of early 1997. Just further proof that in the world of web hacking, nobody's in control."[298] However, HFG, the group who hacked the *New York Times* website had ridiculed H4G1S in the code of the hack, so the hack may simply be retaliation against HFG.

The plight of Kevin Mitnick brings to the forefront some of the paradoxes of hacker identity. Although many of the old guard hackers had also been busted, hackers ridiculed Mitnick because of his capture. Moreover, because he had been captured, Mitnick's skills were called into question and maligned. However, it is clear that Mitnick was skilled, at least in social engineering, and may have been more skilled than his detractors gave him credit for. But Mitnick was far from the skill level ascribed to him by law enforcement officials, members of the press (especially John Markoff), and the justice system. It seems that Mitnick served as the scapegoat for both the justice system and the hacker movement. By casting their collective inadequacies upon Mitnick, hackers could avoid considering the possibility that each of them was more like Mitnick than they would like to admit and that, but for the grace of God and the inadequacies of law enforcement officials, they could be the next one to fall.

---

[298] *2600*, "2600 | Slashdot," September 14, 1998, http://www.2600.com/hackedphiles/slashdot/ (accessed March 27, 2006).

The Death of *Phrack*

Dark Sorcerer explains that the fifteen years after Operation Sundevil have brought about a transformation in the hacking community. He compares pioneers and those who come to settle after them:

> When I look at the old, mid 80's *Phrack* versus articles written in the last few years, you can see the change: in are complicated things like Polymorphic Shellcode Using Spectrum Analysis, out are recipes for bathtub crank manufacture. This is a generalization, but the early articles – dumb and inarticulate as they usually were – showed more of a wide-ranging desire to conquer time and space. If you're going to sail around the world, then lock picking and acetylene balloon bomb making are definitely good skills to have, but if you're going to stay in London and work on maps, there's not much that's going to benefit you other than a slightly improved recipe for ink or parchment making."[299]

Phrack has officially ended, and in contrast to previous occasions in which the pronouncement of death had been premature, it seems that this time the pronouncement has been made not only by the editors of *Phrack*, but also by the hacking community. Dark Sorcerer, on the Cult of the Dead Cow website, had this to say: "Is Phrack more or less popular than it was five years ago? Ten years ago? I don't know. It does seem as though Phrack has followed a classic organic cycle: a naive, exuberant youth paving the way for a stodgier, more establishment-minded adulthood. That's not to say that it's

---

[299] Sorcerer, *Operation Sundevil... 15 Years Later*.

irrelevant, but rather that it was doing what it should have. Evidently now - whether due to exhaustion, boredom, or just plain realizing it's time to move on - someone has decided to give it a rest. Twenty years was definitely a good run - so RIP, Phrack."[300]

But *Phrack* had been traveling down the road to legitimacy for over a decade before it ended. In the March 1, 1993, issue Erik Bloodaxe took over the editorship and noted that "there are a few very distinct differences beginning with this issue of *Phrack*. First and foremost, Phrack is now registered with the Library of Congress, and has its own ISSN. Yes, boys and girls, you can go to Washington, D.C. and look it up. This adds a new era of legitimacy to Phrack in that with such a registration, Phrack should never again face any legal challenge that would bypass any paper based magazine."[301] Other elements demonstrate that *Phrack* was beginning to cover itself legally, such as the implementation of a PGP key and the requirement that all government and industry members register and pay a fee for access to *Phrack*.

There was an impulse toward inclusion early on in *Phrack*. For example, the September 25, 1986, issue of *Phrack* begins: "Anyone can write for Phrack Inc. now. If you have an article you'd like published or a story for Phrack World News, get in touch with one of us (Knight Lightning, Taran King, and Cheap Shades) and as long as it fits the guidelines, it should make it in. If you have been one of the many ragging on Phrack Inc., please, write a phile and see if you can improve our status with your help."[302] This is

---

[300] Dark Sorcerer, "A Short Requiem for _Phrack_ . . . Life Sucking in the Middle East," *Cult of the Dead Cow*, April 22, 2005, http://www.cultdeadcow.com/archives/2005/04/a_short_requiem_for_.php3 (accessed March 21, 2006).
[301] Erik Bloodaxe, "Introduction," *Phrack* 4, no. 42 (March 1, 1993): file 1.
[302] Taran King, "Introduction," *Phrack* 1, no. 7 (September 25, 1986): phile 1.

re-emphasized two issues later; Taran King states, "Let me once again stress that ANYONE can write for Phrack Inc. You aren't required to be on a particular board, much less a board at all, all you need is some means to get the file to us, as we do not discriminate against anyone for any reason."[303] But the times changed quickly in light of events such as Operation Sundevil with more attention by the law enforcement communities and the telco industry, most notably due to a document detailing the 911 phone system.[304] The editors of *Phrack* could no longer afford to publish just anything.

The urge for legitimacy can be seen in other parts of the hacker community. Part of this impulse has resulted in visibility for hackers. Members of L0pht testified before Congress. Cult of the Dead Cow appeared in *Spin* magazine.[305] Other groups have made explicit efforts to alter public perceptions of hackers. For example, 2600 meetings implemented a dress code in 2005 that requires formal business attire for attendees, explaining that "dressing in this manner will convey the image that is necessary for us to be seen as rational, decent, and acceptable members of society. There simply is no reason to convey another image. While some will see this as an unreasonable restriction on their freedom of expression and individuality, we think that that is an irresponsible attitude for these times. Can we really put a price on the importance of maintaining a good image? Is the comfort of walking around in blue jeans and tank-tops really worth sabotaging our

---

[303] Taran King, "Introduction," *Phrack* 1, no. 9 (December 1, 1986): phile 1.
[304] See Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, 261-281 for the document in question and the trial surrounding it.
[305] Mike Romano, "The Politics of Hacking," *Spin*, November 1999.

futures? The answer should be obvious. These are difficult times and we all must make sacrifices."[306]

Has hacking reached a point of no return at which the irreverent text philes describing homemade methamphetamines and grenades made out of shotgun shells can no longer stand side by side with technical documentation? It seems that the adolescence of hacking has ended and the death of *Phrack* marks a perhaps painful transition to adulthood. Even so, much as adolescence shapes individual adulthood, the adolescence of the hacker movement has left an impression upon the collective identity of the movement. This is illustrated by the continued relevance of *Phrack's* most lasting contribution to the shaping of the hacker movement—an early text phile entitled "The Conscience of a Hacker," more commonly referred to as "The Hacker Manifesto." L. A. Kauffman states that "identity politics express the principle that identity—be it individual or collective—should be central to both the vision and practice of radical politics. . . . Identity politics also express the belief that identity itself—its elaboration, expression, or affirmation—is and should be a fundamental focus of political work."[307] The "Conscience of a Hacker" is the foundation for hacker collective identity.

Entering the World of the Hacker: The Hacker Manifesto

On January 8, 1986, a young man named Loyd Blankenship sat in his bedroom and used his Apple IIe computer to write a document that would change the way people

---

[306] *2600,* "2600 Meetings Today - Formal Attire Required," April 1, 2005, http://www.2600.com/news/view/article/2200 (accessed March 27, 2006).
[307] L. A. Kauffman, "The Anti-Politics of Identity," *Socialist Review* 20, no. 1 (1990): 67.

looked at technology. He had recently been arrested, but his was not a typical crime. Blankenship was a hacker. In the computer underground, he was not known by his given name, but as "The Mentor," which is the name by which this section will refer to him. The document he wrote, "The Conscience of a Hacker," was published in the hacking magazine *Phrack* with the heading "The following was written shortly after my arrest. . . ." This document is commonly known as the "Hacker Manifesto."[308]

Contrary to what some scholars have insinuated or outright stated, The Mentor was not a member of the hacker group Legion of Doom (LOD) until after his arrest.[309] As part of the settlement with the phone company, The Mentor is not allowed to discuss the circumstances surrounding his arrest, so there can be little historical discussion on the text. Surprisingly, there has been very little scholarly literature on this document even though it has woven its way into popular culture, with parts of it being used in the movie *Hackers,* for example. Two decades later, The Mentor's words are still held up as an ideal, a touchstone for ostracized youth who love computers. Few scholars have taken an in-depth look at The Hacker's Manifesto, and some do not do this document justice and

---

[308] Throughout this section, I will use the version of the hacker manifesto found on Phrack. Because this is the original posting, I consider this the definitive version. However, the manifesto has been reprinted in many other works and is not to be confused with other hacker manifestoes. See The Mentor, "The Conscience of a Hacker," *Phrack* 1, no. 7 (1986): phile 3.

[309] According to an email conversation I had with Blankenship on May 4, 2003, he was not a member of the Legion of Doom when this text was written. He joined as part of the "second wave," about one to two years after he wrote "The Conscience of a Hacker." Several scholars seem to assume that The Mentor was a member of the LOD at the time the manifesto was written. See Steven M. Furnell, Paul S. Dowland, and Peter W. Sanders, "Dissecting the 'Hacker Manifesto,'" *Information Management & Computer Security* 7, no. 2 (1999); Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier;* Thomas, *Hacker Culture*.

seem to entirely miss the point.[310] However, Douglas Thomas does provide an excellent reading of the document.[311]

The Mentor creates a situation for reading his text. The introductory sentence states, "The following was written shortly after my arrest. . . ." Although he does not explain where he was at the time, this statement, and the fact that he credits The Mentor—his hacker name—as author, conjures up the image of an unrepentant criminal in his jail cell justifying his crimes to the public. This statement lends a sense of gravity to the text; the text is part manifesto and part confessional. He was paying the price for hacking. However, this was not the case. The Mentor explains that the text was written in his bedroom rather than in a jail cell.[312] But "unrepentant" may accurately describe his behavior, considering that he later went on to join the hacking group Legion of Doom. Bruce Sterling describes The Mentor as "a hacker zealot who regarded computer intrusion as something close to a moral duty."[313] Although history and image may be dissonant, the reader receives a rhetorically constructed image of history rather than an accurate portrayal of events, which guides the reader's perception of the text.

The medium in which the manifesto was published is significant. *Phrack* is an online magazine devoted to hacking and phreaking, and as such, would not have likely had an audience outside of this collective. The Mentor explains this further: "I was just really pissed off and spewing, and was thinking that I would never again be able to participate in the hacker underground again (of course, as it turns out, that wasn't the

---

[310] The article I refer to here is Furnell, Dowland, and Sanders, "Dissecting the 'Hacker Manifesto.'"
[311] Thomas, *Hacker Culture*.
[312] Loyd Blankenship, email message to author, May 2, 2003.
[313] Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, 133.

case). It was going to be my last missive to the troops. It went into Phrack because I was good friends with Craig, and I knew he'd print it. It never crossed my mind to send it elsewhere, because my intended audience probably wouldn't see it anywhere else."[314] This was a message for the underground, strategically targeted to the hacker collective. The hacker movement needed a rallying cry, and in "The Conscience of a Hacker," they now had one.

There is significant rhetorical force in naming a document a manifesto rather than a diary or a statement, implying that the text is destined for a larger audience. Even so, this document has achieved a kind of status that Blankenship never imagined when he wrote it: "At the time it was written, if you'd have told me people would fly me to NYC in 2002 to read it out loud in front of a thousand people, I'd have laughed at you. What has amazed me the most about it is how it continues to resonate with people nearly two generations removed from me."[315] A simple search on Google, a popular search engine, performed on March 28, 2006 for the exact phrase "conscience of a hacker" retrieved 13,600 documents. This document resonates even with those outside of the hacker underground because it encompasses themes of alienation, discovery, and identity, themes as old as human existence.

The text begins with the following lines (throughout this analysis, I leave the text unaltered):

---

[314] Loyd Blankenship, email message to author, May 2, 2003.
[315] Loyd Blankenship, email message to author, May 2, 2003.

Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...

Damn kids. They're all alike.[316]

While this is hardly a common scenario, The Mentor taps into the age-old observation that youth get into trouble. Adult responses to these impulses are predictable—a response of both dismissal and disgust. The refrain, "Damn kids. They're all alike," figures prominently throughout the text. This is one instance in which Furnell, Dowland, and Sanders demonstrate a lack of rhetorical sensitivity. In response to this refrain, they point out evidence that youth are not, in reality, all alike and seem to take the statement literally and not as a sarcastic statement attributed to adults.[317]

Teenagers may have a propensity to get into trouble—some more than others—but not all youth trouble winds up "all over the papers." Perhaps one reason why this behavior is so disconcerting to the establishment (adults) is the site of transgression. That a teenager can access a person's bank account and not only look around, but also alter or destroy information as he or she pleases must come as quite a shock to those who work in the bank and those who have money there. But why does the adult respond so dismissively to the news? Perhaps this reveals the tendency to believe that although kids get into trouble, it is always *someone else's* kid. W. Phillips Davison calls this the "third person effect," in which individuals perceive that others will be more affected by

---

[316] Throughout this section, I will reproduce the entire text of "The Conscience of a Hacker." Copyright 1986 by Loyd Blankenship (mentor@blankenship.com). Used with permission. All rights reserved.
[317] Furnell, Dowland, and Sanders, "Dissecting the 'Hacker Manifesto.'"

mediated messages than themselves.[318] Richard Perloff writes, "The 'third person' term derives from the expectation that a message will not have its greatest influence on 'me' (the grammatical first person), or 'you' (the second person), but on 'them'—the third persons. Individuals may overestimate the impact that media messages exert on others, underestimate media effects on the self, or both."[319] The adult figure can afford to be smug; it will not be anyone that he or she knows. The adult can attribute the actions of the adolescent in the headlines to poor parental upbringing, lack of discipline, or a host of other causes to which his or her children are, thankfully, immune.

> *But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?*
>
> *I am a hacker, enter my world...*

The Mentor invokes another timeless theme: "adults just don't understand." However, in this case, it is more a consequence of circumstance than of adult apathy. In today's society, computers are ubiquitous; in 1986, when the manifesto was written, the technological landscape was much different. The Mentor reminds the imaginary adult that the world has changed technologically and the adult has not kept up with this change. Nicholas Negroponte argues that "the haves and the have-nots are now the young and the old. Many intellectual movements are distinctly driven by national and ethnic forces, but

---

[318] W. Phillips Davison, "The Third-Person Effect in Communication," *Public Opinion Quarterly* 47, no. 1 (1983): 1-15.

[319] Richard M. Perloff, "The Third Person Effect in Media Effects," in *Media Effects: Advances in Theory and Research*, ed. Jennings Bryant and Dolf Zillmann, 489-506 (Mahwah, NJ: Lawrence Elbaum Associates, 2002), 490.

the digital revolution is not. Its ethos and appeal are as universal as rock music."[320] As with many things that the adult world does not understand, the digital realm is fraught with fear and uncertainty, while for the young, it is a world of exploration and promise.

The Mentor refers to "three piece psychology." It is unclear what he means here, but it conjures up the image of a stuffy adult, a banker perhaps, in a three piece suit, which would continue the theme of the bank that was described in the first paragraph. It may also be an allusion to Freud, with the idea of Id, Ego, and Superego. The term "1950's technobrain" invokes the mental image of a country mired in the industrial era. By 1986, the ideas and values of the 1950's seemed quaint, more nostalgic than realistic. The world was evolving and 1950's modes of thinking had become hopelessly outdated. The Mentor distances himself from this mentality and positions himself at the nexus between the digital age and the industrial age.

The Mentor identifies with the digital age but demonstrates that he has not yet completely made the shift into the digital realm. The Mentor uses the terminology of mechanical watches and clocks, or the analog world, to describe hackers. It is unlikely that he is trying to speak the language of the adult. Rather, The Mentor had not yet completely given up his analog self. This shifting back and forth between the digital world and the analog world demonstrates a time in which The Mentor—and society as a whole—was transitioning between different forms of literacy. Walter Ong argues that the shift from orality to literacy completely changed the human consciousness. More specific to this situation, he states, "Writing and print and computers are all ways of

---

[320] Negroponte, *Being Digital*, 204.

technologizing the word. Once the word is technologized, there is no way to criticize what technology has done with it without the aid of the highest technology available."[321] Without the ability to understand the dawning new age, a "1950's technobrain" is ill-equipped to critique it.

This linguistic shift is essential both for The Mentor and for the adult world he addresses. Benjamin Lee Whorf argues that "the possibilities open to thinking are the possibilities of recognizing relationships and the discovery of techniques of operating with relationships on the mental or intellectual plane, such as will in turn lead to ever wider and more penetrating significant systems of relationships. These possibilities are inescapably bound up with systems of linguistic expression."[322] So long as the mode of expression is that of the 1950's technobrain, the individual will continue to think on that intellectual plane. To break out of the 1950's technobrain mentality requires one to abandon 1950's linguistic expression.

At this point in the text, The Mentor identifies himself as a hacker. He makes it clear that becoming a hacker is a process. Both external and internal forces shape and mold hackers. At this point, the reader—presumably the imaginary adult—is commanded, not invited or asked, to enter the world of the hacker. This demand drags the reader into the digital world, one that may seem alien and uncomfortable, but inevitable in its coming. This is a world that The Mentor has both discovered and helped to create.

---

[321] Ong, *Orality and Literacy: The Technologizing of the Word*, 80.

[322] Benjamin Lee Whorf, *Language, Thought, and Reality: Selected Writings* (Cambridge, MA: M.I.T. Press, 1956), 83-84.

The forces that shape and mold the hacker are the same forces that shape the world in which the hacker lives.

In the next passage, The Mentor explains that school is one of the forces that shaped his outlook.

> *Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me...*
>
> *Damn underachiever. They're all alike.*

His world begins at school rather than before. Perhaps his entry into an institution of "education" was part of his socialization into the greater society as well as his gateway into the world of the hacker. Peter Berger and Thomas Luckmann explain that school acts as a form of secondary socialization.[323] Exploration is encouraged, or, at the very least, tolerated, in young children. In school, the focus shifts from play and exploration to memorization of facts and repetitive skill building exercises. Behaviors that had been commonplace earlier are now being squelched; one must learn to color inside lines and people can no longer be colored blue.

The Mentor learns from his experience in school that he is different, smarter than other children. This is an example of defining the self through differentiation from what one is not, or the "other." But who is the aberration? The Mentor seems to define himself, rather than the other children as the anomaly. This theme will eventually become firmly entrenched in the hacker collective identity, reinforcing the belief that the majority of people are of substandard intelligence, at least by hacker standards.

---

[323] Peter L. Berger and Thomas Luckmann, *The Social Construction of Reality: A Treatise in the Sociology of Knowledge* (New York: Anchor Books, 1966), 140-144.

The Mentor explains that what school has to offer is of little value; it's "crap," it's "boring." The attributed adult response, however, demonstrates the irony of the situation. Rather than being recognized as more intelligent and unchallenged, he is viewed as less intelligent or lazy. The phrase, "They're all alike," here focuses on the underachiever, rather than on children in general. The adult eludes any responsibility in whether or not the child is an underachiever. There is an essentializing quality to this sentiment. Underachievers are underachievers by nature and they are all the same, much as Aristotle argued that slaves were slaves by nature.[324]

Here we gain insight into The Mentor's choice of name. The Mentor, in his *Phrack* pro-phile, stated that he chose his handle from The Grey Lensman series by E. E. 'Doc' Smith.[325] In this series, Mentor is the Arisian who supplies the people who will serve as the protectors of civilization with "lenses," which serve both as a tie to the Arisians as well as a way to help focus each individual's strengths. Mentor is intelligent, superhuman, and a force for good who does not fear the bestowal of knowledge and power and builds others up for the good of the universe.[326] But there is more to Mentor's altruism—the Arisian's recognize their limitations, so the goal is to create a race that surpasses them in ability.[327] Mentor recognizes that the true goal of a Mentor is to make oneself obsolete.

Even without this knowledge, the reader is left with the mental image of a mentor as a kind of teacher. But to be a mentor is to go beyond simply teaching—mentoring

---

[324] See Aristotle, "Politics," 1252a30-1252b9.
[325] Taran King, "Phrack Pro-Phile XXIII: The Mentor," *Phrack* 2, no. 23 (January 18, 1989): file 2.
[326] See Edward E. Smith, *First Lensman* (Reading, PA: Fantasy Press, 1950), 30.
[327] See Edward E. Smith, *Children of the Lens* (Reading, PA: Fantasy Press, 1954), 86-90.

implies a more intimate relationship with the person being mentored and as such, the mentor's relationship with that person more closely approximates that of master/apprentice than teacher/pupil. Berger and Luckmann, in their discussion of secondary socialization, explain that "teachers need not be significant others in any sense of the word. They are institutional functionaries with the formal assignment of transmitting specific knowledge. The roles of secondary socialization carry a high degree of anonymity; that is, they are readily detached from their individual performers. . . . they are in principle interchangeable."[328] A teacher may teach a skill or a principle, but a mentor indoctrinates and provides a model for living. It is a much more personal relationship requiring that the pupil have a greater sense of identification with the mentor, more closely approximating primary socialization.[329]

The Mentor seems to realize that this identification was a missing element in his education. Teachers were simply dispensers of information rather than mentors. By defining himself as a mentor, he takes on the responsibility inherent in that position. However, not only has he defined himself as *a* mentor, but he has defined himself as *The* Mentor, the archetypal mentor—the standard by which others are assessed, and in the case of the teachers, found wanting. The Mentor provides a model for being that can be adopted by other hackers. The sharing of knowledge is a core ideal of the hacker movement. Hackers are not content to simply know the knowledge themselves; they must disseminate that knowledge and teach others the skills that they possess.

---

[328] Berger and Luckmann, *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*, 142.
[329] See Ibid., 144-146.

The Mentor has provided a model for living, something that others could identify with. In this sense, The Mentor can almost be viewed as a prophetic figure. Three passages illustrate the impact that The Mentor has had on others.[330] The first one was posted on February 13, 2002:

> I was 9 when the Mentor read that.
>
> I was 13 when I read it for the first time.
>
> I knew then exactly how he felt.
>
> At 25, today I know exactly what he means.
>
> Since I have been 17 I have always had a copy printed out.
>
> Since 19 it has hung in my office at work.
>
> Now, 6 years in the computer field, and 4 in network computer security it hangs in my office.
>
> These words always make me remember where i started, my roots, what what my brothers in the underground, of yester-year and today have to endure everyday.
>
> Best words written!

Another poster wrote on December 30, 2001:

> I read this a few years ago (yeah I'm pretty new in hacker's world. But, in fact I think I may not say I'm in hacker's world...), and what I felt was... undescribable. What was written fits exactly with what I felt, especially at school.

---

[330] These remarks were taken from the message board attached to the manifesto on the *Phrack* website (http://www.phrack.org/show.php?p=7&a=3). Formatting and punctuation have been preserved (along with spelling errors), but I have removed the email addresses, which identifies the author. Unfortunately, *Phrack* is in the process of closing down and the message boards are no longer available. These messages were accessed May 1, 2003.

> Still now, when I read it again, I find this is really wonderfully written. It gave me a purpose in my life, a thirst of knowledge. I'd like to meet this man, to say him "thanx" for that...
>
> Another writer posted this message on January 17, 2002:
>
> > I believe in this manifesto and have been living it for more than 10 years. It is not an idea but a way of life.
> >
> > Dream on dreamer and remember to always question why?.....

These are only a few of the people who have taken on The Mentor's words as a guiding philosophy. To many, it seems that The Mentor has proven himself worthy of the name.

In the next passage, The Mentor illustrates more vividly his experience in school:

> *I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..."*
>
> *Damn kid. Probably copied it. They're all alike.*

At the time this document was written, The Mentor was 21 years old and not actually in junior high or high school, so we are still exploring the processes that shaped him.[331] This is a retrospective documentation of specific instances of the school system's inability to account for and effectively accommodate those students with abilities far above or far below those of the average student. The argument seems to be that teachers believe that if the vast majority of students cannot do the work in their heads, from the

---

[331] Loyd Blankenship, email message to author, May 2, 2003.

teacher's perspective, those who do not show their work can safely be considered to be a cheater. This is a bleak description of the adult world's perception of adolescents.

The Mentor engages in some hyperbole in order to illustrate the elementary level of education even at the junior high and high school level. However, there is the possibility that his characterization is closer to the truth than many educators would care to admit. One also must wonder who is really not getting the point here. If a teacher has to constantly repeat simple concepts such as reducing fractions, is it the teacher who is ineffective or are the students simply "playing dumb" in order to avoid working harder than they must? Either way, The Mentor's assessment calls strongly for more effective teachers.

Thomas claims that the voice of the adult, which embodies authority, "reveals itself as hypocritical, unable to realize the cultural, pedagogical, or social import of technology itself" and further argues that "the hacker's intelligence and boredom are nothing more than an expression of this ambivalent relationship to technology, but that expression is systematically ignored, transformed, and labeled as undesirable."[332] This is one consequence of the digital youth being taught by the analog adults; the 1950's technobrain rears its ugly head. However, I disagree with Thomas's point that hackers are expressing an ambivalent relationship to technology. Hackers seem to be fascinated with and celebratory of technological systems. Rather, it seems that the adult world harbors this ambivalence toward technology. Armed with limited understanding and experience with technology, much of the adult world walks around in a perpetual state of

---

[332] Thomas, *Hacker Culture*, 75.

"technological somnambulism," never really understanding the technological systems that envelop and structure their lives.[333] Those who are the guardians and acolytes of this new technological priesthood are generally revered—except when they are children. This transgresses too many closely held beliefs of the 1950's technobrain, chief among them is that teachers should be adults and they should know more than the child/student. As such, hackers must be considered anomalies, a kind of person out of place, viewed with a mixture of fear for understanding that which the teachers do not comprehend and contempt for having the audacity to refuse their correct place in the social order.

> *I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me...*
>
> *Or feels threatened by me...*
>
> *Or thinks I'm a smart ass...*

This discovery endowed The Mentor with a feeling of power. Thomas goes one step further and explains that this is the acquisition of responsibility.[334] In other words, this is part of learning to become an adult, further differentiating himself from childhood. John Van Beveren states that "hackers often claim that the thrill of illicit searches in online environments is more exciting than their offline life. Hackers often comment on their powerless offline life often in contrast to the control they may have online over the computer systems of major military or corporate institutions. Community peer

---

[333] Langdon Winner, *The Whale and the Reactor: A Search for Limits in an Age of High Technology* (Chicago: University of Chicago Press, 1986), 10.
[334] Thomas, *Hacker Culture*, 78.

recognition from other hackers is gained through involvement in the activity of hacking, and often they discuss their exploits to future computer users or to owners of computer networks that they have identified security loopholes in."[335]

The Mentor declares that he made a discovery; he found the computer. It was not introduced to him by another person. When asked in an interview about his first experience with a computer, The Mentor replied: "We moved from Austin right before the summer between my 5th and 6th grade years of school (early 1976). When I got to San Marcos, I didn't know anyone, and started hanging out at the Southwest Texas State U. computer lab in the college library. It was populated with Pet-10s, CompuColors and some early Apple II machines. I mostly played games on them (Artillery, etc.)."[336] Once again, reality and mythology are at odds—the machines were not lost and had no need of discovery. The text describes not a lonely kid hanging out in a computer lab playing video games, but rather an odyssey in which the miraculous discovery led to enlightenment and fulfillment. The reader is encouraged to view this as not a commonplace or chance finding, but as a discovery of epic proportions.

This passage provides insight into how The Mentor believed adults viewed him. His is a world in which adults can tell the adolescent that what they have done is wrong simply because the adult does not like them. This subjectivity grates on The Mentor's emerging digital mind. He lists some possible reasons why they were either unable or unwilling to value his skills: they dislike him, they fear him, or they do not respect him.

---

[335] John Van Beveren, "A Conceptual Model of Hacker Development and Motivations," *Journal of E-Business* 1, no. 2 (2001): 4.

[336] Elf Qrin, "Elf Qrin Interviews the Mentor," *elfqrin.com*, July 31, 2000, http://www.elfqrin.com/docs/hakref/interviews/eq-i-mentor.html (accessed March 28, 2006).

All of these are subjective judgments that can often be unfair or unwarranted. The Mentor portrays adults as slaves to their emotions, petty, and spiteful. In contrast, the computer is objective. If the command that is entered into it is incorrect, it *cannot* work, regardless of how it feels about the person who input the command. The Mentor, having been disillusioned by adults and misunderstood by his peers, can now seek validation through machines. He enters into a partnership with the machine that had been previously unimaginable because his peers lacked the intelligence to keep up and the teachers lacked the patience and skill.

Or doesn't like teaching and shouldn't be here...

The Mentor revisits the theme of the inadequate teacher. With the argument that teachers who do not like teaching should not teach, The Mentor places different ethical considerations on the profession of teaching than those found in other industries. Those in manufacturing or sales jobs who hate the job but stick with it for the money are not denigrated. Why then is teaching any different? Few in American society would argue that teaching is just like any other profession, akin to manufacturing widgets; many consider teaching to be a labor of love. What The Mentor does is make the enthymeme explicit: if one does not like teaching, one should not be a teacher. Later on in the text, The Mentor describes experiences with good teachers as few and far between.

But there is more to the enthymeme when we consider The Mentor's name. Teachers, as part of the structure that shapes the lives of youth, are squandering the opportunity to make a difference in the life of a child. He implies that if a teacher is not willing to accept responsibility for shaping people's lives, then they should not be a teacher. In short, teachers should be mentors. Two decades later, The Mentor's outlook

remains the same: "My wife is a high school teacher, and looking at it from the teacher's point of view, I still see it as 100% valid. She has colleagues who aren't fit to be working at a car wash, and kids that are every bit as bored and tuned out as I was. I become physically angry when I get on a rant about the state of public education in the US today."[337]

Damn kid. All he does is play games. They're all alike.

Once again, the imaginary adult paints a picture of youth as engaging in nothing more than play. But for adolescents, play is not merely play. Play is a way of navigating identity and one's place in the world. Berger and Luckmann argue that play is a way of exploring possibility of other realities and Brenda Danet, Lucia Ruedenberg-Wright, and Yehudit Rosenbaum-Tamar explain that the Internet is an inherently playful medium.[338] Perhaps this is one reason that the adult and the hacker have difficulty understanding what the other does. If the Internet is an inherently playful medium, then adults, who are unfamiliar with the nature of work in that medium, may see only play. The Mentor demonstrates the dissimilarity between work in the world of the 1950's technobrain and work in the world of the hacker.

> *And then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found.*

---

[337] Loyd Blankenship, email message to author, May 2, 2003.

[338] Berger and Luckmann, *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*, 25; Brenda Danet, Lucia Ruedenberg-Wright, and Yehudit Rosenbaum-Tamari, "Hmmm...Where's That Smoke Coming From?: Writing, Play and Performance on Internet Relay Chat," *Journal of Computer-Mediated Communication* 2, no. 4 (1997), http://jcmc.indiana.edu/vol2/issue4/danet.html.

The analogy to drug addiction, specifically heroin addiction, tends to undermine The Mentor's cause by portraying the hacker in a way that is unflattering and criminal. Not only is he or she breaking the law, they are compelled to do so by addiction. But this possibility has been proposed. One such instance took place in the trial of Paul Bedworth, a hacker in the United Kingdom, who used an addiction defense and was found innocent.[339] This characterization of hacking as addiction is damaging in several ways. It minimizes the role of the hacker's own intellect in the discovery and exploitation of weaknesses in electronic systems. The hacker is weak willed and open to suggestion; one need only to plug in a modem and the hacker loses control. It also paints a picture of the hacker as abnormal, a deviant. Even so, it is understandable how one could reach the conclusion that hacking is addictive. Many hackers continue in the underground, even after getting busted; The Mentor is one such case. Also, a commonly noted trait of hackers is the ability to place everything else to the side, including food and sleep, in the search for knowledge. Consistent with the addiction metaphor, The Mentor removes the agency from this entire passage. "It happened," "a door opened"—as if hacking is something that magically happens to someone, rather than something that one does. Although The Mentor is the one sending out the electronic pulse, he has subtly removed himself from the prose, which allows the reader to insert him or herself into the text.

The electronic pulse can be viewed as an extension of The Mentor himself, much as the voice can be viewed as an extension of the body. The boundaries of physical shape

---

[339] Owen Bowcott, "Hacking and the Bedworth Syndrome," *The Guardian*, April 1, 1993. Besides the addiction defense, there was also public sympathy for Bedworth because of the way he was treated by the authorities.

and location no longer constrain him. It is not his agent in the phone line, but his own voice. It is not the computer that is seeking, but The Mentor. He is now in the phone lines while making the phone lines an extension of himself. He is both the vein and in the vein. The Mentor hints at a new way of viewing the self in the digital realm, where one is both the media and the mediator. Scholars have begun to recognize the issues surrounding this new way of being in cyberspace, for example with the conception of "cyberrape."[340] The digital world and the analog world are connected. Lawrence Lessig argues against the idea of a system of cyberlaw that is separate from law in the physical world on this premise: "The effects of that place [cyberspace] will never be far removed from this [physical space]. And our understanding of what that place will become is just beginning. We, here, in this world, will keep a control on the development there. As well we should."[341]

A new world is continually unfolding before us as we shape and create it. But this new world is still connected to the "real" world which has helped cast the mold for the digital world. Diane Nelson argues that "both the nation and cyberspace are founded on exclusions marked by race, gender, sexuality, and so forth—the nation-state through historically embedded racism, sexism, and homophobia and cyberspace through

---

[340] For a discussion of virtual rape and other criminal behaviors in cyberspace as well as the perception of the self in cyberspace, see Dibbell, "A Rape in Cyberspace"; Susan J. Drucker and Gary Gumpert, "Cybercrime and Punishment," *Critical Studies in Media Communication* 17, no. 2 (2000): 133-58; Richard MacKinnon, "Virtual Rape," *Journal of Computer-Mediated Communication* 2, no. 4 (1997), http://jcmc.indiana.edu/vol2/issue4/mackinnon.html; Matthew Williams, "Virtually Criminal: Discourse, Deviance and Anxiety within Virtual Communities," *International Review of Law, Computers & Technology* 14, no. 1 (2000): 95-104.

[341] Lessig, "The Zones of Cyberspace," 1403.

educational and financial limits on who has access to the internet."[342] Cyberspace cannot overcome the problems of the physical world when those in the physical world are creating cyberspace.

The Mentor states that a door has opened to a world but he does not explicitly state that it is a *new* world. Perhaps it is not a new world after all—at least for him. It may be that this is the world that The Mentor has lived in all of his life without realizing it, which is why it seemed so inviting when it presented itself. In much the same way that the square protagonist in the book *Flatland* did not realize that there were three dimensions to the world that he had always been a part of, perhaps many live in the analog realm while simultaneously enveloped by, but unaware of, a digital realm.[343] Watzlawick, Bavelas, and Jackson explain that our view of the world is transparent and in order to change our view, we must do so from a higher level of abstraction but that this level of abstraction "seems to be very close to the limits of the human mind and awareness at this level is rarely, if ever, present."[344]

When The Mentor enters this world he finds an answer to his search for "a refuge from day to day incompetencies"—a board. It may seem odd that what amounts to little more than an electronic bulletin board can provide such a sense of salvation. But it is not the board itself that is the answer, but the people he finds posting on it. In her study of Internet usage, Bakardjieva found that "representatives of disenfranchised groups . . .

---

[342] Diane M. Nelson, "Maya Hackers and the Cyberspatialized Nation-State: Modernity, Ethnostalgia, and a Lizard Queen in Guatemala," *Cultural Anthropology* 11, no. 3 (1996): 297.
[343] Edwin Abbott, *Flatland: A Romance of Many Dimensions*, 5th , rev. ed. (New York: Barnes & Noble, 1963).
[344] Paul Watzlawick, Janet Beavin Bavelas, and Don D. Jackson, *Pragmatics of Human Communication: A Study of Interactional Patterns, Pathologies, and Paradoxes* (New York,: Norton, 1967), 267.

were using the technology as a tool to carve spaces of sociability, solidarity, mutual support and situated, appropriative learning in communion with others."[345] This can be seen in his description of the board in the next passage:

> *"This is it... this is where I belong..."*
>
> *I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all...*

The Mentor, as digital self, has found the home for the self that he most identifies with. He has found kindred souls that he recognizes as similar to himself. The Mentor has now repudiated the analog world, the world that he has been conditioned all of his life to consider himself a part of. Although he remains a part of the physical world, he knows that he belongs is in the virtual world.

But this is a strange place to call home. The Mentor states that he knows everyone, but has never met them, has never talked to them, and may never hear from them again. In such a transitory world, it would be difficult to form relationships with others. Even so, some scholars argue for a model of the ideal public sphere that is similar to such a place. Richard Sennett argues that the public sphere began to diminish when people could no longer deliberate in public as strangers, explaining that "people can be sociable only when they have some protection from each other; without barriers, boundaries, without the mutual distance which is the essence of impersonality, people are destructive."[346] For Sennett, this kind of impersonality may be the savior of the public

---

[345] Maria Bakardjieva, *Internet Society: The Internet in Everyday Life* (London: Sage, 2005), 180.
[346] Sennett, *The Fall of Public Man*, 311.

sphere. Jürgen Habermas describes the ideal public sphere as one that "preserved a kind of social intercourse that, far from presupposing the equality of status, disregarded status altogether."[347] The transitory nature of the digital world may be a useful attribute, but one that is inherently part of the public sphere, which cannot completely remove the needs fulfilled in the private sphere. The digital world can be only a part of one's existence; to completely abandon the physical world seems in practice only briefly fulfilling. This can be seen by the proliferation of hacker conventions in which hackers can meet and socialize in the analog world, solidifying relationships forged in the digital world.

Damn kid. Tying up the phone line again. They're all alike...

The stereotype of the teenager on the phone works here, but from a different angle. While many teenagers talk to nearby friends, it is likely that The Mentor is talking to people all over the world. Interaction is still happening but in a different, textual form. It is also a different way of tying up the phone line, a conversation that adults are no longer able to monitor. If a parent picks up a phone during a conversation their child is having with a friend, the parent can listen in on the conversation. With modem transmissions, if a parent tries to listen in they hear only harsh noise. Not only can the child transcend place in the quest for interaction, they can also evade parental attempts at surveillance. In this world, only the child knows with whom they interact, and, at times, perhaps even the child does not know. The modem becomes a means of liberation from parental control.

---

[347] Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*, 36.

There is another sense in which a hacker's way of tying up the phone line is different. Many hackers of the day were also phreakers, which means that they also hacked phone systems. Using various tone generators (or "boxes"), phreakers are able to call long distance without being charged. In this way, they are not only tying up the phone line at home, but they are also gaining control over the phone system itself. They are essentially "dark matter," evading surveillance by both parents and the phone company. With this illicit knowledge, they no longer even need parental permission to use a phone—they can use any number of public pay phones free of charge.

A Shift in the Text

At this point, the relationship between The Mentor and the imaginary adult shifts significantly and the subdued resentment of the first half now gives way to openly expressed anger. Janet Lyon explains, "Linked with the [manifesto] form's passion for truth-telling, is its staging of fervid, even violent, rage."[348] The calm explanation of The Mentor's journey into the digital world now gives way to a diatribe, directed first at the educational system:

> *You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.*

[348] Janet Lyon, *Manifestoes: Provocations of the Modern* (Ithaca, NY: Cornell University Press, 1999), 14.

The Mentor has already stated that he was smarter than most kids his age and that this was a cause of frustration for him. The Mentor points to the homogenizing force of the public education system that seems destined to teach to the lowest common denominator in his statement, “You bet your ass we’re all alike!” The children are all alike because the school system has worked toward that end. This *telos* is not inherently sinister. The school system does not adequately assess the level of student understanding, failing to recognize that students may be at a higher level than expected. Therefore, by targeting the lowest common denominator to make sure that these students do not slip through the cracks, the school system allows those who are not adequately challenged to slip through the cracks. This can be seen in recently passed legislation that strives for the goal of “no child left behind.” In this passage, The Mentor has exposed a “one size fits all” attitude that seems to be prevalent in education.

This attitude permeates the system, and can also be found in the teachers themselves. Once again, we return to The Mentor’s argument that the teachers that are there should not be teaching. These teachers seek to satisfy a lust for power and domination (the sadists) or do not take the role of teacher seriously (the apathetic). However, The Mentor does not level this criticism at all teachers. He admits that there have been some, albeit few and far between, that both understood and fulfilled what The Mentor seems to view as the sacred act of being a teacher. But he describes them as those who had something to teach. Once again, The Mentor revisits the theme of sharing knowledge as a means of salvation.

When The Mentor describes students as "willing pupils," it is unclear whether he is making a blanket statement for all students or if he only refers to himself and other hackers. Based on his previous assessment of himself as smarter than other students and the fact that this is a description of what shapes hackers, The Mentor is likely referring to himself and other hackers rather than to students as a whole. Here we see reinforcement of the conception of the hacker as more intelligent than others, which remains a core value of hacker collective identity.

Thomas explains that "the hacker faces two alternatives: become a hacker and enter the refuge that provides an escape from the 'day-to-day incompetencies' of the world or remain a spoon-fed, dominated, ignored student subsisting on 'drops of water in the desert.' Those worlds, in their stark contrast, are the two worlds of technology: one represents the greatest danger by treating the world and everyone and everything in it as part of an institutional matrix that is defined by order; the other represents the greatest hope through a revealing of technology and through an examination of our relationship to it."[349] Thomas's circular reasoning here is a troubling—of the two options that a hacker has, one of them is to become a hacker. But more importantly, the world is not so binary. One who wishes to transcend the spoon-fed world of compulsory education has other opportunities—art, music, literature, writing—besides computer hacking. All of these creative outlets allow the individual to go beyond what is mandatory in school and to challenge and build oneself.

---

[349] Thomas, *Hacker Culture*, 78.

But only hackers are able to transcending their spoon-fed state. The Mentor implies that the other students need to be spoon-fed in a way that hackers do not. Here we see the converse of the argument that hackers are smarter than everyone else—"those who are not as smart as me must be stupid." This mentality proved to be one of the major downfalls of the hacker collective during Operation Sundevil. The hackers had gotten away with their intrusions for so long that they seemed to believe that the law enforcement agencies and telephone companies did not know as much about the systems as the hackers and that the hackers would continue to evade detection and arrest. Hackers had not only overestimated their own abilities, but had underestimated the abilities of everyone else.

The Mentor's food analogy demonstrates again that he has not completely let go of the physical self. This is a vivid image, calculated to induce in the reader a sense of disgust. But there is more to this analogy. There is the indictment of a paternalistic mode of teaching that sanitizes the information which does little to prepare the student for the raw problems of the real world. By pre-chewing the information, students will never develop the muscles necessary to chew the food themselves and students participating in such an educational system may never even see a need to do so. Each generation will become progressively weaker than the one before them and the problems with which they can deal will become less and less complex. The Mentor makes it clear that the adult world is hindering the adolescent developmental cycle. By denying the youth steak (adult knowledge), adults can continue to uphold the illusion that youth may be treated as

children and that they must be protected.[350] By depriving them of the nourishment and the water that they need, the adult world is mentally killing them. In this sense, the education system is a course of calculated psychological genocide, engineered to create weak, docile bodies that lack the strength to fight the adult power structures. By keeping the young weak, the youth will remain in their place, not because they believe that it is their place or that they are happy there, but because they have no other choice.

> *This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals.*

The Mentor acknowledges that this world did not completely belong to hackers from the beginning. This claim represents not a reclamation of that which was built by them, but a coup, a revolution, the overthrow of a tyrannical system. He states that the service is being run unfairly with profit as the end and not with knowledge as its goal. He accuses those who run the communications infrastructure of inflating the price of access in the pursuit of these profits. Although this text was written shortly after the breakup of the ATT/Bell monopoly, the capitalist structure of maximizing profits remains intact. The Mentor paints this as a class struggle but here the distinction between bourgeois and proletarians is blurred as neither are actually workers in the Marxian sense, nor are the

---

[350] Perhaps the most prevalent place to see this kind of mentality is in the advocating of censorship as a way to protect children. There are other instances of institutionalized resistance to adolescents becoming adults. For example, Matthew Waites discusses the tensions between citizenship, sexuality, and protection for children in age of consent laws, which are also tied up in developmental theories of adolescence and gender socialization. See Matthew Waites, *The Age of Consent: Young People, Sexuality, and Citizenship* (New York: Palgrave Macmillan, 2005), 11-39.

means of production mutually exclusive to either group (although the phone system itself remains largely in the hands of a few). This is yet another indication that the social order of the industrial era has been altered.

The Mentor avoids negatively valenced terms such as "stealing" or "phreaking," saying that hackers "make use of" already existing service. This utilitarian view of the world demonstrates that the ends, knowledge and exploration, are appropriate justification for breaking what he perceives as unjust laws. Yar states that "in hackers' self-presentations, they are motivated by factors such as intellectual curiosity, the desire for expanding the boundaries of knowledge, a commitment to the free flow and exchange of information, resistance to political authoritarianism and corporate domination, and the aim of improving computer security by exposing the laxity and ineptitude of those charged with safeguarding socially sensitive data."[351] The Mentor and the imaginary adult(s) have differing definitions of what constitutes a criminal act.

Jean Baudrillard argues that there is "no more subject, no more focal point, no more center or periphery: pure flexion or circular inflexion. No more violence or surveillance: only 'information,' secret virulence, chain reaction, slow implosion, and simulacra of spaces in which the effect of the real again comes into play."[352] The virtual world can no longer be seen only as an extension of the physical world. There are different rules in the digital world, and although the rules should be influenced by the effects that the digital world has on the analog world, this should by no means be the sole

---

[351] Yar, "Computer Hacking: Just Another Case of Juvenile Delinquency?" 391.

[352] Jean Baudrillard, *Simulacra and Simulation*, trans. Sheila Faria Glaser (Ann Arbor: University of Michigan Press, 1994), 29-30.

criteria. For hackers and phreakers, to charge for phone access is as ludicrous as selling air in the physical world. But if the digital world is to be chained to the rules of the analog world, then the rules should at least be applied consistently—after all, The Mentor had just claimed the digital world for the hackers, and this is an event with historical precedent. "The Conscience of a Hacker" was a declaration of independence long before Barlow wrote his "Declaration of the Independence of Cyberspace."[353] Much as the British colonies declared independence from the motherland that sent them forth, the hackers have liberated the digital "new world" from the oppressive homeland and have claimed it for their own. Of course, those already in the digital world may protest that the hackers have no right to come in and take over. However, the hackers have done so, much as the colonists did to the Native Americans.

"Beauty" is a term that warrants further exploration. To define beauty in terms of the baud seems to exemplify the high status given the ability to explore. It is also the means by which one gains information, going from a state of ignorance to an understanding of arcane knowledge. But the baud offers more than simply the anonymous transfer of information; there is now the possibility of fostering solidarity and forging relationships. What makes the baud so beautiful is that it provides a gateway to escape the isolation that these hackers feel. The hacker is no longer restricted by geographic location in a quest to find others with whom he or she can relate. Through the baud, one can virtually connect to peers who are truly equals, rather than engaging with one's spoon-fed (inferior) colleagues. Yar states that "in 'virtual' or online settings, peer

---

[353] Barlow, *A Declaration of the Independence of Cyberspace*.

groups are formed and sustained via computer mediated interaction in 'chat rooms' and via 'bulletin boards'. Such groups are held to provide not just opportunities for novice or would-be hackers to learn the 'tricks of the trade' from their more experienced counterparts, but also to socialise new 'members' into the distinctive ethos and attitudes of hacker culture."[354]

> *We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals.*

In each of these accusations, there seems to be an implicit counter-accusation. The unspoken, underlying idea is that each phrase could end with the words, "and you do not." Yar argues that The Mentor's reasoning

> clearly justifies hacking activities by re-labeling "harm" as "curiosity," by suggesting that victims are in some sense "getting what they deserve" as a consequence of their greed, and turning tables on accusers by claiming the "moral high ground" through a citation of "real" crimes committed by the legitimate political and economic establishment. Again, we see an inter-generational dimension that references commonplace understandings of "misunderstood youth" and the corrupt and neglectful nature of the "adult world." Thus young

---

[354] Yar, "Computer Hacking: Just Another Case of Juvenile Delinquency?" 396. Yar parenthetically cites Dorothy Denning. "Hacker Ethics." Paper presented at the National Conference on Computing and Values. New Haven, CT: Research Center on Computing and Society (RCCS), August 1991.

> hackers themselves invest in and mobilise a perennial, socially available discourse about the "gulf" between "society" and its "youth."[355]

But The Mentor is also differentiating between the new (hacker's) world and the old (adult) world. He argues that adults, specifically those who operate the structures of power, do not seek after knowledge, do not explore, and tend to judge based on race, nationality, and religion. These phrases demonstrate the asserted values of the digital world, or world that the hackers are constructing in contradistinction to the analog world. In the digital world, knowledge and exploration come before individual characteristics and physical characteristics disappear. But The Mentor has not yet let go of his physical self. The new world was born out of the old one and therefore has some of the characteristics of its parent. The same people who created and shaped the old world are now creating and shaping the new world—and people are not perfect. Gunkel explains that "participation in the virtually utopia of cyberspace, where there is supposedly no race, gender, or class, requires that one also negotiate the 'old boy network' that already dominates, informs and configures this space."[356]

Gender is not mentioned in The Mentor's litany of that which hackers exist without. His previous mention of "Ms. Smith," a teacher, demonstrates that gender still plays a role in the digital world. Another clue is the question, "Did you ever wonder what made him tick, what forces shaped him, what may have molded him?" This male domination of hacker subculture remains. Paul Taylor points out that there may be several reasons for this including misogyny, discomfort with females in the physical

---

[355] Yar, "Computer Hacking: Just Another Case of Juvenile Delinquency?" 392.
[356] Gunkel, *Hacking Cyberspace*, 163.

world, and a projection of their sexuality into hacking itself. In short, a successful hack is penetration and orgasm.[357] Elsewhere, Taylor postulates that societal factors, the masculine environment of computer science, and male gender bias in computer languages can also account for this lack of females in the hacker subculture, and other scholars have likewise argued that cyberspace is largely masculine space.[358]

The next passage takes a more accusatory tone changing the subject from the collective "we" to the "you" of the adult world / power structure.

You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

For those who remember drills where students got under desks in the event of a nuclear attack, this is a powerful *pathos* appeal. Simply mentioning the atomic bomb in 1986 was enough to conjure up images of the Russians attacking the United States and ushering in World War Three. This imagery guides the reader to the second two accusations of waging war and murder because most people already link atomic bombs to waging war and death. This is consistent with the priming effect discussed by David Roskos-Ewoldsen, Beverly Roskos-Ewoldsen, and Francesca Carpentier, in which they argue for a priming model that takes into account the existing cognitive frameworks of

---

[357] Paul A. Taylor, "Maestros or Misogynists? Gender and the Social Construction of Hacking," in *Dot.Cons*, ed. Yvonne Jewkes, 126-46 (Portland, OR: Willan Publishing, 2003).

[358] Taylor, *Hackers: Crime in the Digital Sublime*, 33. See also Melanie Stewart Millar, *Cracking the Gender Code: Who Rules the Wired World?* (Toronto: Second Story Press, 1998); Thomas and Wyatt, "Access Is Not the Only Problem: Using and Controlling the Internet"; Turkle, *Life on the Screen: Identity in the Age of the Internet.*

the receiver of media messages.[359] When The Mentor writes "atomic bomb" the reader already has other ideas or thoughts associated with that mental image and waging war is an obvious next step. The Mentor then subtly guides the reader to associate war with murder by leading them through an already established mental framework and attempting to add to it. Many place the idea of waging war outside of the domain of murder, but not always. This was part of the symbolic battle surrounding the war in Vietnam—defining a soldier as a protector of freedom rather than a murderer presents a constant challenge to the military. The Mentor works in this area of ambiguity to guide the reader to his conclusion: the structures of power, including the military, are working to thwart the common good.

The Mentor concludes his list by painting a picture of the adult world as a propaganda machine. For a group that values, above all, the acquisition of knowledge and truth, few crimes compare with the willful dissemination of falsehoods and the obstruction of knowledge gathering. Halbert writes that "the lifeblood of the hacker ethic is freedom of information."[360] "Information wants to be free" is a common slogan in the hacker community. The hacker exposes these lies, which is the true crime of hackers. Other groups have also recognized the problems of a propagandistic society. Where hackers may view it as a form of indoctrination and control, others, such as Robert McChesney see a much more banal motive—profit—and point out that the mass media has been usurped by the PR industry. According to McChesney, Americans can no longer

---

[359] David R. Roskos-Ewoldsen, Beverly Roskos-Ewoldsen, and Francesca R. Dillman Carpentier, "Media Priming: A Synthesis," in *Media Effects: Advances in Theory and Research*, ed. Jennings Bryant and Dolf Zillmann, 97-120 (Mahwah, NJ: Lawrence Erlbaum Associates, 2002).
[360] Halbert, "Discourses of Danger and the Computer Hacker," 362.

expect the news to offer unbiased reporting, but instead receive "inexpensive syndicated material and fluff."[361] Describing the consequences of news media corporatization, he states, "With fewer journalists, limited budgets, low salaries and lower morale, the balance of power has shifted dramatically to the public relations industry, which seeks to fill the news media with coverage sympathetic to its clients. . . . Their job is to offer the news media sophisticated video press releases and press packets to fill the news hole, or contribute to the story that does fill the news hole."[362] Whether through motivations of profit or deception, The Mentor argues that the search for truth is hampered by agents of the adult world. In his report on the keynote address of a hacker convention, Winn Schwartau writes: "'You guys are a national resource. Too bad everyone's so scared of you.' Applause from everywhere. The MIB knows how to massage a crowd. Hackers, according to [keynote speaker Robert Steele, ex-CIA type spy, senior civilian in Marine Corps Intelligence and now the President of Open Source Solutions, Inc.], and to a certain extent I agree, are the truth tellers 'in a constellation of complex systems run amok and on the verge of catastrophic collapse.'"[363]

Although The Mentor describes "crimes" on both sides, he engages in a form of moral justification by advantageous comparison.[364] The crimes that The Mentor attributes to hackers are not really crimes at all. He avoids the idea that hackers are stealing or

---

[361] McChesney, *Corporate Media and the Threat to Democracy*, 24.
[362] Ibid., 25-26.
[363] Winn Schwartau, "Cyber Christ Bites the Big Apple - Hope - Hackers on Planet Earth, New York City - August 13-14, 1994," *Phrack* 5, no. 46 (September 20, 1994): file 23.
[364] See Albert Bandura, "Social Cognitive Theory of Mass Communication," in *Media Effects: Advances in Theory and Research*, ed. Jennings Bryant and Dolf Zillmann, 121-53 (Mahwah, NJ: Lawrence Erlbaum Associates, 2002), 133.

breaking and entering. Even so, there is a significant difference between stealing phone service or breaking into a computer system and murder. This allows The Mentor to justify his actions by comparing it to the actions of others that are far worse and claim that his actions affect a greater good on society through the acquisition of knowledge through exploration and the breaking down of racial and social barriers (gender excluded for the moment). Yar explains, "Self-attributed motivations may well be rhetorical devices mobilised by hackers to justify their law-breaking and defend themselves against accusations of criminality and deviance."[365]

> *Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like.*

Once again, The Mentor reconstructs the notion of crime and criminal to his own ends and reinforces the hacker assertion that hacking is a means of satisfying curiosity. Some scholars believe that there is a limit to this kind of curiosity and that if hacking were more difficult, beginning hackers would never progress: "If the challenge is beyond the Newbie hacker then the less likely he/she is to achieve flow and therefore the less likely to develop their skill."[366] This is simplistic and ignores other underlying reasons for hacking. Eric Raymond argues that hacking is much more than simply breaking into computer systems or writing a better line of code: "The joy of hacking is a self-actualization or transcendence need which will not be consistently expressed until lower-level needs (including those for physical security and for 'belongingness' or peer esteem) have been at least minimally satisfied. Thus, the reputation game may be critical in

---

[365] Yar, "Computer Hacking: Just Another Case of Juvenile Delinquency?" 391.
[366] Beveren, "A Conceptual Model of Hacker Development and Motivations," 7.

providing a social context within which the joy of hacking can in fact *become* the individual's primary motive."[367] This places restrictions on who can attain this level of fulfillment through hacking because one must be able to afford the equipment, or, at the very least, be in a station in life where one has access to the equipment.

In this segment, The Mentor continues to emphasize the mind over the body. The mind/body separation is problematic because it is not as binary as it seems. Jewkes and Sharp point out that "identity is multidimensional and amorphous; we can be whoever, whatever, wherever we wish to be. And the Internet is the postmodern medium *par excellence;* the slate upon which we can write and rewrite our personalities in a perpetual act of self-construction."[368] They argue that the Internet "can liberate its users from the usual constraints of corporality. The Internet thus gives users a freedom of expression—a freedom of *being*—quite unlike anything they have at their disposal in the physical world."[369] Other scholars agree that this shift in identities may prove liberatory and even necessary for future political action. Brian Babcock states that "cyborg identities may well be the most suitable grounding for political struggle in a technologized world poised to enter a new millennium."[370] Babcock continues, "Adaptability and technical sophistication are requirements for success in such an environment; those people who, cyborg-like, possess technical skill and are comfortable floating in a fluid [sea] of

---

[367] Raymond, *The Cathedral & the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*, 102.
[368] Jewkes and Sharp, "Crime, Deviance and the Disembodied Self: Transcending the Dangers of Corporeality," 3.
[369] Ibid.
[370] Brian Babcock, *Cyborgs and Nomads: A Vision of Identity for the Information Age* (Stanford, CA: Humanities Honors Program, Stanford University, 2001), 59.

information [flow], will be the ones who are capable of effective social action in the twenty-first century. The strategic contested ground of politics has shifted; informational politics is a border war."[371]

The Mentor exults in his digital presence and the perhaps overstated claim that he can transcend beliefs about others based on their corporeal attributes. But even if he can, it is still unlikely that others will do the same. Vivian Sobchack explains that the body cannot simply be relegated to the hyperreal.[372] Human experience is lived in a corporeal state, an interaction and intertwining of the real and the hyperreal. Digital presence is linked to the body and the body influences one's digital presence. Throughout the manifesto, The Mentor demonstrates that the body still matters, even for hackers.

My crime is that of outsmarting you, something that you will never forgive me for.

The Mentor becomes more smug, revisiting two themes: that of the spiteful, bitter adult, and the assertion that he is smarter than others. The adult cannot handle being bested by the adolescent. The 1950's technobrain states that children should be seen and not heard. It is against convention that a child should be more intelligent than an adult, except in the case of a child prodigy. Although child prodigies are often revered for their skill, the nature of the mastered skill has changed. A child prodigy with a gift for music can be revered because adults understand the nature of music. A prodigy with a skill for computer systems cannot be understood and therefore is not revered. Rather, because

---

[371] Ibid.

[372] Vivian Sobchack, "Beating the Meat/Surviving the Text, or How to Get out of This Century Alive," in *Cyberspace/Cyberbodies/Cyberpunk: Cultures of Technological Embodiment,* ed. Mike Featherstone and Roger Burrows, 205-14 (London: Sage, 1995).

people tend to fear that which they do not understand, the result is often ostracism and demonization.

There is a sense of finality to The Mentor's statement, "something that you will never forgive me for," that demonstrates the world of the adult and the power structure that has been put into motion. The reason that The Mentor cannot be forgiven is because his act threatens the whole system of power. To those who stand to lose power when the system is overturned, this is the unpardonable sin. It is even more damnable when threatened by one who does so outside of the traditional methods of power. Society seems more forgiving of those who rise to power through military or financial means than of those who rise to power by infiltrating the communication networks (i.e., con men and propagandists).

> *I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.*

Once again, The Mentor identifies himself as a hacker and labels this document a manifesto. Lyon argues that a manifesto "seeks to assure its audience—both adherents and foes—that those constituents can and will be mobilized into the living incarnation of the unruly, furious expression implied in the text. The manifesto is, in other words, a genre that gives the appearance of being at once both word and deed, both threat and incipient action."[373] The manifesto closes with an ominous warning that is especially poignant in light of his arrest a short time before. Government, law enforcement, and telecommunications companies can stop individual hackers, but the ability and the *need*

---

[373] Lyon, *Manifestoes: Provocations of the Modern*, 14.

to hack is in place and as long as that situation exists, there will be hackers. Gunkel provides further insight into this passage: "Hacking, like a parasite, takes place in and by occupying and feeding off a host that always and already has made a place for it to take place. It is for this reason that, despite the valiant efforts of law enforcement, hacking cannot be stopped or even hindered by cracking down on and punishing individual hackers."[374] Hacking is a natural consequence of the system. Curiosity is embedded in human nature. As long as there is a system at work, someone will want to know how the system operates and try to make it do something else.

The Mentor closes with his name, marking his words with his underground identity rather than his given name. This is the beginning of his conversion to the digital realm. He has repudiated the physical world in favor of the digital world and has taken on a new name; one that signals that he is willing to help others to the place where he has come. But a subtle linguistic twist illustrates the kind of mentor he is and the kind of hacker that one should become—he brands this document as "his" manifesto. Although there is resonance in his words, this label serves as a reminder that each hacker must find his or her own way into and through hacking. With this maneuver, he stops just short of speaking for all hackers and invites each to form his or her own manifesto. It was not The Mentor who named this the "Hacker Manifesto," but others, including hackers.

The Mentor states that the manifesto has been reprinted on websites, shirts, and textbooks but he has never received any compensation for his writing. "I've never taken a dime for any of it. I'm not some kind of Stallman-esque 'information must be free' freak,

---

[374] Gunkel, *Hacking Cyberspace*, 9.

but I would feel grossly hypocritical if I tried to milk cash out of the people who identify with it enough to be willing to pay for it."[375] Two decades later, The Mentor still fulfills the role of mentor for new generations of hackers through his words and his actions.

What Does the Hacker Manifesto Reveal About Hacker Collective Identity?

Several recurring themes within "The Conscience of a Hacker" illustrate core tenets of hacker collective identity: hackers are not like others—they are digital beings endowed with superior intellect; the masses are blind and the education system is facilitating that blindness; the adult world is not to be trusted; hacking is not a crime; power can be gained through the use of technology; and cyberspace is a site of freedom.

The Mentor makes it clear that *hackers are not like other people*; they are more intelligent. This intelligence is both a blessing and a curse. While others may require spoon feeding in school, hackers are forced to endure it. This ideal of intelligence as the norm can be seen today in assertions of the elite-ness of one's hacking. Moreover, the hacker is a being residing in, but not of, the physical realm, and rejects the laws and rules of the analog world. This complete repudiation of physical space provides hackers with the manifest destiny to colonize and rule cyberspace.

The masses are blind and the education system is facilitating this blindness. But it is not only the educational system that is facilitating this blindness—it is the entire media system. In describing the ways that information is now used, Tiziana Terranova draws heavily on a fundamental assumption of information theory: "information can only be

[375] Loyd Blankenship, email message to author, May 2, 2003.

defined as a ratio of signal to noise."[376] She explains that communication, then, relies upon the ability to clear a channel of noise. Although later on, she points out the inadequacies of this view when examining an information society (or, to use Terranova's term, "informational milieus") this is still a useful way to consider why hacking is a necessary political strategy.[377] If a signal cannot be cleared—in other words, if the lies cannot be separated from the truth—the public will remain in a state of blindness. However, unlike the protagonist in Plato's allegory of the cave, the hacker takes no pity upon those who remain in the cave and has no desire to go back into the cave to enlighten the masses.[378] Hackers fall into the essentializing trap, considering the blindness of the masses to be the mark of an inferior intellect rather than the result of a sustained systematic psychological assault by the adult world.

The adult world is not to be trusted. This is a problematic value because everyone ages. A youthcentric movement seems destined to an existence of perpetual adolescence. Lessons learned by those who have gone on before may be rejected, much like parental advice that is rejected by children as "too old fashioned." This privileging of youth may seem paradoxical because hackers also value knowledge, which comes with time and experience. Although older hackers exist, hacker collective identity values youth and distrusts the adult world. Even some of the old guard hackers can seem curmudgeonly to the rising generation of hackers. For example, Oxblood Ruffin's support of the World

---

[376] Tiziana Terranova, "Communication Beyond Meaning: On the Cultural Politics of Information," *Social Text* 22, no. 3 (2004), 56.
[377] Ibid., 60.
[378] See Plato, "Republic," in *The Collected Dialogues of Plato, Including the Letters*, ed. Edith Hamilton and Huntington Cairns, 575-844 (Princeton, NJ: Princeton University Press, 1961), 7.516c.

Trade Organization's right to free speech is at odds with the distrust of power structures found in this manifesto.[379]

Hackers distrust the adult world because it represents fear and ignorance of technology and forgetfulness of adolescence. The adult world includes the structures of power embodied in nation states, law enforcement agencies, and corporate interests that seek to demonize and destroy the hacker. Nelson argues that "the nation-state and cyberspace as environments are also both the monstrous spawn of the military-industrial matrix: gridded and programmed in accordance with the demands of command-control-communication-intelligence, or C3I. Both the nation state and cyberspace are concerned with mapping territories, constituting boundaries, and charting population movements, as well as constituting identities and determining potential risks."[380] The world of the adult is a world of control—for the ideal adult, as far as the hacker can tell, there would be no more frontier, no new puzzles to solve. Everything would have its place and uncertainty would be eradicated from the world.

The idea that *hacking is not a crime* is reinforced in this manifesto. Hackers are part of the information society elite. Even those who own the infrastructure would be unable to use it if hackers chose not to cooperate. Although hackers are often viewed as a destructive force, without them, creation would be difficult or impossible. Jon Erickson argues that hackers are pioneers.[381] Without individuals who are willing to use things

---

[379] See Oxblood Ruffin, "Hacktivismo," *Cult of the Dead Cow,* July 17, 2000, http://www.cultdeadcow.com/archives/2000/07/hacktivismo_by_oxblo.php3 (accessed January 30, 2006).
[380] Nelson, "Maya Hackers and the Cyberspatialized Nation-State: Modernity, Ethnostalgia, and a Lizard Queen in Guatemala," 297.
[381] Erickson, *Hacking: The Art of Exploitation,* 4.

differently, it is conceivable that humans would never have evolved into the tool-using stage. Those who possess the spirit of hacking create and recreate the technological infrastructures that the adult world seeks to protect. So long as there are communication networks, hackers will attempt to break into them. Rather than trying to fight them, perhaps there is much that can be learned from hackers. Cyberspace is the world of the hacker and members of the adult world, who enter not as natives but as immigrants, must negotiate a place within that world.

For hackers, *power can be gained through the use of technology.* Through technology, hackers can resist the evils that are placed upon them by the adult world. Sal Randolph writes:

> All social structures require acceptance in order to operate. The Internal Revenue Service can intimidate individuals, but the system would be impossible to maintain if *everyone* simply refused to pay. The fact that we don't refuse implies that over all, and in practice, a majority of U.S. citizens accept the basic workings of their government. This is not to deny that the government and the IRS have real power, but to some extent that power is created, as if by magic, by our belief that it is so. Part of that belief is created by the fear of punishment. Governments consciously deploy that fear as a means of control but this only demonstrates more clearly that the main powers of governments and organizations are psychosocial.[382]

---

[382] Sal Randolph, "Free Words to Free Manifesta: Some Experiments in Art as Gift," *Ethics & the Environment* 8, no. 1 (2003): 71-72.

Hackers reject the rules of the analog world and are able to resist and evade government control through an understanding of technology and intellectual capacity. They believe that the structures of power represented by telephone industries, government officials, and law enforcement agencies are not to be trusted. Hackers do not seem to fear punishment, recognizing that the fight will continue and that they will eventually emerge victorious. The Mentor writes, "You may stop this individual, but you can't stop us all."

Cyberspace is a site of freedom. In the digital realm, the digital self of the hacker finally finds a home. The land of the boards is where being takes place for hackers and where connections are forged and information is exchanged. Jan Fernback explains that "cyberspace is a repository for collective cultural memory—it is popular culture, it is narratives created by its inhabitants that remind us who we are, it is life as lived and reproduced in pixels and virtual texts. It is sacred and profane, it is workspace and leisure space, it is a battleground and a nirvana, it is real and it is virtual, it is ontological and phenomenological. . . . Cyberspace is essentially a reconceived public sphere for social, political, economic, and cultural interaction."[383] This uncertainty makes cyberspace exciting for the hackers and frightening for the adult world. In 1986, cyberspace was a world out of control, a frontier that may or may not be tamed. But cyberspace has gone the way of other previously radical elements, going through the cycle of wild abandon and passion, a period of mainstreaming in which it the rough edges are knocked off to make it palatable for the masses, and, finally, complete co-optation and sanitization by the structures of power.

---

[383] Fernback, "The Individual within the Collective: Virtual Ideology and the Realization of Collective Principles," 37.

The collective identity forged in “The Conscience of a Hacker” provides a way of being for hackers even today. In the next chapter, we will see how this collective identity is enacted and reinforced through actual hacking activities. Some elements of the hacker identity have been altered. For example, in contrast to The Mentor’s professed color blindness and exhortation to judge others by their words, a hack can create a collective identity that is homophobic and xenophobic, riddled with racial slurs. Some of the elements of the hacker collective identity laid out in this manifesto are beautiful and would provide a good model for living, while others are naïve at best and dangerous at worst. Even so, this manifesto provides insight into the genesis of hacker collective identity.

Conclusion

Exigencies such as Operation Sundevil spurred hackers to organize from a loose collective to a social movement. The formation of hackers into a social movement was necessary because of increasing pressure by the United States government and the continual demonization of the hacker by the media, government agencies, and legislation. With this mounting force, the hackers had to organize, be driven even further underground, or eventually destroyed. As they organized into a movement, they developed a collective identity through their publications, especially “The Conscience of a Hacker,” which is commonly accepted as the “Hacker Manifesto.”

Chapter 4

Hacktivism as Rhetorical Action

When hackers became politicized, it made sense that they would use their skills for political ends. Although this seems reasonable on the surface, it is clear that society was not, and still is not, prepared for the potential actions of a political group with the ability to shut down anything connected to a networked computer. The distributed nature of telecommunication grids, information systems, databases, and government communication systems creates a situation in which hackers can wield an extraordinary amount of power. Members of L0pht, a hacking collective, testified before the Senate Subcommittee on Governmental Affairs that "in a matter of 30 minutes, they could make the entire Internet unusable for a couple of days."[384]

Much of the literature on hackers and hacking has focused on the damage inflicted by hackers, strategies for keeping hackers out, or legal implications of hacking.[385] Although there are instances where hackers have broken into a server simply to see if they can, there are also occasions when the hack was motivated by political ends. This chapter provides a framework for examining hacktivism as a means for political action and as a rhetorical strategy. Hacktivism overcomes some of the limitations of

---

[384] Senate Governmental Affairs Committee, "Weak Computer Security in the Government: Is the Public at Risk?" *Senate Governmental Affairs Committee*, May 19, 1998, http://www.senate.gov/~govt-aff/051998_summary.htm (accessed February 13, 2006).

[385] For example, see John Conley, "Outwitting Cybercriminals," *Risk Management* 47, no. 7 (2000): 18-26; Jim Kates et al., "The Reality of Hackers," *Risk Management* 48, no. 7 (2001): 50-57; Mark G. Milone, "Hacktivism: Securing the National Infrastructure," *The Business Lawyer* 58, no. 1 (2002): 383-413; Schwartau, *Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Destruction*.

traditional means of protest and can be accomplished by using many techniques. Some hacktivism techniques are disputed within the hacker community. A case study of a politically motivated hack of the *New York Times* website provides a way to examine some of the rituals and norms of hacking that are enacted and reinforced through acts of hacktivism. The *New York Times* hack demonstrates how hacktivism may serve mainly to fulfill what Richard Gregg described as the "ego function" of protest rhetoric, rather than seeking to enact actual change within society.[386]

What is Hacktivism?

Hacktivism is often referred to as "electronic civil disobedience" (ECD). Stefan Wray states that in electronic civil disobedience, "The same principles of traditional civil disobedience, such as trespass and blockage, will be applied, but more and more these acts will take place in electronic or digital form: The primary site for ECD will be in cyberspace."[387] The main difference between hacktivism and simple criminal hacking is intent. Any unauthorized access to another computer system or network is criminal behavior. Even so, there is criminal behavior that seeks to right some social injustice and there is criminal behavior that seeks only to enrich the individual engaging in the criminal activity. Simple criminal hacking, such as hacking to steal credit card numbers and identities or breaking into websites, is the type of hacking that is the most well known.[388]

---

[386] See Gregg, "The Ego-Function of the Rhetoric of Protest."
[387] Stefan Wray, "On Electronic Civil Disobedience," *Peace Review* 11, no. 1 (1999): 108.
[388] See note 385 above.

Hacktivism is using the tools of hacking to disseminate a political or social message. Maura Conway notes the shift from hacking for enjoyment and hacking as political action:

> Hacktivism grew out of hacker culture, although there was little evidence of sustained political engagement by hackers prior to the mid-1990s. 1998 is viewed by many as the year in which hacktivism really took off. It was in '98 that the US-based Electronic Disturbance Theatre (EDT) first employed its FloodNet software in an effort to crash various Mexican Government websites to protest the treatment of indigenous peoples in Chiapas and support the actions of the Zapatista rebels. Over 8000 people participated in this, one of the first digital sit-ins. It was also in '98 that JF, a young British hacker, entered about 300 websites and replaced their home pages with anti-nuclear text and imagery. At that time, JF's hack was the biggest political hack of its kind. 'Hacktions' also took place in Australia, China, India, Portugal, Sweden, and elsewhere in the same year. Michael Vatis, one-time Director of the FBI's National Infrastructure Protection Center (NIPC), has labeled such acts as cyberterrorism."[389]

Perhaps the main difference between hacking as white collar crime or corporate espionage and hacking as hacktivism is that hacktivism is a rhetorical act. In hacktivism, the hacker is not interested in personal gain, but in the dissemination of a particular message. That message may be directed at a particular organization, such as the case where an anti-fur activist hacked the website of a furrier, or the website itself may be

---

[389] Conway, "Hackers as Terrorists? Why It Doesn't Compute," 12.

inconsequential, serving only as a means of reaching viewers. Intent is perhaps the most important element for defining hacktivism but ascribing intent to any organization or individual is a troubling prospect. After all, a hacker may download a file containing credit card information in order to sell the information or to damage the reputation or financial situation of a corporation that the hacker finds socially or politically repugnant—or both. Despite such grey areas, motivation, whether implied or expressed, is a key element that distinguishes hacking as mere criminal activity from hacktivism, if not from a legal perspective, from rhetorical and ethical standpoints.

The rise of the hacker marks a shift in the locus of power. Debora Halbert points out that American society is growing increasingly dependent on technology.[390] With this dependence comes a price; a natural consequence of this dependence is greater vulnerability. This type of vulnerability can be exploited from anywhere a modem connection is available. The individuals who pose a threat—and how they are rhetorically constructed—have also changed. Sandor Vegh states that "most works on the subject, whether classified as information security, computer crimes, online social activism, or cyberterrorism, intentionally or unintentionally blur the boundaries of socially justified activism and criminal or even terrorist activities. The simple injection of colorful terminology, such as cybervandalism, cyberterrorism, or malicious hackers, disregards the motives and goals of online activism and puts those socially or politically progressive

[390] Halbert, "Discourses of Danger and the Computer Hacker," 368.

but marginalized voices whose main chance to be heard is through the Internet even more to the peripheries."[391]

The way hacktivism is defined carries rhetorical consequences. Sometimes it is difficult even for participants to agree on a definition for their actions. In their observations of a protest against the Vietnam War, Thomas Benson and Bonnie Johnson describe such an occurrence: "Was the action primarily a rhetorical one, designed to persuade the government, public, and participants to work for an end to the war? Or was it, as some said, an act of resistance, designed to cripple the war effort by attacks upon the government's time and property? Even the labels used to describe the event were dichotomized: some called it a *march, rally,* or *demonstration,* others a *resistance,* or *mobilization.* The word *confrontation,* chosen by its organizers as the official title of the event, seems to be capable of synonymity with either side of the dichotomy, depending on the user."[392] Confrontation is a common frame when considering social movement rhetoric but confrontation can be a dangerous strategy. Robert Scott and Donald Smith explain that when the establishment is threatened, it often responds violently. Even this seemingly self-defeating strategy can be used for a rhetorical ends: "Those who would confront have learned a brutal art . . . which demands response. But that art may provoke the response that confirms its presuppositions, gratifies the adherents of those presuppositions, and turns the power-enforced victory of the establishment into a

---

[391] Vegh, "Hacktivists or Cyberterrorists? The Changing Media Discourse on Hacking," para. 7.
[392] Thomas W. Benson and Bonnie Johnson, "The Rhetoric of Resistance: Confrontation with the Warmakers, Washington D.C., October 1967," *Today's Speech* 16 (September 1968): 35-36.

symbolic victory for its opponents."[393] Regardless of how social movement phenomena are defined—protest, resistance, violence, rioting, civil disobedience, hacktivism, terrorism—in order to disclose the underlying meaning of a particular action, it is necessary to examine the action *as if it were rhetorical* even if the strategy appears on the surface to be non-rhetorical.[394] There is certainly nothing to be lost by adopting such an approach and a world of meaning and understanding to be gained.

But who actually practices hacktivism? Hackers speak derisively of "script kiddies" who do not hack into a system using their own ingenuity, but rather choose to rely on readily available scripts that exploit weaknesses in networks. Although this is not a distinction that the general populace makes, it raises an important issue—the availability of scripts for hacking into computer systems on the Internet levels the field. Hugh Martin explains that "electronic protesting these days is a simple matter of downloading easy-to-use software from the Web, or of visiting a protest site where you can set your browser to bombard a target site with requests for information. Anyone can be a hacktivist."[395] Even those without technical expertise can now do the work of the hacker.

---

[393] Robert L. Scott and Donald K. Smith, "The Rhetoric of Confrontation," *Quarterly Journal of Speech* 55 (1969): 8.

[394] For example, Robert Doolittle explains that even riots can be viewed as rhetorical phenomena. Robert J. Doolittle, "Riots as Symbolic: A Criticism and Approach," *Central States Speech Journal* 27 (1976): 310-17. Other scholars have made a case for uncivil discourse, such as obscenity and diatribes, as potentially useful rhetorical strategies. See Haig A. Bosmajian, "Obscenity and Protest," *Today's Speech* 18 (1970): 9-14; Theodore Otto Windt, Jr., "The Diatribe: Last Resort for Protest," *Quarterly Journal of Speech* 58 (1972): 1-14.

[395] Martin, *Hacktivism: The New Protest Movement?* para. 6.

Hacktivism is an important component of many protest activities because the Internet is becoming more and more ingrained into our lives. But the Internet can be used not only as a tool of liberation, but as a tool of oppression. It can also be used as a tool of escape by those seeking to avoid dissenters. For example, Norman Solomon described plans by the World Bank to cancel a physical meeting in Barcelona, choosing to hold the meeting in cyberspace as a way to avoid protesters.[396] In his discussion of Critical Art Ensemble, Wray states, "Electronic Civil Disobedience is seen as imperative by these writers, not only because of the proliferation and importance of computer technology, but also because traditional forms of civil disobedience have become less and less effective. The streets, they say, have become the location of dead capital. To seriously confront capital in its current mobile, electronic form, resistance must take place in the location where capital now exists in greatest concentrations, namely in cyberspace."[397]

How is Hacktivism Done?

There are many means by which hacktivism takes place. There are many sources that provide detailed explanations of hacking techniques.[398] Common methods for performing hacktivism include: social engineering, website defacement, email bombs, and electronic sit-ins and denial of service attacks. These techniques are not universally

---

[396] Solomon, "Hiding out in Cyberspace," 17.
[397] Wray, "On Electronic Civil Disobedience," 109.
[398] For more in-depth discussion of the techniques used to compromise computer systems, see Erickson, *Hacking: The Art of Exploitation.* This is widely considered to be one of the best technical discussions of hacking because rather than simply teaching one how to use exploits that already exist, this text teaches one how to create exploits. However, the book is extremely technical and requires a high level of computing knowledge, including machine language.

accepted as ethical within the hacker community, and are part of an ongoing debate concerning the means and ends in hacktivism.

Social Engineering

Perhaps the first rule of hacking is that the simplest way into a system is not through technology but through people. Accessing systems through human rather than technological means is referred to by hackers as "social engineering."[399] If a hacker wished to access a computer system at a particular corporation, he or she could call in to a customer service department and claim to be a member of the corporation's Information Technology department. After making a bit of small talk and asking about call volume in the call center that day, the hacker would ask the person if he or she has been having trouble with his or her computer that day. The person will likely perceive some kind of trouble, whether it be a slower connection than normal, slower download times, or misplaced documents. The hacker would then state that there is a problem with the person's network connection and ask the person for his or her login and password. If only one person provides the login and password, the hacker can access the network. Mitnick states, "It's human nature to trust our fellow man, especially when the request meets the test of being reasonable."[400] If the customer service representative believes that the hacker is with the IT department and that the person will fix the network connection, it may seem reasonable to provide the login and password. Many people are still unaware

---

[399] For discussion and examples of social engineering, see Earth, "Social Engineering"; Mitnick and Simon, *The Art of Deception: Controlling the Human Element of Security*.
[400] Mitnick and Simon, *The Art of Deception: Controlling the Human Element of Security*, 32.

of the dangers of providing their login and password information. Using a similar scenario as recently as December 2004, the Internal Revenue Service found that "[they] were able to convince 35 managers and employees [out of 100] to provide us their username and to change their password."[401]

Website Defacement

In website defacement, the goal is to break into the system and upload a new version of the page that has been modified by the hackers. However, there is (sometimes) more to this than simply uploading a new webpage. If the hackers gain complete access to the system ("root") they may be able to alter the user IDs and passwords such that the page cannot be taken down until the system administrators are able to break into their own system. This prolongs viewer exposure to the modified page. There seems to be a kind of ethical code to website defacement. For example, it is rare for hackers to delete content—generally it is placed in another folder. Also, it is common for hackers to explain how they gained access to the system and sometimes even explain how to patch the system.

There are varying degrees of sophistication within the hacker community and this is reflected in website defacements. A casual examination of defacements on Zone-H[402], a security website, reveals that a majority of defacements fall into the category of "script kiddie" hacks that say little more than "ZafT 0wnz j00" or something similar, sometimes

---

[401] See "While Progress Has Been Made, Managers and Employees Are Still Susceptible to Social Engineering Techniques," (Washington, DC: Department of the Treasury, 2005), 3.
[402] See http://www.zone-h.com/en/defacements for a constantly updated archive of website defacements.

with a graphic. These are often mass defacements, done by simply scanning networks for servers with open ports or looking for unpatched systems. This is hacking by the path of least resistance. On the other hand, some defacements are clearly targeted and send a message to the owner of the website. These are more often done by "real hackers" although sometimes script kiddies employ similar tactics.

Email Bombs

As with denial of service attacks, email bombs overload email servers so legitimate email cannot be received. Most email servers have a set amount of space allocated to each user and once this limit is reached, no new messages can be delivered. The sender receives an error message and must resend the message later. Email bombing is done by sending the recipient many large messages, or an astronomical amount of small messages. Some servers limit the size of messages that can be received, thus limiting the tactic to sending small messages. As with denial of service attacks, email bombing can be easily automated and the necessary resources for the attack can be distributed.

Electronic Sit-ins / Denial of Service Attacks

As the name implies, electronic sit-ins are similar to physical sit-ins—both seek to deny access by occupying space. Rather than occupying space physically, as in a traditional sit-in, electronic sit-ins occupy space in the form of connections and

bandwidth. Servers can handle only as many connections as bandwidth allows. When this connection limit is exceeded, others attempting to access material on that server will be denied access until those who are already connected are no longer accessing material. This is why these kinds of actions are called denial of service (DOS) or distributed denial of service (DDOS) attacks.[403] This is a very simple attack to implement and one needs little skill to enact it—some groups have even automated the process.[404] At its most basic level, a denial of service attack could be enacted by simply going to a webpage and continually hitting the refresh button. Most servers could handle this kind of action, but if hundreds or thousands of computers do this, even powerful servers may be brought down.

Because many network attacks are more efficiently done with many computers, it is in the interest of the attacker to gain access to many machines—whether through a collective united in the attack or by commandeering the machines of unwitting accomplices. One lesser publicized danger of spyware and viruses has to do with the creation of "zombie networks." Many types of spyware allow for both reception of messages and the transmission of data. If a person has spyware on his or her machine, it is possible to create an exploit that will use the existing spyware to send data to a different server—the target of the attack. This is also a problem of various kinds of viruses that can install a backdoor into the system that can also be used to take over the computing resources of the machine such as bandwidth, processing power, and email

---

[403] For more on DDOS attacks, see Conley, "Outwitting Cybercriminals."

[404] One example of this is Electronic Disturbance Theater's program called Zapatista Floodnet. For more on this, see Jill Lane, "Digital Zapatistas," *TDR: The Drama Review* 47, no. 2 (2003): 129-44.

send capabilities. A person whose computer is infected with spyware or certain viruses may unknowingly participate in a denial of service attack.

What's New and Different about Hacktivism?

Scholars sometimes conflate hacking with traditional forms of protest. For example, Schwartau states, "Graffiti on billboards, graffiti on web sites, same difference, different medium."[405] However, the medium makes a considerable difference. Hacktivism has attributes that differentiate it from other forms of protest, even mediated forms such as culture jamming.

A Brief History of Hacktivism

Perhaps the first group to use technology for political activism was the Technological American Party (TAP), which came out of the Yippies. According to Tim Jordan and Paul Taylor, TAP's newsletters "provided a raft of detailed technical information, predominantly about how to phone-phreak (obtain free phone calls through the technical manipulation of the phone system), but also on a range of artifacts including burglar alarms, lock-picking, pirate radio and how to illegally alter gas and electric meters."[406] In 1981, Chaos Computer Club (CCC) began in Germany. They describe themselves as "a global community, which campaigns transboundarily for the freedom of

[405] Schwartau, *Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Destruction*, 25.
[406] Tim Jordan and Paul A. Taylor, *Hacktivism and Cyberwars: Rebels with a Cause?* (New York: Routledge, 2004), 14.

information and communication without any censorship - by any government or company, and which studies the impacts of technology for the society and the individual. These goals are also stated in the preamble of the club's constitution, and are implemented in a lot of projects by members and friends of the CCC."[407] Although this statement was written in 2003, Steven Furnell explains that "the exploits of [CCC] over the years have had a considerably political slant," and that members were linked to an espionage case in the late 1980's.[408]

Shortly after the Chaos Computer Club began, *2600* (named after the frequency that allowed phreakers to make free phone calls from pay phones) began publishing in the United States in 1984. The date is significant, as the publisher operates under the pseudonym Emmanuel Goldstein, the protagonist from the George Orwell novel *1984*. *2600* is still operating and has had its share of legal battles, most notably due to its publication of the DeCSS code which allows DVD owners to circumvent the copy protection on their DVDs.[409] Shortly thereafter, *Phrack* began publishing digitally in 1985.

In 1984, Cult of the Dead Cow (CDC) formed, which is perhaps one of the most politically active and high profile hacker groups. One of their members, Omega, is said to have coined the term "hacktivism."[410] Like L0pht (which shares some members with CDC), they are best known for revealing security flaws in software, specifically with

---

[407] Chaos Computer Club, "CCC Summary: What Is the CCC?" May 10, 2003, http://www.ccc.de/club/?language=en (accessed January 27, 2006).
[408] Steven Furnell, *Cybercrime: Vandalizing the Information Society* (Boston: Addison-Wesley, 2002), 72.
[409] For extensive documentation on this legal battle, see http://www.2600.com/dvd/docs/.
[410] See Oxblood Ruffin, "Hacktivism, from Here to There," *Cult of the Dead Cow*, March 28, 2004, http://www.cultdeadcow.com/cDc_files/cDc-0384.html (accessed February 1, 2006).

their “Back Orifice” utility, which demonstrated significant security flaws in the Microsoft Windows operating system. In 1999, they began to draw more explicit links between activism and computer technology by forming “Hacktivismo.” The Hacktivismo Declaration draws on the United Nations Universal Declaration of Human Rights, stating that:

> We are convinced that the international hacking community has a moral imperative to act, and we declare:
>
> That full respect for human rights and fundamental freedoms includes the liberty of fair and reasonable access to information, whether by shortwave radio, air mail, simple telephony, the global internet or other media.
>
> That we recognize the right of governments to forbid the publication of properly categorized state secrets, child pornography, and matters related to personal privacy and privilege, among other accepted restrictions. But we oppose the use of state power to control access to the works of critics, intellectuals, artists, or religious figures.
>
> That state sponsored censorship of the Internet erodes peaceful and civilized coexistence, affects the exercise of democracy, and endangers the socioeconomic development of nations.
>
> That state-sponsored censorship of the Internet is a serious form of organized and systematic violence against citizens, is intended to generate confusion and xenophobia, and is a reprehensible violation of trust.

> That we will study ways and means of circumventing state-sponsored censorship of the Internet and will implement technologies to challenge information rights violations.[411]

Here we see an extreme depiction of the hacker motto, "information wants to be free." For CDC, censorship of the Internet is equivalent to "systematic violence." Yet the CDC recognizes the right to "forbid the publication of properly categorized state secrets, child pornography, and matters related to personal privacy and privilege." But what constitutes a "properly categorized state secret?" Governments can enact wholesale censorship and still remain within the bounds of this declaration by simply declaring the censored material a "state secret."[412] Hacktivismo recognizes this issue:

> The term "lawfully published" is full of landmines. Lawful to whom? What is lawful in the United States can get you a bullet in the head in China. At the end of the day we recognize that some information needs to be controlled. But that control falls far short of censoring material that is critical of governments, intellectual and artistic opinion, information relating to women's issues or sexual preference, and religious opinions. That's another way of saying that most information wants to be free; the rest needs a little privacy, even non-existence in

---

[411] Hacktivismo and Cult of the Dead Cow, "The Hacktivismo Declaration," *Hacktivismo*, July 4, 2001, http://www.hacktivismo.com/public/declarations/en.php (accessed January 27, 2006).

[412] The George W. Bush administration has often hidden behind the veil of "security" when pressed for information. See "Government Secrecy Continued to Rise in 2004."

> the case of things like kiddie porn. Everyone will have to sort the parameters of this one out for themselves.[413]

However, hacker groups have come to different conclusions as to how these parameters should be sorted out. One such group that came to different conclusions is the electrohippie collective, a hacktivist group in the United Kingdom.

The Question of Means and Ends in Hacktivism

The question of means and ends in hacktivism is disputed within hacktivist collectives. Perhaps the most problematic aspect of the Hacktivismo Declaration is the conclusion: "We will study ways and means of circumventing state-sponsored censorship of the Internet and will implement technologies to challenge information rights violations." What, exactly, is an information rights violation? Hacktivismo is making an argument based on the consumption of information but the production of information is also essential. In the Hacktivismo FAQ, they write, "We are also interested in keeping the Internet free of state-sponsored censorship and corporate chicanery so all opinions can be heard."[414] This underlying focus on information access and consumption at times paints CDC into an ideological corner, which can be observed in their response to a paper published by the electrohippies, titled "Client-side Distributed Denial-of-Service: Valid

---

[413] Oxblood Ruffin, A Dwarf Named Warren, and Little Marie, "The Hacktivismo FAQ v1.0," *Cult of the Dead Cow*, 2000-2001, http://www.cultdeadcow.com/cDc_files/HacktivismoFAQ.html (accessed January 30, 2006).
[414] See Ibid.

Campaign Tactic or Terrorist Act?" in which the electrohippies defend the use of client side denial of service attacks.

The electrohippies reveal their anti-capitalist leanings at the very beginning: "As Jesus ransacked the temple in Jerusalem because it had become a house of merchandise, so the recent attacks on ecommerce web sites are a protest against the manner of its recent development. But, do we label Jesus as a terrorist? Those involved probably have a reverential view of the 'Net. The public space that the 'Net represents is being promoted as a marketplace for large corporate interests, and many of those who use the 'Net for other purposes are dissatisfied with this."[415] The electrohippies are not content with a consumption model of information—the ability to express one's opinions by eclipsing those held by the more powerful is a justifiable use of technology. The disagreements between Hacktivismo / CDC and the electrohippies help to illuminate the ideological split within the hacker community concerning what are appropriate means for enacting hacktivism.

The groups view the legitimacy of denial of service attacks differently. The electrohippies argue that client side denial of service attacks have greater legitimacy as a protest action: "Client-side distributed actions require the efforts of real people, taking part in their thousands simultaneously, to make the action effective. If there are not enough people supporting then the action it doesn't work. The fact that service on the WTO's servers was interrupted on the 30th November [and] 1st of December, and

---

[415] DJNZ and the Action Tool Development Group of the electrohippies collective, "Occasional Paper No. 1: Client-Side Distributed Denial-of-Service: Valid Campaign Tactic or Terrorist Act?" *the electrohippies collective*, February, 2000, http://www.fraw.org.uk/ehippies/papers/op1.pdf (accessed January 30, 2006).

significantly slowed on the 2nd and 3rd of December, demonstrated that there was significant support for the electrohippies action."[416] They contrast this form of denial of service attack with server side denial of service attacks that can be done with only a few individuals and a legion of zombie computers. The use of client-side attacks by the electrohippies provides what they call "the electrohippies democracy guarantee."

Cult of the Dead Cow rejects this premise, arguing that "Denial of Service, is Denial of Service, is Denial of Service, period. The only difference between a program like Stacheldraht [a DDoS application written by The Mixter] and the client side javascript program written by the Electrohippies is the difference between blowing something up and being pecked to death by a duck. And if numbers lend legitimacy—as the Electrohippies propose—then the lone bomber who tried to assassinate Hitler in his bunker was wrong and the millions who supported the dictator were right."[417] Ignoring for the moment the logical fallacy in this statement, what this illustrates is a fundamental disagreement on the nature of democratic practice. The electrohippies seem to subscribe to the great hope of democracy—that the majority of the people will support that which is just and good the majority of the time. If CDC does not believe that numbers grant legitimacy, then what does? In their opposition to denial of service attacks, CDC appeals to the First Amendment but it is difficult to ascertain whether they appeal to a transcendent ideal of freedom of speech, appeal to the First Amendment as rule of law, or conflate the First Amendment with a transcendent ideal of freedom of speech. Any of these possibilities are problematic. If the first proposition, what gives the CDC the right

---

[416] Ibid., 3.
[417] Ruffin, "Hacktivismo."

to define this ideal of free speech? If the second or the third, then they ignore the global nature of the Internet; the United States Constitution should not necessarily set the standard by which other nations should be judged.

The electrohippies recognize that by engaging in denial of service attacks they are preventing freedom of speech. However, they justify this in two ways: the target must be reprehensible to a majority of the people and the attack should be limited to a specific, politically salient occasion. For example, they point out that their actions against the World Trade Organization (WTO) took place only during the conference in Seattle, which provided an opportunity to raise consciousness concerning the actions of the WTO and allowed those who opposed the WTO to voice their arguments.[418] But does this actually work? Wray explains that the effectiveness of electronic civil disobedience as a strategy is contingent on the desired ends:

> If the desired goal of ECD is to draw attention to particular issues by engaging in actions that are unusual and will attract some degree of media coverage, then these actions have a high degree of effectiveness. If, however, effectiveness is measured by assessing the action's ability to catalyze a more profound mobilization of people, then probably these new techniques are not effective. . . . Electronic civil disobedience is not likely to be an organizing tool, and the end result of the ECD is not likely to be an increase in the ranks of the disaffected.

---

[418] See DJNZ and collective, "Occasional Paper No. 1: Client-Side Distributed Denial-of-Service: Valid Campaign Tactic or Terrorist Act?" 7-8.

> Rather ECD appears to be a means to augment or supplement existing organizing efforts, a way to make some noise and focus attention.[419]

In the case of the WTO protests, where the actions of the electrohippies were likely to generate news coverage in addition to that already generated by the disruptions taking place in the physical space of Seattle, this would likely be an effective use of denial of service attacks. One can only speculate on how effective electronic civil disobedience would be with little action taking place in physical space but it seems unlikely that the electrohippies would engage in such actions because they would be less likely to bear a stamp of legitimacy (the organization must be reprehensible to a majority of the people).

Another fundamental difference between the two groups concerns the nature of cyberspace compared to physical space. The electrohippies argue that "as another part of society's public space the Internet will be used by groups and individuals as a means of protests. There is no practical difference between cyberspace and the street in terms of how people use the 'Net."[420] The electrohippies seem to believe that the tactics that work in the real world will work in the digital world. This is further demonstrated in their comparison between protest actions online and offline: "Distributed clientside DoS action is only effective if it has mass support, and hence a democratic mandate from a large number of people on the Net to permit the action to take place. These type[s] of actions

---

[419] Wray, "On Electronic Civil Disobedience," 110.

[420] DJNZ and collective, "Occasional Paper No. 1: Client-Side Distributed Denial-of-Service: Valid Campaign Tactic or Terrorist Act?" 2.

are directly analogous to the type of demonstrations that take place across the world. One or two people do not make a valid demonstration – 100,000 people do."[421]

The electrohippies view the Internet as a public space rather than a private space, which eliminates arguments of "virtual trespassing." If the website is publicly accessible and a large group of people wish to hinder the website's ability to disseminate information, the electrohippies claim that they have a right to enter the website repeatedly. The result is similar to having a large group of people filter in and out of a particular public building repeatedly to hinder traffic into the building. The electrohippies are correct that this is a large group of people assembling. It may be a virtual presence rather than a physical presence but this does not make the presence any less recognizable or identifiable. The electrohippies argue that the strategies of the digital world and the strategies of the physical world are equally valid, and this is demonstrated in the means of electronic protest. They borrow strategies that have worked in the past (sit ins, demonstrations) and adapt them to the digital world—only the location has changed.

CDC dismisses the core assumption that there is little difference between cyberspace and physical space: "Where a large physical mass is the currency of protest on the street, or at the ballot box, it is an irrelevancy on the Internet. Or more correctly, it is not always necessary. . . . But to think that it takes a lot of people to execute an act of civil disobedience on the Internet is naive. Programs make a difference, not people."[422] If this is the case, then from what source does the CDC claim any form of legitimacy for

---

[421] Ibid., 5.
[422] Ruffin, "Hacktivismo."

action? From a legal standpoint, Lessig argues against the idea of a system of cyberlaw that is separate from law in the physical world because "the effects of that place [cyberspace] will never be far removed from this ["real life"]. And our understanding of what that place will become is just beginning. We, here, in this world, will keep a control on the development there. As well we should."[423] The physical world and the digital world may not be the same, but they are certainly connected.

CDC argues that programs are what matter in cyberspace, and both the electrohippies and Cult of the Dead Cow have written programs for use in protest activities. But the split between programs and people is problematic because programs are written by people who instill in them certain values:

> Engineers write the code; the code defines the architecture, and the architectures define what is possible within a certain social space. No process of democracy defines this social space, save if the market is a process of democracy. This might not be so bad, assuming that there are enough places to choose from, and given that it is cyberspace, the places to choose from could be many, and the costs of exit are quite low. Even so, note the trend: the progression away from democratic control. We will stand in relation to these places as we stand in relation to the commodities of the market: one more place of unending choice; but one less place where we, collectively, have a role in constructing the choices that we have.[424]

Lessig argues that "code is an efficient means of regulation. But its perfection makes it something different. One obeys these laws as code not because one should; one

---

[423] Lessig, "The Zones of Cyberspace," 1403.
[424] Ibid., 1410.

obeys these laws as code because one can do nothing else. There is no choice about whether to yield to the demand for a password; one complies if one wants to enter the system. In the well implemented system, there is no civil disobedience. Law as code is a start to the perfect technology of justice."[425] Even so, Lessig allows for a different kind of civil disobedience by hackers: "Hackers define for themselves a certain anarchy, by devoting themselves to finding the holes in the existing code. Some believe that the complexity of the code means these holes will always exist, and hence this anarchy will always exist. But I don't think one need believe hacking impossible to believe it will become less and less significant. People escaped from concentration camps, but that hardly undermines the significance of the evil in concentration camps."[426] It seems that both Lessig and CDC are basing their beliefs on one important assumption—that the code will become more and more perfect. But as systems become more complex and more programs become available, the security holes will increase rather than decrease and that contrary to CDC's assertion that programs are really what matter, people are really what matter. It is not just operating systems, programs, and open ports on a machine that are vulnerable to hackers—people are also vulnerable.

Lessig compares the battle against code to the desire to escape concentration camps and seems to believe that as code becomes more and more difficult to break, the number of hackers trying to break it will decrease. Lessig reinforces the misconception that hackers are opportunists (and to an extent they are, which is why social engineering is such a powerful tool) and that once it becomes difficult, the number of hackers will

---

[425] Ibid., 1408.
[426] See Ibid., 18n.

decrease. While this may be true of script kiddies, those who would define themselves as "true hackers," or those who create the exploits that the script kiddies use, would still be motivated to break the code. It is not simply a utilitarian need for the information that resides on a particular system, but rather a desire to unlock the puzzle, although there are also hacking acts of self-preservation or revenge.[427]

One should not have to choose between people and programs; rather, one should take full advantage of both. This argument between the electrohippies and the CDC illuminates some of the basic issues surrounding the ethics of hacktivism. The disagreement also illustrates how two groups with similar aims (social justice) can disagree on the means to that end. Because each considers their respective stances to be axiomatic truths—CDC argues that denial of service attacks violate First Amendment rights and the electrohippies believe that the more people involved, the more democratic—the electrohippies and the CDC seem to be talking past each other.

Despite core epistemological differences, both parties have valid concerns. However, each group has flaws in their arguments. Does one take for granted that the First Amendment is always good? Is this an appeal to the amendment itself or an appeal to the idea that free speech is an inalienable human right? To whom does such a right of free speech belong—to citizens, corporations, political parties? The courts have ruled that commercial speech is not protected by the First Amendment. Although there is the problematic nature of corporations being granted some of the rights of citizens, they do

---

[427] For some examples of these acts of self preservation or revenge, see Martin Sprouse, *Sabotage in the American Workplace: Anecdotes of Dissatisfaction, Mischief, and Revenge* (San Francisco: Pressure Drop Press, 1992).

not have the same protection under the law as a citizen.[428] Thus, the argument that CDC makes about suppressing a company's First Amendment right is problematic and misguided. Especially if upholding the website owner's freedom of speech by squelching the hacktivists denies the hacktivists' equally valid (in terms of the First Amendment) right to peaceably assemble.[429] The electrohippies seem to believe that if you have thousands of people on your side, you also have justice on your side. Although numbers do grant a sense of legitimacy, despite CDC's claims, the amount of people it takes to shut down a website is a very small percentage of the population. Even if one takes the electrohippies' assertion that around 450,000 people took part in the action against the WTO (believing for the moment that these were separate individuals, which would be difficult to verify) at face value, with a world population of approximately six billion people it would mean that roughly 0.0075% of the world's population participated. This is hardly a democratic majority.

What we see in the disagreement between the electrohippies and the CDC is a continuation of familiar arguments concerning protest rhetoric: Do the ends justify the means? What is the difference between terrorism and activism? Where does one draw the moral and ethical lines for protest behavior? Are extralegal means of protest still ethical?

---

[428] For more on the idea of corporate personhood, see Aljalian, "Fourteenth Amendment Personhood: Fact or Fiction?"; Edwards and Valencia, "Corporate Personhood and the 'Right' to Harm the Environment"; Manning, "Corporate Responsibility and Corporate Personhood"; Rafalko, "Corporate Punishment: A Proposal"; Wilson, "Corporations, Minors, and Other Innocents - a Reply from R. E. Ewin." The notion of corporate personhood is problematic in the sense that corporations enjoy many rights of citizens, yet also receive special protections not offered to individuals.

[429] Many people think of the First Amendment only in terms of freedom of speech, but the entire amendment packs many ideas into 45 words: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."

These questions are important, and the answers to each one by different groups are bound to differ, depending on the fundamental assumptions of each group. If an organization has a fundamental assumption, for example, that the legal system is irreparably corrupt and broken, they may be more likely to resort to extralegal means of protest rather than working for change through the legal system.

One fundamental assumption of the electrohippies is that they are not simply silencing the WTO—they are opening a space in which other voices can be heard that are overshadowed when the WTO is granted the opportunity to continually speak. In considering the restriction of protest activities in residential neighborhoods, Haiman asks, "The question, I think, is what price a society is willing to pay to insure that the messages of minority groups are not screened out of the consciences of those to whom they are addressed. For once the principle is invoked that listeners may be granted some immunity from messages they think they would rather not hear, or which cause them annoyance, a Pandora's box of circumstances is opened in which the right of free speech could be effectively nullified."[430] Similar arguments can be made concerning the WTO protests. Hacktivists can easily post web pages arguing against WTO policies, just as one Black person could have easily marched in his or her own neighborhood during the civil rights era. But if the point of the march is to take the message *en masse* to those who the protestors believed needed to hear it, single marchers in their own neighborhoods would be ineffective. Silencing the WTO's digital voice drew attention to those who had not been heard by the supporters of the WTO and their policies. The CDC would argue that

---

[430] Haiman, "The Rhetoric of the Streets: Some Legal and Ethical Considerations," 106.

this is still wrong, but what other option do the electrohippies have in order to place their message on a relatively level playing field with the WTO which has the backing of the establishment? Dean Barnlund and Franklyn Haiman explain, "When one person or a few people in a group or society possess all the guns, muscles, or money, and the others are relatively weak and helpless, optimum conditions do not exist for discussion, mutual influence, and democracy. Discussion in such circumstances occurs only at the sufferance of the powerful; and generous as these persons may sometimes be, they are not likely voluntarily to abdicate their power when vital interests are at stake."[431]

One ethical consideration concerning hacktivism has to do with its lack of permanence. Unlike the physical world, the medium of the Internet is a constantly shifting, evolving space. If one burns down a building in the physical world as a means of protest, that building must be painstakingly rebuilt at a significant cost. If a web site is defaced, it can often be fixed quickly. Unlike spray paint, which must be cleaned off using a solvent, a defaced web page can simply be replaced with the original version and uploaded again. In other words, hackers are not defacing property so much as they are defacing a *presentation of self.* No *physical* property has been damaged. Even if the target of hacktivism argues that intellectual property was damaged, such property may also still be possessed, unharmed, by the owner. The digital nature of that which is damaged in hacktivism creates problems when attempting to quantify the damages to the organization that has been defaced. In the physical world, there are usually physical damages that go along with "pain and suffering," but even pain and suffering are rooted in the physical

---

[431] Dean C. Barnlund and Franklyn Saul Haiman, *The Dynamics of Discussion* (Boston: Houghton Mifflin, 1960), 12.

domain. How does one compensate for a brief loss of image? Most hackers do not attempt to represent the organization, although this does sometimes happen. Hackers generally seem to want the defacement to be obvious so it is unlikely that visitors to the defaced site will mistake the defaced site for an authentic version of the website. Even denial of service attacks are generally only temporary—it takes significant resources to launch such an attack, thus a sustained effort is difficult to maintain. Any attack that takes place in the digital domain will be temporary at best. When considering the ethics of hacktivism, this fact must be taken in to account—the destruction of a virtual presence is not equal to the destruction of a physical presence.

Limitations of Traditional Protest Activity

Online activism, or hacktivism, overcomes many of the obstacles found in traditional activism and protests. Schwartau writes, "Thirty years ago, a demonstration or protest required organization and the congregation of huge numbers of people, all within the limits of the necessary police permit. Signs and slogans and chants prefaced the occasional Mayor Dalylike headline-grabbing overreactions. Today, the netherworld of cyberspace offers an unrestricted, unregulated and certainly unorganized refuge as an alternative to conventional assembly. Cyberspace provides the ideal mechanism for cyber-civil disobedience, the protest means of choice for the Information Age."[432] But is cyber-civil disobedience really the protest means of choice for the Information Age?

---

[432] Schwartau, *Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Destruction*, 70.

Traditional means of protest seem to be alive and well. Marches in Washington D.C. are still common. Letter writing campaigns are also in heavy use. Lobbyists still wield significant power. It seems that there is still a considerable amount of protest activity outside of the digital realm.

Despite the current prevalence of protest activity in the physical world, McKenzie argues that "as the site of power moves from physical locations into digital networks and as universal knowledge gives way to situated knowledges, new forms of resistance also emerge. Long-entrenched practices of political activism—street protests, strikes, sit-ins, boycotts—are becoming less and less effective and in their place have arisen practices of 'electronic civil disobedience' and 'hacktivism.'"[433] Physical demonstrations of protest are often covered in the media, but this attention does not seem to have had much effect. McKenzie's indictment of these modes of protest and his argument that they seem to have lost any effectiveness as a mode of social change that they had previously possessed, seems justified. This may be partially because of laws that limit the ability to assemble. Permits must be obtained, police dressed in riot gear may shoot rubber bullets and tear gas into the crowd, and protesters may be arrested.

Although McKenzie suggests that electronic civil disobedience and hacktivism will take the place of physical forms of protest, Wray explains that the future will build on the past: "As hackers become politicized and as activists become computerized, we are going to see an increase in the number of cyber-activists who engage in what will become more widely known as Electronic Civil Disobedience. The same principals of

---

[433] John McKenzie "!Nt3rh4ckt!V!Ty," *Style* 33, no. 2 (1999): para. 32.

traditional civil disobedience, like trespass and blockage, will still be applied, but more and more these acts will take place in electronic or digital form. The primary site for Electronic Civil Disobedience will be in cyberspace."[434] Protests and civil disobedience may look very familiar in the digital realm. The digital world allows citizens to engage in "real world" activities such as letter writing campaigns and speaking out in public fora as well as digital activism. This blending of the digital and physical endows cyberspace with great potential for political activism. Jan Fernback states that "the public arena of cyberspace allows us to break our public silence." [435] This is possible partly because cyberspace does not *feel* like a public space. Diane Nelson argues that "cyberspace is a utopia in two senses. Many proponents excitedly proclaim that you can be anything you want to be there; it promises unlimited information and communication—the ultimate public sphere. . . . However, it is a utopia as well in the etymological sense of a no-place."[436]

Hacktivism is inviting is because it takes place in this "no-place" where time and space are malleable; activism is no longer relegated to where and when one happens to be. Kovacich writes, "The hackers of the world are using the Internet to communicate and attack systems on a global scale. Much of the attacks are aimed at totalitarian governments, government agencies, political parties, against the slaughter of animals for their fur, all of which can be considered politically-motivated attacks. These are the worst

---

[434] Wray, "On Electronic Civil Disobedience," 108.
[435] Fernback, "The Individual within the Collective: Virtual Ideology and the Realization of Collective Principles," 37.
[436] Nelson, "Maya Hackers and the Cyberspatialized Nation-State: Modernity, Ethnostalgia, and a Lizard Queen in Guatemala," 296.

kind and most feared by nation-states. The mounted attacks by global hackers, based on a 'call to arms' by hackers, against the government of Indonesia's Web sites is an example of what they can do and more importantly what is yet to come."[437] As the world becomes more globalized, protest activities also become more globalized because the effects of organizations and legislation may be experienced beyond national borders. Moreover, because there is no longer a need to assemble, the risks inherent in assembly are dissipated as well. One need no longer risk bodily harm by engaging in protest activity. Law enforcement officials are highly skilled in crowd control, but in the virtual domain, the playing field is slanted toward the activists. Thomas points out that a virtual presence can be a powerful tool when considering the legal implications of one's actions: "The virtual presence of the hacker is not enough to constitute a crime—what is always needed is a body, a real body, a live body."[438]

Perhaps the core way that hacktivism overcomes limitations of traditional protest is by its ease—not necessarily in action, but in automation. Hacktivism can overcome temporal barriers as well as spatial ones. Bakardjieva writes: "[The world of policy and mass media] have been experienced as a separate sphere of practice to which ordinary people have had no access in terms of their everyday action. They have not been able to afford to 'leave what you are doing now and go' . . . The handiness of the Internet access to these institutions—from amid everyday life—now generates the feeling that they are within 'attainable reach,' that people, as citizens, can actually perform action onto them, that they are part of the subjective everyday lifeworld and not a detached 'province of

---

[437] Kovacich, "Hackers: Freedom Fighters of the 21st Century," 575.
[438] Thomas, *Hacker Culture*, 182.

reality.' Thus 'easy' may actually mean 'it is now possible for me to act politically from where I stand.'"[439] One need not be technically skilled to be a hacktivist. One need only have a computer and an Internet connection. But Bakardjieva's idea that people are now able to act politically through the medium of the Internet is problematic because for many the entry costs are still too high. To participate in a traditional march, one need only have the time and the ability to walk at the specified location. However, if one has the access, but not the time, hacktivism is a way that people can feel involved without disrupting their daily lives. In this way, hacktivism enables the would-be activist to make his or her actions invisible, perceptible only by examining his or her Internet traffic patterns or noticeable as only one of many incoming requests to a particular server. Through hacktivism, activists can outsource their political activity to the computer.

Hacktivism Versus Culture Jamming

According to Christine Harold, culture jamming "seeks to undermine the marketing rhetoric of multinational corporations, specifically through such practices as media hoaxing, corporate sabotage, billboard 'liberation,' and trademark infringement. Ad parodies, popularized through magazines such as *Adbusters* and *Stay Free!* and countless websites, are by far the most prevalent of culture jamming strategies."[440] Hacktivism techniques such as website defacement may seem like another form of culture jamming but there are aspects of hacktivism that distinguish it from the practice

---

[439] Bakardjieva, *Internet Society: The Internet in Everyday Life*, 127.

[440] Christine Harold, "Pranking Rhetoric: 'Culture Jamming' as Media Activism," *Critical Studies in Media Communication* 21, no. 3 (2004): 190.

of culture jamming: hacktivism does not rely on parody or trope, hacktivism need not conform to social norms, and hacktivism generally seeks to make the argument explicit rather than implicit.

Although hacktivism may incorporate aspects of parody, this is not a necessary component. For culture jamming, this is often a necessary component in order to escape litigation. Parody is one of the few protections for those who engage in copyright and trademark infringement.[441] Hacktivists recognize that what they are doing is against the law—if one is going to illegally enter a computer system, why worry about lesser laws such as trademark infringement?

Culture jamming seems to depend more on established social norms, hence the idea of interfering with those norms. However, those norms must simultaneously be subterranean in the collective conscience of society while close enough to the surface that when culture jamming calls attention to these norms, they are recognizable. In order for culture jamming to operate, it must still, to some extent, play by the rules of the culture. This is in part because culture jamming is often dependent upon society for its very expression. For example, *Adbusters* is relevant only so long as individuals are willing to pay $35 per year for the privilege of reading it. It is unlikely that *Adbusters* will publish their magazine and distribute it free of charge. However, if they push the envelope too far to the point of offending those who support it, support wanes and *Adbusters* must make decisions as to whether they can continue as a going concern. In some instances, artists

---

[441] But this is still by no means complete protection. One prominent culture jamming band, Negativland has had many legal battles because of their samples. See Francis Gary Powers, *Fair Use: The Story of the Letter U and the Numeral 2* (Concord, CA: Seeland, 1995).

and cultural activists use institutionalized funding to make a statement, as in the case of an electronic billboard art installation overlooking Times Square that focused on the "alienating" price of advertising which was funded by the Public Art Fund.[442] But institutionalized outlets must protect themselves. Messages deemed to be too incendiary or otherwise dangerous are unlikely to find support and art that transgresses social norms too much is likely to be attacked.[443] Those who cannot find public support will likely be relegated to the fringes.

Hacktivism need not recognize or conform to social norms and can potentially act independent of such constraints. Hackers are able to bypass institutionalized means of acquiring access to the mass media. Because they answer to no institution and are able to disseminate messages anonymously, hackers are free to transgress social boundaries and taboos. Although this is not explicitly discussed in the extant literature, one major reason for the rise of hacktivism is the difficulty in gaining access to existing mass media systems. A. J. Liebling remarked, "Freedom of the press is guaranteed only to those who own one." Few people with dissenting voices have access to an electronic billboard in Times Square. For hacktivists, the Internet is an available means to gain an audience for their cause and it is a medium that hackers understand and can control. It is much more difficult to break into a television show or a radio station than it is to break into a website.

---

[442] See Anne Bray, "The Community Is Watching, and Replying: Art in Public Places and Spaces," *Leonardo* 35, no. 1 (2002): 17.

[443] For example, Robert Mapplethorpe's homoerotic and sadomasochistic themed photography were used as examples of what was "wrong" with the National Endowment for the Arts (NEA) by some members of Congress and offered as one reason to shut down the NEA. See Linda Greenhouse, "Justices Uphold Decency Test in Awarding Arts Grants, Backing Subjective Judgments," *New York Times*, June 26, 1998.

Perhaps another reason for the timidity of culture jammers is that culture jammers are trespassers on the media of their choice. This is not the case in hacktivism. Hackers created and have shaped the Internet; this is their home. With the rapid commercialization of the Internet, the Internet is moving from an "information superhighway" to a worldwide shopping mall and hackers often view this encroachment as trespassing on their territory—as The Mentor put it, "this is our world now."[444] This sense of ownership on the part of the hacktivists may allow a greater sense of boldness not only in the means of attack, but also in the argument itself. While culture jamming seems to operate implicitly, hacktivists tend to make the argument explicit. Culture jamming works because it plays on people's subconscious, working enthymematically. Hacktivism, following the clear rules of code, works by making all of the premises explicit. Where culture jamming is a subtle nudge to realization, hacktivism is a blow to the head with a tire iron.

Tiziana Terranova argues that "political intervention in an informational milieu . . . involves more than the production of counterinformation but also an engagement with the dynamics of information diffusion as such (opening up channels, selective targeting, making transversal connections, using informational guerrilla tactics)."[445] It seems that hacktivism fits this well. Although some scholars seem to consider hacking to be a form of culture jamming, there remain significant differences in how they operate rhetorically.[446] Culture jamming is intentionally vague, allowing the viewer to reach his

---

[444] Mentor, "The Conscience of a Hacker."
[445] Terranova, "Communication Beyond Meaning: On the Cultural Politics of Information," 54.
[446] See Harold, "Pranking Rhetoric: 'Culture Jamming' as Media Activism," 206.

or her own conclusions. Hacktivism does not allow this potential, making all points of the argument explicit such that there is no room for interpretation other than agreement or disagreement. Although enthymematic reasoning can be a powerful persuasion technique, there are occasions in which the issues are too nebulous, too difficult to parse, that invite a more direct approach, which is one of the strengths of hacktivism. Hacktivism and culture jamming are distinct rhetorical strategies with separate strengths.

Hacktivism seems to be a two edged sword. There are ethical dilemmas concerning the silencing of other voices, but there is also the increased possibility for more individuals to engage in activism in previously impossible ways. Hacktivism takes advantage of the networked society in ways that traditional means of protest cannot. However, these hacktions cannot stand alone—they are best understood within the context of movements and actions that take place in the physical world. We are far from the science fiction fantasy of leaving the body behind as our minds traverse the vast expanse of cyberspace. Thus, we cannot completely abandon the physical world and the material considerations with which most social movements are concerned.

Case Study: The New York Times Hack

Erving Goffman states that for each role, there is a self-image, and that "a self, then, virtually awaits the individual entering a position; he need only conform to the pressures on him and he will find a *me* ready-made for him.[447] The rituals and norms of

---

[447] Erving Goffman, *Encounters: Two Studies in the Sociology of Interaction* (Indianapolis: Bobbs-Merrill, 1961), 87-88.

hacking help to define what that ready-made individual does, and thus *is*. By examining the rituals of hacking, we may begin to understand more about the nature of the ideal hacker.

On Sunday, September 13, 1998, the *New York Times* website was hacked by a group of hackers called HFG, or H4ck1ng for Girl13s (Hacking for Girlies). The hack was a response to a July 4, 1994, news article by John Markoff that appeared on page one of the *New York Times*.[448] Markoff's article portrayed Kevin Mitnick, a hacker, as a danger to society. A common complaint within the hacker community is that Markoff has profited from the arrest of Mitnick, first writing *Cyberpunk,* which featured Mitnick, then writing another book, *Takedown,* about Mitnick's arrest which was, at the time, being converted into a screenplay.

It is odd that hackers waited so long to attack the site. Perhaps the hack served as a reminder to the *New York Times* that the hacker community had not forgotten the role of the *Times* in capturing Mitnick.[449] Mitnick stated that Markoff was the main reason that he was still in custody: "Markoff has single-handedly created 'The Myth of Kevin Mitnick,' which everyone is using to advance their own agendas. I wasn't a hacker for the publicity. I never hacked for personal gain. If I was some unknown hacker, accused of copying programs from cell phone companies, I wouldn't be here. Markoff's printing false and defamatory material about me on the front page of *The New York Times* had a substantial effect on my case and reputation. He's the main reason I'm still in

---

[448] See Markoff, "Cyberspace's Most Wanted: Hacker Eludes F.B.I. Pursuit."

[449] It is interesting that Mitnick did not condone the hacking of the New York Times. See Adam L. Penenberg, "Mitnick Speaks!" Forbes.com, April 5, 1999, http://www.forbes.com/1999/04/05/feat.html (accessed April 29, 2003).

custody."[450] On one hand, there is a hacker who, in the eyes of the law, is a criminal. On the other hand, there is an overzealous, potentially unethical journalist, who, if libelous, is also a criminal in the eyes of the law. This chain of events set the stage for the hacking of the *New York Times.*

The timing for the hack was well thought out; Kenneth Starr had just published his report to Congress concerning President Bill Clinton and Monica Lewinski. Traffic to the site was higher than normal, although Nancy Nielsen, a spokeswoman for the *New York Times*, explains that Sunday morning, which is when the hack took place, is traditionally slow.[451] Comments within the text of the hack illustrate that HGF recognized the significance of the timing: "HFG 1Z N0W G0ING INT0 THE C1GAR BUS1NESS T00. W3 W1LL S3LL 0UR 0WN L1N3 0F DES1GN0R C1GARS, START1NG W1TH THE 'L3W1NSKY C1GAR'. 1T HAS A FAIRLY D1STINCT TAST3. (AND W3 TH0UGHT *W3* W3R3 K1NKY!)"[452]

What first draws the eye of the viewer is the suggestive logo shown in Figure 1. Although pornography and hacker culture seem to intersect (links to pornographic websites are common on warez sites and some hacker sites), it is less common to find pornographic imagery on hacked web pages. Even so, this imagery is far from extreme.

---

[450] Ibid., para. 15.

[451] Arik Hesseldahl, "All the News That's Fit to Hack," *Wired News*, September 14, 1998, http://www .wired.com/news/politics/0,1283,14990,00.html (accessed April 29, 2003).

[452] Hacking For Girliez. September 13, 1998. "HFG Owns Mah Dumb Azz." *2600*, http://www.2600.com/ hackedphiles/nytimes/hacked/ (accessed February 3, 2006). To view the code on a windows machine, right click and select "view source." In this analysis, I quote the text exactly as it appears on the hacked page. For the code, I remove the HTML tags, but the text is unaltered. Spelling and grammatical errors have been preserved.

In fact, what makes this particular instance interesting is its subtlety. HFG included a more explicit tie to pornography at the bottom of the web page. Figure 2, "HFG Certified!" is more blatant with its depiction of a woman's breasts; it is also a link to http://www.persiankitty.com/, a pornography site.

Figure 1: Hacking For Girliez Logo

Figure 2: HFG Certified! Logo

Some hackers use pornographic imagery as commentary much as political cartoonists sometimes tread into grey areas of decency as a means to jolt the reader into thought. For example, in 1996, a hack of the Air Force website included an animated GIF (image) of three people engaged in sexual activity and the caption "This Is What your gov't is doing to you everyday."[453] However, it seems that in the case of HFG the links to pornography and the suggestive imagery is self-referential rather than functioning as shock value or commentary. Perhaps this is because for hackers it is not necessary; the Internet is full of pornographic images and when imagery becomes commonplace, it ceases to have shock value. The *New York Times* description of the imagery as "nude women" and "offensive" stands in contrast to a news article earlier that year describing Robert Mapplethorpe's

[453] See *2600*, "The Air Force: Hacked Webpage," December 29, 1996, http://www.2600.com/hackedphiles/airforce/hacked_af/www_af_mil.html (accessed February 3, 2006).

work as merely "sexually explicit."[454] "Sexually suggestive" would be a better way to describe the HFG imagery. The *New York Times* paints the hack in the most drastic possible terms, knowing that a large portion of the population had probably not seen the actual hacked page. What was likely meant to be suggestive was painted by the *New York Times* as extreme.

One particular hacking ritual that is immediately evident is the use of "leet-speak," a stylized version of English that replaces certain letters with numbers and contains its own spelling rules and slang elements. For example, there is prominent use of the term "own." To own a box means to have complete control of another's server. Placing the cursor over the logo reveals alt text which states, "HFG OWNS". The title of the page has been changed to read, "HFG OWNS MAH DUMB AZZ," and the text beneath the logo proclaims, "F1RST 0FF, WE HAVE T0 SAY.. WE 0WN YER DUMB ASS. 4ND R3MEMB3R, DUMB ASS 1S OFT3N CUTE 4SS. AND WE L1KE CUTE ASS." Although it is readable, the use of jargon and leet can be used to maintain in/out group boundaries. HFG demonstrates an awareness of these boundaries within the code of the page.

Joseph Hermanowicz and Harriet Morgan state that "whether they promote acceptance of a group's values among group members, outsiders, or both, rituals are prescriptive. For group members, they reward group identification. In some cases, such as

---

[454] Greenhouse, "Justices Uphold Decency Test in Awarding Arts Grants, Backing Subjective Judgments." I am not arguing that Mapplethorpe's work is not sexually explicit, only that the *New York Times* is minimizing the reasons why conservatives in Congress used Mapplethorpe's work as a reason to limit funding for the National Endowment of the Arts. For example, one of Mapplethorpe's self portraits depicts him with a bullwhip protruding from his anus and another photograph portrays a man urinating into another man's mouth. It seems that the status Mapplethorpe has as an artist legitimates the work while HFG enjoys no such protection.

shaming rituals, they sanction deviants and warn potential deviants, protecting an identity."[455] One such ritual can be found in the greets and ridicules section of the text. This is where hackers publicly acknowledge or criticize one another. Some prominent greets include Kevin Mitnick (three times), themselves (seven times), and *Phrack*, a hacker magazine. Those ridiculed include several other hackers or hacker collectives and "other lamers." Despite the venom unleashed at Markoff in the text of the site, his name is not mentioned in the ridicule segment. "Affirmation," according to Hermanowicz and Morgan, "tends to highlight group boundaries. While customary practice may entail some relations with the profane, affirmation reasserts its sacred aspects. Although outsiders may be able to observe ritual events, participation is predominantly internal."[456] Shaming rituals also delineate group boundaries, which explains the absence of both Markoff and Carolyn Meinel, another target in the hack, from the ridicule segment. Although the hack specifically targets these two individuals, they are not hackers in the eyes of HFG (despite Meinel's assertion to the contrary that she is a hacker, albeit an ethical hacker)—to include them in the ridicule section would symbolically bring them into the collective, affording them "equal" status with other hackers. For Meinel, this is a particularly blatant snub.

---

[455] Joseph C. Hermanowicz and Harriet P. Morgan, "Ritualizing the Routine: Collective Identity Affirmation," *Sociological Forum* 14, no. 2 (1999): 199.
[456] Ibid., 210.

Links are another website defacement ritual. The first link listed states “Free Kevin Mitnick Ya Dumb Whorez!” which is a link to www.kevinmitnick.com. Other links include: the Church of Scientology, with the title, “Fight These Criminals”; a link to www.hackerz.com that reads, “If You Can’t Afford Our Seminar”; and a link to www.l0pht.com with the title, “These Guys Rool.” L0pht is well respected among hackers because of their skills, even though they fall into the category of “white hat” hackers while HFG self identifies as “grey hat” hackers. In the world of hacking, skills remain a common currency regardless of which side of the fence the hacker stands on. In the code, there is only one comment about the links: “L0PHT <HEARTS> HFG.” This is a bit mysterious because it implies that l0pht supports the efforts of HFG despite the fact that l0pht are avowed white hat hackers who would not publicly admit to illegal hacking activity. This is likely to remain a subject of speculation until the members of HFG are identified. Two other links that are a bit more subtle are embedded in images, shown here. The image depicted in Figure 3 is a link to *Phrack* and has the alt text “VI ROOLZ.” There are no comments explaining what is meant, but perhaps they are referring to the VI UNIX text editor. The other image, shown in Figure 4, has alt text that reads “HFG NOW” and links to www.hfg.org, or the Harry Frank Guggenheim Foundation. Here we see a humorous play on how acronyms can misrepresent an organization because of similarity. The Internet has had many such occurrences of mistaken identity. One such case is with the domain “whitehouse.” The URL www.whitehouse.gov takes the viewer to the United States White House site;

Figure 3: Best Viewed with VI

Figure 4: Get Hacked Now! HFG

www.whitehouse.org takes the viewer to a satirical website, which has links for categories such as “Department of Faith” and “Fraternal Affairs”; www.whitehouse.com currently contains only Google ads, but until 2004 it was an online pornographic website that had parodies of the President and featured an “Intern of the Month.”[457]

On the surface, HFG maintains common conventions of website defacement (use of leet-speak, ridicules and greets), but viewing the source code exposes the reader to an entirely different message than that displayed on the web page. By inserting an HTML comment tag (coded as <!-- comment text -->) HFG inserted comments that are invisible to the casual viewer. HFG displays a keen awareness of the ability of code to create and maintain boundaries between those with the technical understanding to read the code and those without this technical skill who will remain on the surface of the page. The HFG hack had two audiences—the public and the private—or, to use Goffman’s terminology, the front stage and the back stage.[458] HFG tries to blend these two audiences by inviting those in the front stage to come backstage. In the portion of their message directed at Markoff, they write, “(R3AD THE HTML C0MM3NTS IF YOU CAN’T GU3SS WH0 THAT 1Z M0R0N),” and toward the end of the page, they write, “PS: 0UR C0MMENTS ARE M0RE ‘LEET THAN 0UR TEXT. DOWNLOAD THE SOURCE T0 TH1S PAGE AND P0NDER 0UR W1ZD0M.” These are clear invitations to delve beneath the surface of the page to see what lies beneath. However, this requires some technical knowledge on

---

[457] The pornographic website whitehouse.com was not a web presence for the British pornographic magazine “Whitehouse.” This was a common misconception. The British magazine was not intended to be a parody of the United States White House, but rather named in opposition to U.K. anti-pornography crusader Mary Whitehouse.

[458] Erving Goffman, *The Presentation of Self in Everyday Life* (Garden City, NY: Doubleday, 1959).

the part of the reader; the reader must first recognize that he or she is being invited to examine the code of the page and, second, know how to view the source code. Because of these constraints, the code was probably ignored by many who viewed the website. HFG recognized that this would be the case, stating in the comments, “You foolish windows chumps probably will never see any of the real meaning of this page. Your loss.” For the general public this invitation amounts to little more than a taunt.

By using code to maintain group boundaries, HFG is able to create two personas that stand in stark contrast to each other. In the public face they portray a juvenile, less serious persona. In the comments HFG is considerably more articulate, dropping the leet speak altogether and citing such literary greats as John Milton and Voltaire. The hidden side of HFG is also much more logical and sharper in their criticism of Markoff and of Carolyn Meinel, who was supposedly writing a book about their exploits. Here is an example of the differences in these presentations:

> TH1S T1ME, CAR0LYN M3INEL ASKED US TO HIT A B1GG3R AND M0RE TRAFFICKED SIT3. SH3 T0LD US TH3 0THER DAY THAT SH3 1Z ALM0ST D0N3 W1TH THE B00K. 1TZ AMAZ1NG H0W SH3 SP1NS TH1NGZ AR0UND. H3R3 W3 TH0UGHT SH3 W0ULD G3T MAD AT US F0R BR3AK1NG 0UR AGR33M3NT, BUT SH3 SA1D “D0N’T W0RRY HFG, N0 0N3 W1LL BEL1EVE YOU S1NCE Y0U AR3 BLACKHAT HACK3RS. B3SID3Z, TH1S ADDS M0RE MYST3RY AND SUSP3NCE F0R ME. C0NTR0V3RSY SELLZ!”. 0K. 1F Y0U S4Y S0.

Here is what is written directly beneath this portion of the text in the comments:

> Truth be known, she is writing a chapter about us in her second book. She has contacted HFG on numerous occasions asking us if we could show our 'hacking prowess' (her words) so that she may cover it exclusively in her book. She offered us 10% of the book earnings and we agreed. Since she doesn't know how to read these comments using her Internet Explorer, we are giving her a slap in the face. Her goal all along has been to lead us on, watch us get busted, then write about us.. a la Markoff/Mitnick, Shimomoru/Mitnick, Quittner/MOD, Stoll/Hess.. see a pattern forming here? We sure do.

Wayne Booth explains that within a text, there exists an implied author.[459] In the public text there is the prominent use of leet speak, making the hacker appear simultaneously familiar and alien. The reader is invited to make an immediate distinction between himself or herself and HFG based on this difference. HFG creates a persona within the text that is irresponsible (breaking an agreement) but also dangerous (black hat hackers). Concerning the identification of black hat hackers, they subtly demonstrate the power of naming. Meinel described them as black hat hackers; HFG self-identifies as "grey-hat" hackers. Even so, despite HFG's self definition, because they have been labeled black hat, they have been silenced ("no one will believe you since you are blackhat hackers.")

HFG creates a persona that is unconcerned and unknowledgeable about financial gain and naïve concerning the ways of the world ("controversy sells! OK. If you say so.") As HFG depicts themselves as rubes that are being used by Meinel for her financial gain,

---

[459] Booth, *The Rhetoric of Fiction*, 71-77.

the reader is invited to view Meinel as unethical and opportunistic. This is reinforced elsewhere in the hack where they paint an image of the group as bored teenagers (describing Master Hacker's employment at Taco Bell and Arbys, explaining that they hacked the site because they were bored). Finally, HFG establishes a clear tie with Meinel (the mention of an agreement, "She told us the other day") and frame her as the mastermind of this and previous hacks ("This time, Carolyn Meinel asked us to hit a bigger and more trafficked site.")

In the comment section, or the backstage persona, HFG completely abandons leet speak. Under the veil of code, HFG is free to behave as they wish and speak clearly because outsiders are less likely to see the way they "really" are—they need no longer keep up a front. Goffman explains, "Just as it is useful for the performer to exclude persons from the audience who see him in another and inconsistent presentation, so also is it useful for the performer to exclude from the audience those before whom he performed in the past a show inconsistent with the current one."[460] HFG demonstrate faith in the ability of the code to exclude the masses, thus shielding them from the inconsistency of their performance in the public text.

In the code, they discard the naïve, immature persona and express an understanding of their peril. However, they still seem cavalier in the face of the Faustian deal that they have made with Meinel. They admit to agreeing to a deal that would garner them ten percent of Meinel's book earnings, yet understand that Meinel's goal is to gain the greater publicity afforded to those who have chronicled the capture of hackers. The

---

[460] Goffman, *The Presentation of Self in Everyday Life*, 137-138.

main impressions available to the reader of the comments are that HFG harbors self-destructive tendencies or that HFG has an almost hubristic belief in their ability to evade capture. This reinforces the belief held by many in the hacker community that "real hackers don't get caught."[461]

In the code, they differentiate hackers from security professionals by insulting Meinel further. It is unlikely that HFG truly believed that Meinel would not be able to examine the code; she is a computer security consultant who had already experienced attacks by hackers. The explicit reference to Microsoft Internet Explorer creates a kind of inside joke for the hacker community who recognizes the inherent security flaws in the Microsoft OS architecture, opting instead for the more powerful UNIX or the "peer reviewed" Linux. HFG, with their "slap in the face," explain that they are now on the offensive. Whether or not HFG is affiliated with Meinel in any way is open to debate, but Meinel was considered to be a suspect in the HFG case and was questioned by the Federal Bureau of Investigation (FBI).[462]

In response to the *New York Times* hack, Meinel *decreased* security on her website and suggested that HFG broke into the *New York Times* because they were unable to deface her website: "Normally when a hacker gang that has criminal tendencies is really mad, they express their feelings by hacking the website of the person who has given them a case of the mads. Unfortunately, hacking for Girlies has never figured out how to get into http://www.happyhacker.org. So instead they have put up their protests

---

[461] I base this assertion on discussions with hackers who wish to remain anonymous.

[462] Carolyn Meinel, "Happy Hacker Digest," *Happy Hacker*, January 4, 1999, http://happyhacker.org/hhlist/inside1_4.shtml (accessed February 6, 2006).

against me at two Motorola Web sites, the Jet Propulsion Lab, *Penthouse* classified ads, and finally, on Sunday, Sept. 13, 1998, they placed one of their tirades on the *New York Times* newspaper's Web site."[463] She concludes this line of reasoning with the assumption that HFG actually wants to break in to her website but are unable to do so: "If Hacking for Girlies breaks into any other web site to post their gripes against me, I swear I will hold a press conference and show the reporters how easy it is to break into the Happy Hacker Web site. This will make Hacking for Girlies look like lamers and losers."[464] Meinel seems to believe that HFG *wanted* to hack her site and ignores the disparity in traffic between her site and the *New York Times*. If www.happyhacker.org were to be hacked, no one would notice, but the *New York Times* hack was a newsworthy occasion.[465] Moreover, if one wishes to smear the name of another, it is more effective to do so where it will be read by the maximum number of people. For HFG to hack Meinel's site would have been the equivalent of sending a personalized letter stating their grievances; hacking the *New York Times* was like airing those grievances on the national nightly news. To break in to Meinel's site would be a waste of time. If HFG wanted to cause Meinel distress, hacking the *New York Times* and dropping her name was a more efficient way to do so.

---

[463] Carolyn Meinel, "Happy Hacker Digest," *Happy Hacker*, September 25, 1998, http://happyhacker.org/hhlist/digest49.shtml (accessed February 6 2006).

[464] Ibid.

[465] To illustrate the amount of website hacks that are not reported, in one day, February 6, 2006, by 1:30 p.m., Zone-h, a network security site that tracks website defacements, reported 1091 verified hacks, 362 of which were single IP defacements while 729 were mass defacements. In other words, it is highly unlikely that a hack on Meinel's low-profile site would have even been noticed, let alone discussed in newspapers all over the nation including the *New York Times*, as well as in scholarly and trade journals in the areas of computer security and journalism.

There is more to this insult, however, which illustrates a likely reason that Meinel was considered a suspect by the FBI. While the public side of the hack portrays Meinel as a Fagin-esque individual who taught others how to hack and then took advantage of simpleminded individuals by chronicling their exploits for her financial gain, the portrayal within the code is more sinister:

> Speaking of FBI.. did we forget to mention what Carolyn Meinel offered to do for us? If asked who we were, or if she had any knowledge of who we are, she offered to give misleading information to the FBI in order to help us continue our hacking spree. She assured us that she had plenty of other people to focus the FBI's attention on, and that they would "surely take the heat". The only qualifier to this arrangement, is that she get exclusive rights to our 'story'.

Meinel was willing to encourage criminal behavior and, according to HFG, she was willing to lie to the FBI about it, adding perjury to her list of faults. It was well known that she sold books teaching people how to hack. From HFG's perspective, Meinel planned to follow the road that John Markoff took to financial gain—that of participating in and documenting the arrest of hackers. That Meinel had appropriated the term "hacker" for herself was likely the most damning sin. If she ever had been a hacker, she was a traitor; if she was not a "real" hacker, she was a liar.

The most striking distinction between the public and private presentations of HFG appears within the code toward the end. Here, HFG completely cast off the notion that they are immature practical jokesters and demonstrate their ability to gain information by providing Meinel's name, address, phone numbers, social security number, and email addresses, as well as the social security number and email address of Winn Schwartau

(another prominent computer security writer) with the invitation to search for them "in your favorite database." This is a not so subtle reminder that with nine digits you can track down a considerable amount of information about someone and a chilling reminder of how easy it can be for someone to gain access to this information.

Perhaps the most important ritual that separates the hacker from the script kiddie is the revelation of the exploit used to hack the site and the message to the system administrator. In the public text, HFG leaves the cryptic message, "PPPPPS: W3 D1G Y0UR CR0NTABZ!" Alex Wellen writes, "According to some experts, 'CR0NTABZ' refers to a configuration file for the CRON program that runs in Unix and gives an administrator the ability to execute a program at scheduled intervals. For example, HFG might have penetrated the site's security (no simple task in itself) long enough to modify the configuration file. The modification could have instructed the server to replace the *Times* home page with the hacked page at some interval—say, every five minutes."[466] Although script kiddie hacks rarely go beyond posting a message along the lines of "35K470N 0Wn5 7H15 B0x!!!!!!!!," hacks that require skill rather than simply running a script will often have a message to the system administrator and a detailed explanation of how they gained access. This asserts the ethical code of hackers that requires them to share knowledge. There is also a sort of arrogance within this action. In the code, they state, "For everyone who calls us immature kids, it shows one more person has underestimated us. And worse, what does that say about their security? That 'immature kids' were able to bypass their 25,000 dollar firewalls, bypass the security put there by

---

[466] Alex Wellen, "Delving into the Source," *G4 Media, Inc.*, September 16, 1998 http://www.g4tv.com/techtvvault/features/4720/Delving_Into_the_Source.html (accessed January 23, 2006).

admins with XX years of experience or a XXX degree from some college. Nyah Nyah." They quote Voltaire beneath this passage: "The best is the enemy of the good." HFG are comfortable giving the system administrator the information concerning how they hacked the site because hackers recognize that there will always be another way in, another exploit. The hacker must be confident enough in his or her skills to willingly show the system administrator how to secure his or her box against similar exploits. It is not enough to be good—hackers must be the best.

There are two images of the hacker. The public persona invites the viewer to see a youthful, foolish, but still relatively harmless version of him or herself. This persona is naïve in the ways of the world, unconcerned with financial gain, and only acting out of boredom. The persona revealed in the code is almost the polar opposite to the public persona. HFG is educated, articulate, and cocky. They are able to access personal information about people through databases that even today remain a mystery to most people. The persona revealed in the code is a force to be reckoned with. That HFG only defaced the website demonstrates a considerable amount of restraint—it is likely that they could have done considerable damage had they so desired. But in addition to the implied authors, Edwin Black points out, rhetorical discourses also imply an ideal auditor, for whom the discourse is designed, and this implied auditor can often be linked to a particular ideology.[467] Who is the ideal auditor for these discourses, or how are these discourses designed to be received? The public discourse is meant for those who are not

[467] Black, "The Second Persona," 112.

hackers and the discourse found in the code is meant for those who are hackers, but within these discourses, HFG ascribes certain characteristics to these two audiences.

By portraying themselves as immature pranksters, HFG inspires a feeling of moral, intellectual and emotional superiority in the audience. The audience is invited to respond with something along the lines of "these kids today. . . ." HFG declares themselves to be terrorists, but do so in such a way that undercuts any effort to take the assertion seriously, demanding "104 girliez, 6 billion in newspaper subscriptions, and maybe a printing press or something." Moreover, they define themselves as "the grey hat Robin Hoods of hacking," who "feel up the rich and live for more!" They are not in this for financial gain, thus distancing themselves from common fears concerning hackers—identity theft, credit card fraud, and cyberterrorism. The audience is invited to experience HFG as teenage pranksters who have taken over the *New York Times* website to protest Kevin Mitnick's arrest by posting simplistic poetry and softcore pornographic imagery.

So long as HFG can induce the audience into believing that they are better than HFG, the audience will likely view hackers as a relatively harmless nuisance rather than a serious threat. Operation Sundevil, which took place in 1990, altered the landscape of the hacker movement. The hacker was now seen as a threat to everyone—hackers want to destroy phone systems, power grids, air traffic control systems, bank accounts, credit ratings, and access your computer to steal pictures of your children for dubious reasons. Anti-hacker propaganda helped support the law enforcement efforts against the hacker and helped justify the resources being expended on this target. Kovacich argues that with major crimes decreasing and funding to government law enforcement agencies also decreasing, these agencies must find new threats in order to remain relevant: "The new

mission? Hype the hacker threat and the FBI gets $30 plus million to go after the teenage hackers - at a time when the Chinese have stolen and continue to steal our nuclear secrets. At a time when the Russian bear is coming out of hibernation. At a time when real terrorists are gaining new weapons and attacking the interests of the free world in the old fashioned way - by blowing it up! Talk about misallocation of available resources!"[468]

HFG seems to recognize that assuming a militant posture would reinforce existing views of the hacker. Inviting the audience to view themselves as wiser and more mature than HFG minimizes the threat and allows the viewer to see a bit of themselves in HFG. HFG plays to the audience's memory—who has not done foolish things in his or her youth? These foibles of youth are often remembered in a positive light; youthful foolishness seems to be a kind of rite of passage in America, romanticized in books, magazines, television shows, and film. The audience is invited to remember their own youthful mischievousness and thus view themselves in HFG's shoes. Audience members are invited to view HFG as a younger, more foolish version of themselves, which they have, thankfully, outgrown.

Within the code, a different audience is implied—that of the true hacker. Black states that "the critic can see in the auditor implied by a discourse a model of what the rhetor would have his real auditor become. What the critic can find projected by the discourse is the image of a man, and though that man may never find actual embodiment, it is still a man that the image is of."[469] Who is this image? Here, we encounter a hypermasculine, xenophobic, sexual, and, while not necessarily malicious, decidedly less

---

[468] Kovacich, "Hackers: Freedom Fighters of the 21st Century," 575.
[469] Black, "The Second Persona," 113.

harmless person. In describing the process of secondary socialization into a group, Berger and Luckmann explain that a "body of meanings will be sustained by legitimations, ranging from simple maxims . . . to elaborate mythological constructions."[470] One of the maxims that can be distilled from this hack is "a hacker never gives up root." The issue of being "rooted" is mentioned in both the public and the private texts but to understand the issue, one must be acquainted with computer terminology. To gain root access means to have complete control of a machine. To be rooted is to be penetrated in the most complete sense. The hacker does not simply breach the security, the hacker completely "owns" the box.

Some scholars have argued that hacking is a form of sublimated sexuality.[471] Although hacking and computer terminology is tinged with eroticism (penetration, master/slave), the pleasure of hacking can also be compared to the pleasure of solving a difficult puzzle. Levy points out that many of the early hackers were also skilled lock pickers. This was done partly with utilitarian motives, but "the master key was more than a means to an end; it was a symbol of the hacker love of free access."[472] Even so, there may be some truth to the idea that hacking has sexual undertones. To not give up root is to never be penetrated even while the hacker is actively attempting to penetrate others—as many others as possible. To use the idea of hacking as sexuality, one must be honest in the use of this metaphor. Hacking is more akin to rape than it is to consensual sex and rape discourse provides some insight into this world. According to Sandesh Sivakumarin,

---

[470] Berger and Luckmann, *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*, 139.
[471] See Taylor, *Hackers: Crime in the Digital Sublime*, 36-42.
[472] Levy, *Hackers: Heroes of the Computer Revolution*, 103.

"The term 'emasculation' is also frequently used to describe the male victim of rape, the notion being that a male victim of rape has been stripped of his masculinity and has been made weak and effeminate."[473] In the text and the code of the hack, HFG reaffirm their masculinity. Early on in the code, HFG states, "Don't hate us because we nailed your girlfriend," which seems out of place because there is no context for the remark. Likewise, in the list of previous hacks that begins the code segment, next to the entry for classifieds.penthouse.com, they state, "Told you we hacked for girlies!" Statements of sexual conquest spill over into the poetry segment: "We busted root on their women and their suns / next thing you know, we'll be looking for nuns."[474] HFG denounces the hacking group H4G1S not as script kiddies or with an explanation for their lameness as they do with the other groups that they ridicule, but simply stating, "Enough said. (H4G1S == F4GZ)." To be branded as homosexual is enough to make one unworthy of full fellowship in the hacking community. Not only femininity, but any form of the other is suspect. Racial slurs lightly pepper the text of both the public and private discourses with such reference as "Motorola ch1nkz" and "Japboy."

Another distinction is between law enforcement and hackers, or informers and those who are loyal to the hacker cause. The informers seem to draw the most fire. For example, in the public discourse, HFG states that "U4EA SM3LLS LIKE HANDCUFFS. S0 D0ES TSUT0MU SH1M0MURA." In the code, they explain, "For those of you out of

---

[473] Sandesh Sivakumaran, "Male/Male Rape and the "Taint" of Homosexuality," *Human Rights Quarterly* 27, no. 4 (2005): 1282-1283.

[474] In this stanza, "suns" does not appear to be a misspelling of "sons," which would infuse elements of homoeroticism into the text. Rather, it is likely meant to describe Sun Microsystems machines, a popular server running a UNIX variant operating system called Solaris.

the loop, the hacker known as ‘u4ea’ is an FBI informant. He has been for well over a year now. Further, Shimomura was under investigation after the whole Mitnick ordeal. What, you didn’t wonder where HE got some of the proprietary software from? Or his OKI mods for scanning and tumbling? We won’t even go into the abuse and treachery surrounding the whole vigilante justice thing. Or why biased reporter civilians were allowed to partake in any part of the investigation.” Even in the poetry section, HFG states, “to the new writer matt / we say ‘at least you’re not a rat.’” Informants need not be hackers to serve as objects of ridicule and disdain.

Another attribute that distinguishes the hacker from the non-hacker is the ability to gain information and to control computer systems and networks. The opening comments in the code provide a list of sites that HFG had previously hacked. This is consistent with other hacks that they have performed.[475] There is also the assumption that one can gain access to information within the disclosure of Meinel’s address, phone numbers and Social Security number and the invitation to “search for her in your favorite info database.” To issue such an invitation assumes that the reader would already have access to enough databases to have a favorite.

Although the public face leaves the reader with little choice in how they are invited to perceive HFG and gives little rhetorical instruction concerning what kind of individual the reader should become, in the private discourse the ideal auditor and the author are somewhat conflated. HFG invites the hacker to become like them. But to do so is to forever alter one’s place in the world, a consideration that HFG seems aware of in

---

[475] For more examples of HFG’s hacks, see http://www.attrition.org/mirror/attrition/hfg.html. HFG’s hacks follow a similar pattern to that of the *New York Times* hack.

the final quotation found within the code: "So farewell hope, and with hope farewell fear, Farewell remorse: all good to me is lost; Evil, be thou my good." Like Satan in Milton's *Paradise Lost*, to enter the world of the hacker is to experience a kind of fall from grace.

Hermanowicz and Morgan argue that there are three ways that groups use ritual to construct collective identity—transformation, suspension, and affirmation.[476] Hacking rituals seem to almost exclusively use strategies of affirmation. Even when sanctioning deviants, HFG affirms the model of living to which deviants should conform. Parke Burgess states that "the strategies and motives of any rhetoric . . . represent an invitation to a life-style, an invitation to adopt a pattern of strategies and motives, verbal and nonverbal, that determine how men and women will function together in culture."[477] The nature of those greeted and ridiculed provides a clearer picture of the ideal hacker: He (and it is a *he*) doesn't give up root, can get root, can get 0-day warez,[478] is fiercely heterosexual, loyal, and, most of all, has technical skills. These are the traits and characteristics to be applauded—anything less is subject to ridicule and public shaming.

Interpretations of the Action

This hack was considered to be the first time that a major news outlet had been hacked. As such, this occasion received considerable coverage and various interpretations. But rather than the front-page coverage that one would expect from such

---

[476] Hermanowicz and Morgan, "Ritualizing the Routine: Collective Identity Affirmation," 208.
[477] Burgess, "The Rhetoric of Moral Conflict: Two Critical Dimensions," 120.
[478] 0-day warez is software that is cracked and distributed either before or on the day it was released to the public.

an occasion, the story was buried on page A18 of the *New York Times* (it was mentioned on the front page in the section labeled "Inside"; it was placed at the very bottom of the center of the page, beneath such news items as "3 Emmys to 'Frasier.'")[479] It is difficult to understand why such a show of force by hackers was met with such a subdued response. Almost four months earlier, the White House issued a white paper that stated, "Our economy is increasingly reliant upon interdependent and cyber-supported infrastructures and nontraditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy."[480] McCombs and Shaw argue that although the mass media may not tell citizens how to think on a particular issue, it does dictate what issues citizens should think about.[481] The *New York Times* seemed to acknowledge that they were hacked while simultaneously hoping that no one would notice or think much about the issue. The power of silence is considerable. While running the Nazi propaganda machine, "about one fifth of all press directives given by [Josef] Goebbels between 1939 and 1944 were orders to keep silent on one subject or another."[482]

The *New York Times'* own reporting of the incident totaled one article.[483] In the article, the *Times* downplay allegations against Markoff. "The group that took over the

---

[479] "Inside," *New York Times*, September 14, 1998.

[480] "White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," (Washington, DC: 1998), 1.

[481] See McCombs and Shaw, "The Agenda-Setting Function of Mass Media."

[482] Ellul, *Propaganda: The Formation of Men's Attitudes*, 56.

[483] Amy Harmon, "Hacker Group Commandeers the New York Times Web Site," *New York Times*, September 14, 1998. A search of the New York Times historical archive yielded only this article when searching for Hacking for Girlies. I used this as a way to avoid unrelated articles on hacking. It is surprising that "a possible first in security breaches for a news organization" would be dealt with in thirteen scant paragraphs.

Times site directed some of its comments at John Markoff, a reporter for The Times who covered Mr. Mitnick's arrest."[484] The *Times* report portrays Markoff as a reporter who happened to be on the wrong beat at the wrong time who was now being unjustly attacked along with the *Times*. But Markoff had done much more than simply cover Mitnick's arrest. By the time the hack occurred, Markoff had co-written two books about Mitnick and cut a movie deal from the book about Mitnick's pursuit and arrest.[485]

The *Times* explains that the motivation of the attack was to call for the release of Kevin Mitnick, but this is not the overarching theme of the text. Although the *Times* article briefly mentions the comment text, the reporter largely ignores the comments except to quote HFG's assertion that calling them terrorists is absurd. Within the code, they explain why they had singled out Markoff: "The injustice Markoff has committed is criminal. He belongs in a jail rotting instead of Kevin Mitnick. Kevin is no dark side hacker. He is not malicious. He is not a demon. He did not abuse credit cards, distribute the software he found, or deny service to a single machine. Is that so hard to comprehend?" HFG does not claim that Mitnick is innocent, only that the punishment does not fit the crime and that the *Times* helped to exaggerate the danger posed by Mitnick to society. By branding Mitnick "The Dark Side Hacker," Markoff created the image of a mythical hacker with almost superhuman powers.[486] Markoff's front page

---

[484] Ibid.

[485] See Katie Hafner and John Markoff, *Cyberpunk: Outlaws and Hackers on the Computer Frontier* (New York: Simon & Schuster, 1991); Tsutomu Shimomura and John Markoff, *Take-Down: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw--By the Man Who Did It* (New York: Hyperion, 1996). The movie, *Track Down*, which has been heavily criticized, both in terms of artistic merit and accuracy, was finally released in 2004 on DVD.

[486] See Hafner and Markoff, *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. In this book Hafner and Markoff devote 121 pages to Mitnick's story, describing him as "The Dark Side Hacker."

story describing Mitnick states that "as a teen-ager, [Mitnick] used a computer and a modem to break into a North American Air Defense Command computer, foreshadowing the 1983 movie 'War Games.'"[487] Mitnick claims that this is completely false: "No way, no how did I break into NORAD. That's a complete myth. And I never attempted to access anything considered to be classified government systems."[488]

The *Times* is unfair in its description of the content of the hacked webpage and the impact of the hack. Lance Hoffman, a computer science professor at George Washington University and Director of the Cyberspace Policy Institute, stated in the article that "the material posted by the hackers is offensive, childish, threatening and chilling. . . . It's a good example of why we have to bring accountability to the Internet."[489] However, there was little on the site that could not be seen or heard in a typical PG-13 rated movie, so "offensive" seems a bit overstated. The *Times's* claim that the logo had "images of nude women" is also misleading. His assessment of "childish" further demonstrates that he did not choose to look beneath the surface of the text and delve into the comments. The public appearance is juvenile, but the comments are informed and articulate. As for threatening, once again, it appears that Hoffman did not choose to go beneath the surface of the text. Did Hoffman really believe that HFG wanted the ransom of "104 GIRLIEZ, 6 BILLION IN N3WSPAP3R SUBSCRI1PTIONZ, AND MAYBE A PR1NT1NG PR3SS 0R S0M3TH1NG"? The text of the site is only chilling

---

[487] Markoff, "Cyberspace's Most Wanted: Hacker Eludes F.B.I. Pursuit."
[488] Penenberg, *Mitnick Speaks!*
[489] Harmon, "Hacker Group Commandeers the New York Times Web Site."

in the sense that Hoffman, by virtue of his position, has a vested interest in regulating cyberspace.

The article resorts to *ad hominem* attacks as a way to gain the last word. The article concludes with a quote from Meinel, who states that "these people are desperate for fame. . . . These are the kids who used to make stink bombs. Now they have the Internet."[490] In choosing this as the concluding statement, the *New York Times* dismisses HFG. This is further evidenced in the use of weighted terms such as "diatribe" and the description of Mitnick as "the imprisoned computer criminal."[491] Other official reports of the hack also resorted to such *ad hominem* attacks. For example, the *Independent*, a London newspaper, wrote, "Win [*sic*] Schwartau of Infowar, an information warfare web resource and consultancy also mentioned in last Sunday's hack, concurs. 'These are cowards and neo-nazis with no socially redeeming values, who refuse to engage in an intelligent debate.'"[492] Schwartau was mentioned in the code of the hack with his accompanying Social Security number.

The *Times* quoted only sources sympathetic to the *New York Times*, such as AntiOnline and Meinel.[493] They sought reactions only from groups and individuals who

---

[490] Ibid.

[491] Although Mitnick had been convicted previously of computer related crimes, he had not yet stood trial for the current set of crimes. This betrays a kind of "guilty before proven innocent" mentality on the part of the *Times*. It would be unthinkable to describe Mike Tyson as "convicted rapist, Mike Tyson" in a news article about boxing. Although it may be accurate based on the past, the wording makes it sound as if he had already been convicted of the crimes for which he was imprisoned, which was not the case. This betrays a lapse in professionalism on the part of the *Times* which may be attributed to bruised egos.

[492] Tamsin Todd, "Network: The Day the Times Stood Still; Last Sunday, on What Should Have Been One of Its Busiest Days Ever, the Mighty New York Times' Website Was Forced Offline by a Group of Hackers," *The Independent*, September 21, 1998.

[493] AntiOnline is one of the groups singled out in the ridicule section. This group does not seem to be well respected within the hacker community. In fact, one prominent hacker news site, Attrition, has an entire

were ridiculed in the hack and made no attempt to demonstrate the other side of the story from those who were greeted in the hack, such as Emmanuel Goldstein of *2600* (*2600* is mentioned in the article, so ignorance of the group is no excuse), *Phrack*, or l0pht.[494] The *Times* ensured that the coverage of the hack would be negative.

Throughout their coverage of the hack, the *Times* portrayed HFG as stupid, childish, and immature. In so doing, they illustrate the problems concerning such a characterization. If the network infrastructure is so insecure that such individuals can easily penetrate it, then the entire Internet economy and information infrastructure is as a house built on sand. Harmon states that this attack "seemed to underscore the fragility of the global computer network during a period when governments, corporations and individuals are increasingly relying on it as a source of instant news and information."[495] The *Times* article points out that this was a particularly high traffic time for the *Times* because of the publication of Kenneth Starr's report. HFG demonstrates that the timing was intentional: "HFG 1Z N0W G0ING INT0 THE C1GAR BUS1NESS T00. W3 W1LL S3LL 0UR 0WN L1N3 0F DES1GN0R C1GARS, START1NG W1TH THE 'L3W1NSKY C1GAR'. 1T HAS A FAIRLY D1STINCT TAST3. (AND W3 TH0UGHT *W3* W3R3 K1NKY!)"

---

section devoted to correcting misinformation spread by AntiOnline, found at http://attrition.org/errata/charlatan/negation/ that states, "We have proven beyond a reasonable doubt that AntiOnline and John Vranesevich are frauds." See Attrition Staff, "Negation: The End," *Attrition*, http://attrition.org/errata/charlatan/negation/ (accessed February 13, 2006).

[494] Four months previous to the HFG hack, L0pht had testified before the Senate Subcommittee on Governmental Affairs, so not only would L0pht be an ideal source, they had also been greeted in the hack, mentioned in the code, and HFG had even provided a link to L0pht's website. That the *New York Times* did not contact L0pht can only be viewed as a conscious decision to avoid their perspective. See Committee, *Weak Computer Security in the Government: Is the Public at Risk?*

[495] Harmon, "Hacker Group Commandeers the New York Times Web Site."

The Associated Press (AP) picked up the story, which was run by many smaller newspapers, more or less completely. Longer versions of these stories ran in the range of 227 words while shorter versions were in the range of 95 words. Almost all of these stories ran a quote from Nancy Nielsen, a *Times* spokeswoman, who stated that "the material was so offensive," and many referred to the hacked page as a "mishmash of pornographic pictures, creative spelling and vague threats posted on a black background."[496] Even in a 95 word article, the AP managed to make an error by claiming that "HFG, or "Hacking for Girlies," ridiculed several members of the *Times* staff." With the exception of unnamed system administrators, John Markoff is the only member of the *Times* staff explicitly held up to ridicule. Even a cursory reading of the hack reveals that HFG still has some measure of respect for the other named *Times* staffer, Matt Richtel.

Wired News takes a relatively neutral stance on the hack. They quote a segment of a poem questioning the *Times'* journalistic ability, followed by a quote from the comments about Meinel's goal to entrap HFG. However, in this article we also get a piece of the *Times'* interpretation of the event. Bernard Gwertzman, editor of the *New York Times* on the Web, stated, "We consider this very serious. They are interfering with the press' ability to function."[497] In *Editor and Publisher*, Gwertzman makes similar comments: "This is the equivalent of somebody blowing up a press. . . . A lot of people,

---

[496] "New York Times Web Page Is Hacked," *Times – Picayune* (New Orleans), September 14, 1998.
[497] Hesseldahl, *All the News That's Fit to Hack*, para. 24.

I'm sure, were planning to read our coverage of the Starr report and were deprived of it."[498]

These statements raise questions concerning the nature and role of the press in the digital age. How does the press function? Is an online presence necessary? Based on his statement, Gwertzman seems to think that an online presence is necessary, but the *New York Times* is, after all, a newspaper. Had the core function of the *Times* been disrupted by the actions of HFG? The answer to this question depends on what one considers to be the core function of the *New York Times.* If the core function of a newspaper is to distribute and sell newspapers, then no, the core function was not disrupted significantly. There was no alteration to the print version and the Sunday edition of the print version totaled 1,627,099 copies at the time of the hack.[499] The statement equating the hack to the physical destruction of their printing press is hyperbole at best and dangerous at worst. To compare a website defacement to blowing up a printing press is like comparing graffitti to arson. By resorting to such characterizations, Gwertzman short circuits any possibility of rational discussion concerning why the site was hacked and ignores the opportunity to actually address HFG's assertions.

Hesseldahl writes in the *Columbia Journalism Review*, "The apparent goal was to bring attention to the case of jailed hacker Kevin Mitnick, the hacker underground's favorite martyr. . . . The "Free Kevin" crowd blames the *Times*, particularly its San Francisco-based technology reporter John Markoff, for causing Mitnick's arrest in

---

[498] David Noack, "Hack Attack Sends Chill through News Web Sites," *Editor & Publisher*, September 19, 1998.

[499] Circulation figure taken from *The New York Times Company*, "Circulation Data," 2006, http://www .nytco.com/investors-nyt-circulation.html (accessed February 13, 2006).

1995."[500] While Hesseldahl seems more clear on HFG's motivations that the *Times*, his use of terms such as "vandalism," "rambling statement," and "offending page" betray a definite bias against HFG. The article does not mention the comments in the text at all.

But perhaps a rambling diatribe is what HFG was after. Theodore Windt explains that "the diatribe is to rhetoric what satire is to literature. Each attempts to reduce conventional beliefs to the ridiculous, thereby making those who support orthodoxy seem contemptible, hypocritical, or stupid. Each seeks laughter, but not for its own sake. Rather, laughter serves as a cleansing force to purge pre-conceptions about ideas, to redeem ignored causes, to deflate pomposity, to challenge conventional assumptions, to confront the human consequences of ideas and policies."[501] Within the code, HFG explains, "We are bored, want to make people laugh, and most assuredly not malicious." Perhaps the most blatant attempt to mix humor with a message is found in the poetry section, which is the only section on the public side that is not written in leet speak. Within these four stanzas, they argue that Markoff has an unexplained personal vendetta against Mitnick, that Shimomura is a criminal, and that the *New York Times* engages in unfair reporting practices. This is not merely badly written poetry—this is an argument infused with humor, both for the general populace and for the hacker underground.[502]

---

[500] Arik Hesseldahl, "After the Hack," *Columbia Journalism Review* 37, no. 5 (1999): 14.

[501] Windt, "The Diatribe: Last Resort for Protest," 8.

[502] For example, the lines "we busted root on their women and their suns / next thing you know, we'll be looking for nuns" has several layers of meaning. They poke fun at the idea that they are sliding down the path of libertine degradation that leads them to the point of attempting to seduce nuns, a significant religious and social taboo. This is such an exaggeration that the general public would see this as an attempt at humor, further exaggerated with the idea of getting root on their "suns." But "suns" is not a misspelling of "sons"—likely it is a play on words that alludes to Sun servers, a common brand of server running Solaris, a version of UNIX. Here we have the reinforcement of gaining root access on both their women and their machines, reinforcing the hypermasculine performance of hacking.

Moreover, HFG may have gained more psychologically out of the hack by simply attacking the *New York Times* than they would have gained for the movement by engaging in rational discourse. Tiffany Derville argues that "the meager achievements that activists might gain through meaningful discourse with targets leave them with a sense of defeat. However, an outside approach that involves militant acts such as insulting communication leaves activists with a sense of fulfillment.[503]

Some official channels were more accurate in their reporting. For example, the *Register*, a UK security site, stated, "The front page of the *NYT* site was adorned with three females—widely reported as pornographic, but a visit to a mirror at http://www.antionline.com/ will show otherwise—and was an attack on the *NYT*'s reporting of the imprisoned hacker."[504] CNN was one of the few outlets to actually display a screen capture of the hacked web site with the HFG logo displayed unaltered. Nowhere in the article do they refer to the imagery as "obscene" or "pornographic." CNN also notes the distinction between the public persona and the persona portrayed within the code: "In a self-parody, the hackers type in all capital letters, playing the role of stereotypical computer geeks. But in their comment tags, the hackers type almost flawlessly and quote literary figures, such as Voltaire."[505]

The media, for the most part, reinforced misconceptions concerning hackers and misrepresented the hack itself. By conjuring up the image of the juvenile hacker, the

---

[503] Tiffany Derville, "Radical Activist Tactics: Overturning Public Relations Conceptualizations," *Public Relations Review* 31 (2005): 529.
[504] Graham Lea, "New York Times Hacked," *The Register*, September 14 1998, http://www.theregister.co .uk/1998/09/14/new_york_times_hacked/ (accessed February 13, 2006).
[505] Cable News Network, "Hackers Break into N.Y. Times Web Site," *CNN.com*, September 13, 1998, http://www.cnn.com/TECH/computing/9809/13/nyt.hacked/ (accessed February 13, 2006).

Times maintained the mental disconnect that accompanies most official discourse concerning hackers: hackers are simultaneously childish, juvenile delinquents who are breaking into these systems to engage in what amounts to digital graffiti, yet hackers are skilled, brilliant, relentless criminals who are out to break into communication infrastructure, banking systems, and vital services such as hospitals and air traffic control systems. So long as this disconnect is maintained, government, law enforcement, and computer security professionals will profit from the public's fear of the hacker.

Ego Function of Protest Rhetoric

Some reports argued that HFG had made a rhetorical error in placing the coherent, articulate argument within the code while leaving the juvenile persona open to public view:

> If Hacking for Girliez had limited their message to a summary of the Mitnick case, or a critique of Markoff, it might have served as a pure—if illegal—act of protest. But they didn't. Like most website hackers, they devoted much of their fifteen minutes of fame to a lengthy discourse on how great they are, how much other hacker groups suck, and how inept computer system administrators are. Moreover, the message was rife with gratuitous raunch, racism, lowbrow insults, and was written in the stylistic lingua franca of the computer underground, which is nearly incomprehensible to the average reader: "TH3R3 AR3 S0 MANY L0S3RS H3R3, 1TZ HARD T0 P1CK WH1CH T0 1NSULT THE M0ST." As the first known case of a Web hack against a traditional media outlet, the HFG

> action received considerable news coverage around the world—putting the much-neglected Mitnick case back in the news. But, given the intrusion's infantile content, it might do more harm than good to a cause that's on the verge of public acceptance.[506]

However, this seems based on the assumption that HFG wanted to convince the general public of the unethical reporting of the *New York Times* and how it related to the Kevin Mitnick case. Parke Burgess writes that "when viewing culture from the unique strategic view of rhetoric . . . one will conceive of public enactments not simply as substantive statements of moral values and political views, but as strategic invitations to act on such values and views, so that the meaning of public statements always lies, in part, in their strategic intention as symbolic action."[507] Rhetoric is a means of inducing judgment, and the judgment that the public is invited to make is that HFG is harmless and much like they were when they were younger and more foolish—that HFG is simply enacting another mode of youthful rebellion and eventually they will mature and the cycle of life will continue. Had HFG reversed the two faces, providing an articulate message and casting off the juvenile persona, they would have reinforced the perception that hackers are intelligent and dangerous—which was exactly why the general public feared hackers like Mitnick.

The *New York Times* hack may have drawn public attention to Mitnick's situation, but HFG's real rhetorical work takes place beneath the text, within the code. The work

---

[506] Kevin Poulsen, "Grassroots Hacktivism," *G4 Media Inc.*, September 16, 1998, available from http://www.g4tv.com/techtvvault/features/3292/Grassroots_Hacktivism.html (accessed February 13, 2006).
[507] Burgess, "The Rhetoric of Moral Conflict: Two Critical Dimensions," 126.

being done in this hack is the reinforcement of hacker collective identity and what Richard Gregg refers to as the "ego function of the rhetoric of protest," in which "the primary appeal of the rhetoric of protest is to the protestors themselves, who feel the need for psychological refurbishing and affirmation."[508]

According the Gregg, one aspect of the ego-function of rhetoric "has to do with *constituting* self-hood through expression; that is, with establishing, defining, and affirming one's self-hood as one engages in a rhetorical act."[509] There must first be a group to be affirmed. HFG is performing constitutive rhetoric, inviting other hackers to accept HFG's values and ideals. HFG clearly delineates who should be considered a part of this group, interpellating them, as it were.[510] Hackers are invited to see themselves in this ideal auditor. Moreover, hackers and others are encouraged to consider the plight of Kevin Mitnick, the supposed reason for the hack.

Michael McGee writes, "Each political myth presupposes a 'people' who can legislate reality with their collective belief. So long as 'the people' believe basic myths, there is unity and collective identity."[511] Mitnick is the substance and embodiment of one of the core basic myths of the hacker movement. Hackers do not argue about whether he broke the law; rather, the arguments range from whether or not the law is just to disagreements concerning the severity of the punishment. Mitnick serves as synecdoche for the entire hacker movement. The disagreements over the imprisonment of Mitnick

---

[508] Gregg, "The Ego-Function of the Rhetoric of Protest," 74.
[509] Ibid., 74.
[510] For more on social movement rhetoric as a way to constitute a collective identity, see Charland, "Constitutive Rhetoric: The Case of the *Peuple Quebecois*."
[511] McGee, "In Search of 'the People': A Rhetorical Alternative," 245.

reveal the cleavages within hacker collective identity. For hackers, to argue about Mitnick is to argue about themselves.

It is logical that HFG would chose to perform this display of collective identity in the hack of a website. The enactment of hacking constitutes identity as a hacker and the hacking itself reinforces the collective identity through the accompanying rituals. Hermanowicz and Morgan state that "identity often is constructed through a series of ritual practices: special performances call attention to group attributes and to the sacred essence of the group itself."[512] Hacking is a sacrament in the church of hacking—one cannot become a full convert until one has participated in the ritual. "Identity affirmation occurs when practices being celebrated are both customary and already invested with a high level of sacredness."[513]

Within the popular media, hacker is a term synonymous with "geek" or "criminal." The entertainment media have a tendency to romanticize the hacker, albeit in ways that hackers do not identify with. Constructing and reaffirming their identity through hacking allows hackers to help define their identity. Benson demonstrates the transactional quality of defining oneself; when presented with a possible way of defining one's self, the person who would be defined is free to choose whether to accept or reject the offered identity.[514] Terranova explains that what is at stake in any kind of social discourse is the struggle over meaning and definition: "The information transmitted by a news broadcast is secondary when compared with the meanings articulated within it,

---

[512] Hermanowicz and Morgan, "Ritualizing the Routine: Collective Identity Affirmation," 198-199.
[513] Ibid., 200.
[514] Benson, "Rhetoric as a Way of Being."

which in their turn have then to be taken up by social practices to engender a social reality (from support for wars to cultural identities and lifestyles). Information is thus implicitly seen only as a kind of alibi for the communication of social meanings, which is where the 'real' cultural politics takes place. In other words, if meanings arise and return to social reality as an active force, then the political dimension of culture is mainly concerned with the struggle over meaning."[515] Stewart, Smith, and Denton state that "self-naming is often a critical step toward self-identity and mobilizing the oppressed."[516] But naming takes place on both sides. Haig Bosmajian points out that "one of the first important acts of an oppressor is to redefine the oppressed victims he intends to jail or eradicate so that they will be looked upon as creatures warranting suppression and annihilation. I say 'creatures' because the redefinition usually implies a de-humanization of the individual."[517] This took place in many of the mainstream accounts of the hack—HFG was referred to as "cowards," "neo-nazis with no socially redeeming values," "the kids who used to make stink bombs." By demonizing and dehumanizing HFG, it is easier to discount and dismiss their message.

Another possible reason for the hack may be a sense of perceived powerlessness. Mitnick had been in custody for approximately three and a half years by the time the hack took place. Shimomura and Markoff had already written a book about Mitnick's capture and stood to profit even more from a fictionalized movie account. Hackers had had little

---

[515] Terranova, "Communication Beyond Meaning: On the Cultural Politics of Information," 54.
[516] Charles J. Stewart, Craig Allen Smith, and Robert E. Denton, *Persuasion and Social Movements*, 4th ed. (Prospect Heights, IL: Waveland Press, 2001), 60.
[517] Haig A. Bosmajian, "Defining the 'American Indian': A Case Study in the Language of Suppression," *The Speech Teacher* 21, no. 2 (1973): 89.

effect. Haiman argues that "if the channels for peaceful protest and reform become so clogged that they appear to be (and, in fact, may be) inaccessible to some segments of the population, then the Jeffersonian doctrine that 'the tree of liberty must be refreshed from time to time, with the blood of patriots and tyrants' may become more appropriate to the situation than more civilized rules of the game."[518] Perhaps the hack was a virtual equivalent to the display of POW-MIA flags which state "you are not forgotten."

In this hack, HFG serves as a radical faction of the Free Kevin Mitnick movement. Kevin Poulsen considers that "one could theorize that HFG deliberately chose an extreme and ludicrous childish voice, with the sophisticated goal of drawing the most extreme and ludicrous authoritarian reactions from their targets."[519] James Klump explains that overreaction from those in power can have the effect of polarizing support for the two factions, removing the middle ground. When the force is viewed as unjustified by those within the mainstream, this can help to build popular support and sympathy for the radicals.[520] Even where there is no support for the radical faction, the radical faction can claim a moral victory. "By acting out against the enemy, activist organizations declare themselves winners even when no social territory is gained because of member fulfillment."[521]

For radical organizations, extreme action is a win-win situation. Tiffany Derville argues, "By making demands that powerholders are unlikely to accept, radical activist

---

[518] Haiman, "The Rhetoric of the Streets: Some Legal and Ethical Considerations," 105.
[519] Poulsen, "Grassroots Hacktivism."
[520] James F. Klumpp, "Challenge of Radical Rhetoric: Radicalization at Columbia," *Western Speech* 37, no. 3 (1973): 146-56. See also. Scott and Smith, "The Rhetoric of Confrontation."
[521] Derville, "Radical Activist Tactics: Overturning Public Relations Conceptualizations," 530.

organizations stay faithful to their vision and redefine what people consider moderate by moving the ends of the spectrum. By arguing for much more radical demands than mainstream activist organizations request, they increase the reasonableness of mainstream activist organizations' demands."[522] This tactic can be seen in other movements and is one of the tactics most likely to be misunderstood by both those within the movement and those outside of the movement. For example, many within the anti-globalization movement were angered that anarchists broke windows and participated in violent action, but failed to realize that it was those very actions that allowed the movement to receive increased media coverage. Without media coverage, the WTO protests in Seattle would have likely been ignored and quickly forgotten by the general public—the media coverage allowed the public to wonder why the violence was taking place.[523]

The main problem with the strategy of assuming a radical stance for the hacker movement is that there are not many moderate hacker groups and those that are (L0pht, Cult of the Dead Cow) have either been co-opted or remain relegated to the underground.[524] Without a visible moderate element, there is nothing for the mainstream

---

[522] Ibid., 531.

[523] See DeLuca and Peeples, "From Public Sphere to Public Screen: Democracy, Activism, and the 'Violence' of Seattle"; Owens and Palmer, "Making the News: Anarchist Counter-Public Relations on the World Wide Web."

[524] There is some crossover between hacker groups; for example, L0pht and Cult of the Dead Cow share members. As for the co-optation of hacking, one prime example is that of L0pht. L0pht went on to form the network security corporation @Stake, which was recently acquired by Symantec, a multinational corporation of over 14,000 employees. Even so, according to Space Rogue, as of 2004, only one member of L0pht remained at the company they had created—not only had they been co-opted, but they had been driven out as well. According to Space Rogue, "What has been most interesting is to see technology advance and realize that 'Hey, L0pht thought of that 5 years ago.' But due to lack of funds we could never make it happen. Of course after we got the money we no longer had control and can only sit back and watch as other people developed our ideas. Sigh." See Space Rogue, "Lets Set the Record Straight."

population to compare against. To mainstream society, all hackers fit neatly within one category: "criminal." Even organizations that may be sympathetic to hacking, such as the Electronic Frontier Foundation or Electronic Privacy Information Center, are far removed from the collective consciousness of mainstream society and often distance themselves from hackers in an effort to maintain legitimacy. Perhaps this is because the concerns of hackers (as well as others who have a clear stake in the digital world) are far removed from the concerns of ordinary citizens.

Hacking was subtly redefined as terrorism by the USA PATRIOT Act with little concern raised by the general population.[525] But the general public will not fight for the hacker because they cannot identify with the hacker. Hackers have not succeeded in generating a widespread belief in their beliefs as environmentalists and other social justice groups have done. Members of the general public understand the idea of environmentalism and few people wish to live in a world without trees, clean air, and potable water. Hackers have strongly differentiated themselves from the general population while other social movements have tried to engage the sympathy of the public. Perhaps this is a reflection of hacker arrogance—hackers do not need the masses to help them; hackers can do what they need to on their own. But they can't. So long as misinformed fear of the hacker exists, the general public will continue to view them with a mixture of contempt and fear and support harsh sanctions for hackers. But this may

---

Slashdot, September 17, 2004, http://it.slashdot.org/comments.pl?sid=122222&threshold=1&commentsort=0&mode=thread&cid=10280841 (accessed February 14, 2006).

[525] To be fair, the entire USA PATRIOT Act was passed with little concern expressed by much of the population. For more on the connection between hacking and the USA PATRIOT Act, see *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001,* § 814, 816.

serve only to strengthen the collective identity of the hackers, causing it to become even further entrenched: "The paradox of stressing the injustices that arise from some division lies in the seemingly inescapable tendency to become fixed in such a way that transcending identifications become difficult. Wounds suffered become badges of honor."[526]

In order for this state of affairs to change, there would have to be an ideological bridge between the hackers and the general public. Ellul writes, "Propaganda cannot create something out of nothing. It must attach itself to a feeling, an idea; it must build on a foundation already present in the individual," explaining further that "the propagandist must concern himself above all with the needs of those whom he wishes to reach. All propaganda must respond to a need, whether it be a concrete need (bread, peace, security, work) or a psychological need."[527] The general population cannot relate to the needs of the hacking community and does not understand why hackers have a desire to break into other machines. This lack of understanding is partially a result of how hacking has been framed. Hacking can be viewed in many ways—trespassing, breaking and entering, software engineering, reading a book. This last way of framing hacking may seem incongruous when compared to the other possible frames but for many hackers, the quest for knowledge is what drives them. Members of the general public may find such motivations more palatable than the desire to snoop or trespass. But such motivations are not the image held within the collective consciousness of the general public, and it is not

---

[526] Robert L. Scott, "The Conservative Voice in Radical Rhetoric: A Common Response to Division," *Speech Monographs* 40 (1973): 129.
[527] Ellul, *Propaganda: The Formation of Men's Attitudes*, 36-37.

only the fault of governmental agencies and the mass media—hackers also contribute to the general public's lack of understanding.

Eli Zaretsky states that "the notion of identity involves negation or difference—something *is* something, *not* something else."[528] Hackers have always been a group of outsiders and have thrived on this form of ostracism. The fact that they are not like everyone else is worn like a badge of honor, but it is more than the idea of not being like everyone else—rather, the hacker believes that he or she is *better* than everyone else. This mentality is at work in the hack of the *New York Times* and in the "The Conscience of a Hacker." The idea that hackers are more intelligent and more creative than the general population is a core part of hacker identity. Craig Calhoun argues that "it is not just that others fail to see us for who we are sure we really are, or repress us because of who they think we are. We face problems of recognition because socially sustained discourses about who it is possible or appropriate or valuable to be inevitably shape the way we look at and constitute ourselves, with varying degrees of agonism and tension. These concerns frequently, though not uniformly, are expressed in and give rise to 'identity politics.'"[529] For hackers, intelligence and skill are the gold standard; these attributes allow hackers to maintain a sense of superiority because the general public remains largely ignorant concerning technical matters.

---

[528] Eli Zaretsky, "Identity Theory, Identity Politics: Psychoanalysis, Marxism, Post-Structuralism," in *Social Theory and the Politics of Identity*, ed. Craig J. Calhoun, 198-215 (Oxford: Blackwell, 1994), 200.
[529] Craig Calhoun, "Social Theory and the Politics of Identity," in *Social Theory and the Politics of Identity*, ed. Craig J. Calhoun, 9-36 (Oxford: Blackwell, 1994), 20-21.

Hackers are in a double bind—in order to maintain a core tenet of their collective identity, they must be superior to everyone else. This also applies to other hackers; there is a strong urge to be not just a hacker, but an *elite* hacker. However, this self-imposed distance—physical, psychological, and ideological—from the general public engenders fear that leaves hackers vulnerable to persecution. Hackers need a way to relate to the general public. Hackers have attempted this to some extent by redefining hacking outside of computer terminology, but these efforts must go further. To take a lesson from Ellul's propagandist, hackers must connect to some need held by most of the members of the general public.

The Kevin Mitnick case is an example of how hackers have been ineffective in resonating with the general population and part of the reason for this ineffectiveness can be summed up in three words: "free Kevin Mitnick." Although this is a good slogan, it leaves some major premises unspoken. Hackers do not contend that Mitnick is innocent, only that he is being treated unfairly and that the punishment is unjust. But why should the general public wish to release a repeat-offender? They cannot relate to a repeat-offender hacker who has been imprisoned. Perhaps if the public had a clear idea of what Mitnick had actually done and if the reported costs of his crimes were actual rather than projections by the corporations that Mitnick had digitally entered, perhaps the public would take a more sympathetic view of the Mitnick case. In order for the general public to understand exactly what Mitnick had done, hackers would have to do more than hack webpages and post slogans; hackers would have to educate the masses. But hackers believe that the masses are stupid and unable to be educated on technical matters. Like propagandists, hackers do not have to actually change their opinion of the masses to

change the public's opinion of hackers. Hackers would be able to view it as an exercise in social engineering, attempting to create resonance where there should be none. So long as hackers continue to engage in protest actions that do not resonate with the general public, they will remain relegated to the fringes and thus more vulnerable to persecution and legislation that defines them in problematic ways.

The "free Kevin Mitnick" movement illuminates current rhetorical theory, specifically the ego-function of protest rhetoric, because it does not fall neatly into the rubric of self- or other-directed social movements. Although Kevin Mitnick was a hacker, "free Kevin Mitnick" was not all about hackers. Mitnick acted synecdochically as a representative of the hacker movement, serving as the most visible example. Thus, "free Kevin Mitnick" could be considered a "self-directed social movement." But hacktivism keeps hacker identity at the forefront in both self- and other-directed social movements. Charles Stewart found that people in self-directed social movements "saw themselves as innocent, blameless victims, not for anything they had done to deserve victimage, but because of who or what they were."[530] This sentiment is at work in the *New York Times* hack when HFG states in the code of their hack, "The injustice Markoff has committed is criminal. He belongs in a jail rotting instead of Kevin Mitnick. Kevin is no dark side hacker. He is not malicious. He is not a demon. He did not abuse credit cards, distribute the software he found, or deny service to a single machine. Is that so hard to comprehend?" However, the frame changes when hackers take on other movements, which is predicted by Stewart as well, although with a twist—hacktivists often identify as

---

[530] Charles J. Stewart, "Championing the Rights of Others and Challenging Evil: The Ego Function in the Rhetoric of Other-Directed Social Movements," *Southern Communication Journal* 64, no. 2 (1999): 101.

hackers even in other-directed movements, contrary to Stewart's findings that "protesters did not address who or what they were, only what they were protesting because their ego came from the struggle rather than individual identity."[531] For example, a hack of an East Timor governmental website clearly identifies the group as "Portugese Hackers Against Indonesian Tirrany" [*sic*].[532] The group opens the hack by stating "This attack is not against indonesian people but against its government and their opression towards the republic of timor. These actions were made to honour and remember all the 250 people killed in Dili on the 12 november 1991. As a result all sites belonging to indonesia's goverment were erased, the rest only had their webpages changed." The group then proclaims, "!Now for some Haxing!" and quickly moves into a catalogue of other hacks that they have performed.

In hacktivism, it is difficult to separate the hacker identity from the hacker action. The two seem to be inseparably entwined. The ego function in hacktivism may come not from the protest movement itself, but from the means by which the protest is enacted. It is no secret that the hacker movement is fueled by ego, although more in terms of popular usage rather than in the way that Gregg describes. In hacking, it is the *ability to hack* that rehabilitates the bruised ego rather than validation from some external source. It is not that someone is finally listening to and acknowledging a group's pain or how they have been wronged; hackers have the ability to force others to listen to an account of their pain.

---

[531] Ibid., 102.

[532] P.H.A.i.T., "Hacked Timor," *2600*, November 22, 1997, http://www.2600.com/hackedphiles/timor010198/indo/ (accessed February 3, 2006). Spelling has been left as found on the site.

Hacktivism and Democracy

The *New York Times* hack illustrates some of the problems with hacktivism as a strategy for social change and democratic practice. Perhaps the main issues have more to do with the collective identity of those skilled enough to perform hacktivism because hacking serves not only as a political strategy, but as a way to reaffirm hacker identity. Hermanowicz and Morgan write, "Groups affirm their identities through practices that 'ritualize' the routines of their communal life."[533] Hacktivism is not an isolated incident, but a system of rituals that shape the collective identity of hackers. Hacker collective identity embraces a hypermasculine, elitist, radical worldview that maintains a firm belief in the hacker's intellectual superiority.

Hacktivism can be used to try to enact change or to fulfil the ego-function of protest rhetoric. The electrohippies used it to hinder the WTO's online presence and to draw attention to the economic injustices caused by the enactment of WTO policies. However, in the case of the *New York Times* hack, HFG used their temporary bully pulpit as a way to reinforce hacker collective identity. The viewer was invited to identify with HFG somewhat, but this identification was not with an equal, but with a persona that resembled the way the reader once was in a younger, more foolish state.

The *New York Times* hack demonstrates that, although the ends of hacktivism may potentially overcome barriers to political action, the agents of hacktivism subscribe to a worldview that is decidedly undemocratic. Hacktivism has the potential to give voice to those who would otherwise be drowned out in the flood of mass-mediated messages.

---

[533] Hermanowicz and Morgan, "Ritualizing the Routine: Collective Identity Affirmation," 198.

McChesney and others have pointed out that as the mass media have consolidated, the message has become less and less varied.[534] In such an environment, it is difficult to voice dissenting opinions and present alternate viewpoints. In this case, HFG was able to air grievances concerning the *New York Times* to both the *Times* and the general public by hijacking a well-known and heavily trafficked website.

As the costs of participating in the public sphere become higher, fewer citizens will have a chance to participate in deliberations that will have an impact upon their lives. By enabling the automation of political action, hacktivism allows those who may have the desire, but not the time, to participate in social movement actions. Students have long been a staple of social movement protest activity, partly because they have less material concerns than those who are not students. A person working two jobs to make ends meet may believe strongly in the movement to provide for a living wage, but may lack the time and the energy to participate. Hacktivism allows such a person to participate in absentia in a movement that may directly affect his or her life.

But the question of whether the playing field will ever be leveled through technology remains. The person working two jobs to make ends meet may not be able to afford a computer or have the skills to use it to engage in political action. Perhaps hacktivism merely trades one set of access barriers for another set. Even so, hacktivism is an available rhetorical strategy. Even if it is not the panacea that some have hoped for, it does seem to be a useful means of protest that may work well in concert with other protest actions. As society becomes more wired, hacktivism will likely take on a larger

---

[534] See McChesney, *Corporate Media and the Threat to Democracy*; Sussman, *Communication, Technology, and Politics in the Information Age.*

role in social movement rhetoric; there may come a time where it becomes an indispensable rhetorical strategy.

Chapter 5

Conclusion: What are the Prospects for a Technologically Mediated Democracy?

Because hackers are the group most likely to create and shape technology, the question of how technology will affect democratic practice is tied to hacker identity and values. Those who create technology infuse in those technologies their values, and core tenets of hacker identity are at odds with principles of democratic practice. Hackers believe that they are more intelligent than everyone else and that the masses are incapable of understanding technology; are suspicious of the other, especially the feminine; adhere to a strict hierarchy based on technical skill; and are fiercely loyal, preferring to remain separate from the rest of society. These ideals are at odds with the democratic values of inclusion, the idea that all citizens should have a voice, and the belief that if citizens are given adequate information they can make decisions concerning the common good. These findings sound a note of caution to those who look to technology as a means of reinvigorating democratic practice and inclusion.

But there is hope for a technologically enhanced democratic society. Events such as Operation Sundevil and the capture of Kevin Mitnick provided incentive for hackers to organize from a loose collective into a social movement. As hackers have organized, they have become politicized, using hacking for political ends. This is not simply the result of their mobilization as a social movement; hackers had been aware of the political implications of their craft before Operation Sundevil and other hacker crackdowns. But many hackers are now engaging in hacktivism as a mode of political action. Groups such

as the electrohippie collective and Cult of the Dead Cow are actively seeking to promote democratic principles though the use of political hacking. Some groups, such as the electrohippes, have automated the process so anyone with a computer and an Internet connection can do the work of the hacktivist. These instances of reaching out to the general public provide evidence that hacker collective identity may be shifting away from self-imposed isolation and toward awareness that hackers need public support to create social change.

Other instances of hacktivism are not so encouraging. Hacker identity is performed and reinforced through hacking, and some instances of hacktivism serve mainly to reinforce the "ego function" of protest rhetoric, where the focus is psychic rehabilitation rather than societal change. Hacktivism presents a special case of the ego function of protest rhetoric in which hacker identity is never ignored, even in other-directed social movements—psychic rehabilitation comes through the means of protest (hacking) rather than the cause itself. In the case of the *New York Times* hack, Hacking For Girliez (HFG) reinforced the division between hackers and did little to build public sympathy for the plight of hackers. Acts of hacktivism that serve only to reinforce collective identity will do little to enhance democratic deliberation.

The prospects for democratic practice in an information society are bound up in several converging areas. There is the question of identity in an information society and the accompanying issue of identity as citizen. There is the question of who is manufacturing and designing technology and what values those people instill within those technologies. There is the possibility of new, more democratic means of protest and civic engagement, but with these means comes the question of how individual citizens

will use them. In the context of this study, there is another concern to be addressed—the efficacy of unconventional, unsanctioned, and even illegal means of political expression, as is the case of hacktivism.

Identity in an Information Society and Identity as Citizen

Theories of the information society and new media provide some clues concerning the constraints that living in an information society places upon democratic practice. These constraints include interactivity, the ability to transcend national borders and evade state censorship, the importance of information, and the ability to quickly attain information from a variety of sources. These themes are integral to hacker collective identity. In “The Conscience of a Hacker,” The Mentor advocates a digital lifestyle free of corporeal constraints, where ideas are the coin of the realm and connecting with like minded individuals is the goal, regardless of physical location. The electrohippies campaign demonstrates that national politics are no longer limited to particular geographic borders. Because nongovernmental organizations and transnational corporations are no longer tied to a particular nation state, protest against these entities must also transcend national borders. Hackers have adopted the digital persona and recognize that this is now an interconnected world; one can no longer afford to remain isolated.

Identity is tied to technologies that we have created. Dyens argues that “machines coevolve with us; our respective existences are completely tied to each other. To reflect upon technological culture is thus not simply to think about the impact of technologies on

our world, but also to examine the emergence of new strata of reality, where living beings, phenomena, and machines become entangled."[535] By adopting a virtual identity that is technologically dependent, hackers enact this entwinement of the physical and the virtual. However, scholars such as Turkle and others illustrate that this identity shift is not exclusive to hackers.[536] Negroponte writes, "Being digital is different. We are not waiting on any invention. It is here. It is now. It is almost genetic in its nature, in that each generation will become more digital than the preceding one."[537]

The transition to digital identity provides advantages and disadvantages. Fortunati argues that "in post-modern society, the social system of differences developed in the modern age is being completely restructured. Many differences, even between men and women, or more specifically, between the world of production and reproduction, have disappeared, or are at least less clear cut. There is a tendency at the social level to fusion, to the formation of hybrids, to the development of similarity."[538] The elimination of current gender constructions would be beneficial if it eliminated such behaviors as gender bias and misogyny. Even so, Fortunati's claim may be overstated; scholarly exultations of the digital persona cannot erase considerations of the material world. Millar points out that "while affluent western feminists may see themselves as 'cyborgs' as they use digital technologies for creative and professional purposes, less advantaged

---

[535] Dyens, *Metal and Flesh: The Evolution of Man: Technology Takes Over*, 11.

[536] See Leung, "Impacts of Net-Generation Attributes, Seductive Properties of the Internet, and Gratifications-Obtained on Internet Use"; Leung, "Net-Generation Attributes and Seductive Properties of the Internet as Predictors of Online Activities and Internet Addiction"; Turkle, *Life on the Screen: Identity in the Age of the Internet;* Sherry Turkle, *The Second Self: Computers and the Human Spirit* (New York: Simon and Schuster, 1984); Weiler, "Information-Seeking Behavior in Generation Y Students: Motivation, Critical Thinking, and Learning Theory."

[537] Negroponte, *Being Digital*, 231.

[538] Fortunati, "The Human Body: Natural and Artificial Technology," 79.

women—such as those who assemble computer equipment or enter data—experience 'cyborg' life in a profoundly different and exploitative way."[539]

If any group were to dissolve into the sea of hybridity, it should be those most likely to consider themselves "digital," but the hacker manifesto and the Hacking For Girliez hack illustrate that gender is still a relevant construct within hacker collective identity. That hackers cling fiercely to gender constructs casts doubt upon arguments that digital society is moving toward a state of hybridity, as Fortunati claims. Turkle's findings may not be true realities experienced by the respondents, but rather well constructed, realistic fantasies.

Although pronouncements of the elimination of gender seem premature, the digital realm does provide individuals with more possibilities for self presentation. Jones explains that "we have the opportunity online not only to easily seek out communities of interest convergent with our own, but to reshape ourselves, adopt different personae for different communities and environments, and experiences more such fleeting moments of convergence [of interests, goals, language, reality]"[540] Sennett connects citizenship with the idea of civility, defining civility as "the activity which protects people from each other and yet allows them to enjoy each other's company. Wearing a mask is the essence of civility."[541] The Internet may allow citizens to reclaim the kind of impersonal interaction championed by Sennett.

---

[539] Millar, *Cracking the Gender Code: Who Rules the Wired World?* 62.
[540] Jones, "The Internet and Its Social Landscape," 27.
[541] Sennett, *The Fall of Public Man*, 264.

Perhaps the main advantage of the transition to digital identity is the ability to transcend physical limitations of time and space. Alejandro Molina explains that "the immediate, realizable potential of cyberspace, then, is the possibility of connecting, communicating, partnership, publicity, alliances that transcend our material limitations, and, most important, building community in which location refers to a political space that contains collective memory in the struggles for self-determination."[542] But this is problematic. As the public sphere moves into the digital realm, those without access are systematically excluded and even those who have access will be excluded if they lack the requisite digital literacy to join the online dialogue. Molina argues that "[Internet] access is merely a symptom and that the real divide lies in the ability to construct knowledge."[543] Infrastructure to provide access is not enough. If individuals seek only like minded individuals, public discourse will likely become impoverished because dialogue which considers only one possible response to a particular civic problem is unlikely to generate imaginative solutions.

Overcoming physical barriers is important for groups that espouse views not held by the majority of the population. Previously disenfranchised groups may find new power through online organization and collaboration. More viewpoints may be expressed because of the ease of entry into the online dialogue. Even "trolling," or intentionally posting incendiary comments to message boards or email lists, is still potentially useful as a way to generate conversation on topics—if someone posts a diatribe against

---

[542] Alejandro Molina, "Cyberspace: The "Color Line" of the 21st Century," *Social Justice* 30, no. 2 (2003): 147.
[543] Ibid., 148.

Republicans on a Republican message board, it may generate discussion based on the content of the message. Haig Bosmajian explains that the heckler is an important element of civic discourse: "Although it may be more comfortable to silence the heckler, such action may be detrimental to the proper functioning of a democratic society."[544]

The shift to a digital persona has potential disadvantages. Fortunati argues that because of our reliance on ICTs, "beyond the remaining old poverty, which exists even in the industrialized nations, the new poverty that affects everybody is a *poverty of first-hand reality*."[545] Scholars disagree on the Internet's potential to isolate individuals. Robert Kraut, et al. found that "greater use of the Internet was associated with small, but statistically significant declines in social involvement as measured by communication within the family and the size of people's local social networks, and with increases in loneliness, a psychological state associated with social involvement. Greater use of the Internet was also associated with increases in depression."[546] But in a follow up study, Kraut, et al. found that for extraverts, Internet use generated greater community involvement and decreased loneliness but for introverts the reverse was true.[547] In accounting for the differences between the two studies, they suggest that the Internet may have changed in the intervening time: "Simply put, the Internet may have become a more hospitable place over time."[548] Eric Uslaner argues that "there is little evidence that the Internet will create new communities to make up for the decline in civic engagement that

---

[544] Haig A. Bosmajian, "Freedom of Speech and the Heckler," *Western Speech* 36, no. 4 (1972): 219.
[545] Fortunati, "The Human Body: Natural and Artificial Technology," 75.
[546] Robert Kraut et al., "Internet Paradox: A Social Technology That Reduces Social Involvement and Psychological Well-Being?," *The American Psychologist* 53, no. 9 (1998): 1028
[547] Robert Kraut et al., "Internet Paradox Revisited," *The Journal of Social Issues* 58, no. 1 (2002): 67.
[548] Ibid., 68.

has occurred over the past four decades in the United States. Yet, there is even less evidence that the Internet is pushing people away from traditional social ties or making them less trusting."[549]

Despite conflicting evidence, the conception of Internet induced isolation is a continually recurring theme for those considering identity and citizenship in an information society. Bakardjieva suggests that this isolation is not only a consequence of digital life: "The opposite of virtual togetherness is not 'real' or 'genuine' community, as the current theoretical debate suggests, but the isolated consumption of digitized goods and services within the realm of alienated private life."[550] Bakardjieva hints at something many scholars have argued: that a conflation between citizen and consumer is taking place.[551] Heejo Keum, et al. suggest that "consumer culture and civic engagement may be interconnected and mutually supportive rather than opposing, at least in the context of certain brand communities."[552] They note that consumption can be integrated in political action, citing examples such as anti-globalist and environmentalists who purchase goods in socially conscious ways.[553] Margaret Scammell explains, "It is no longer possible to cut the deck neatly between citizenship and civic duty, on one side, and consumption and self interest, on the other."[554] Citizenship and consumerism can be productively mixed

---

[549] Eric M. Uslaner, "Trust, Civic Engagement, and the Internet," *Political Communication* 21, no. 2 (2004): 239.
[550] Bakardjieva, *Internet Society: The Internet in Everyday Life*, 168.
[551] See Greg Dickinson, "Selling Democracy: Consumer Culture and Citizenship in the Wake of September 11," *The Southern Communication Journal* 70, no. 4 (2005): 271-84.
[552] Heejo Keum et al., "The Citizen-Consumer: Media Effects at the Intersection of Consumer and Civic Culture," *Political Communication* 21, no. 3 (2004): 370.
[553] Ibid., 370.
[554] Margaret Scammell, "The Internet and Civic Engagement: The Age of the Citizen-Consumer," *Political Communication* 17, no. 4 (2000): 352.

but there seems to be a shift away from civic participation and toward atomized actions performed by individuals.

The most significant disadvantage of the shift to a digital identity may be the loss of simplicity. In his discussion of Third World countries that have a per capita income of $295 per year, Martin asks:

> Why, in the remote parts of Nepal where you could not even take a jeep and where the income is among the lowest in the world, are the villagers humming with contentment, their faces unquestionably happier than the faces on the streets of New York? It has struck me time and again that the contented faces are in areas where there is no electronic communications. The people are happy with their lot because they do not know of any different way of life. They know their place in the hierarchy of their village, and their aspirations are to grow fat vegetables, to see their children grow up, and to be accepted in their community. They do not know that the United Nations classifies them as "developing." They live in well integrated communities where the patterns of life have been honed over the centuries.[555]

A sense of understanding the social order differentiates these societies from the information society. The advent of the information society has thrust world political actions into local consciousnesses. The world has become more complex and it seems increasingly difficult to keep up.

---

[555] Martin, *The Wired Society*, 266.

The Creators of Technology and Their Values: What Kind of Democracy Would Hackers Create?

In 1922, Walter Lippmann argued that modern society had become too complicated for the average citizen to make informed decisions and called for the bureaus of experts who could help leaders to sort through the confusion.[556] Shortly thereafter, Edward Bernays suggested that "ours must be a leadership democracy administered by the intelligent minority who know how to regiment and guide the masses. Is this government by propaganda? Call it, if you prefer, government by education."[557] Others have made similar arguments. Jordan states that "perhaps changes to governmental politics as part of cyberspace and informational societies are likely to come not from a populist source but from the technopower elite."[558]

Others argue that experts and technologists need not completely usurp power from the people, or even from the leadership. Clift describes the possibility that technologists may help to create a technological democracy: "We need a generation of civic technologists who engage the fundamental infrastructure of the Internet and standards processes in the public interest. We need talented people with an eye toward making the Internet a democracy network by nature."[559] But Lessig explains that the goal of creating a technological democracy through technologists is inherently flawed:

> Engineers write the code; the code defines the architecture, and the architectures define what is possible within a certain social space. No process of democracy

---

[556] See Lippmann, *Public Opinion*, 233-238.
[557] Edward L. Bernays, *Propaganda* (Brooklyn, NY: Ig Publishing, 2005), 127-128.
[558] Jordan, *Cyberpower: The Culture and Politics of Cyberspace and the Internet*, 165.
[559] Clift, "An Internet of Democracy," 31.

> defines this social space, save if the market is a process of democracy. This might not be so bad, assuming that there are enough places to choose from, and given that it is cyberspace, the places to choose from could be many, and the costs of exit are quite low. Even so, note the trend: the progression away from democratic control. We will stand in relation to these places as we stand in relation to the commodities of the market: one more place of unending choice; but one less place where we, collectively, have a role in constructing the choices that we have.[560]

The technologists of tomorrow are the hackers of today and hackers do not possess the civic-mindedness described by Clift. Although some values of the hacker movement are amicable to democracy in an information society—such as the advocacy of freedom of information and access to information systems—other core values and elements of hacker identity are at odds with the democratic ideals of voice, citizenship, and limitation of government power. Only hackers would have a voice, leadership and citizenship would extend only to hackers, and ignorance on the part of the populace would allow for unlimited power for the hackers. Hacker identity is elitist, fragmented, and based on a meritocracy of skills. The notion of peership is important to hackers and is based on skill alone. Manuel Castells points out, "Only hackers can judge hackers. Only the capacity to create technology (coming from any context), and to share it with the community, are respected values. For hackers, freedom is a fundamental value, particularly freedom to access their technology, and use it as they see fit."[561] The key word in this passage is *their* technology. The kind of citizenship that hackers would

---

[560] Lessig, "The Zones of Cyberspace," 1410.
[561] Castells, *The Internet Galaxy: Reflections on the Internet, Business, and Society*, 60.

create illustrates how Touraine's notion of citizenship is not sufficient. For democracy to flourish, one must not only consider oneself to be a citizen and act accordingly—one must also grant this ability to other citizens.[562] But for hackers, the only way to become a citizen would be to become a hacker, which, for the majority of the population, is out of reach.

In their collective worldview, hackers seem to position themselves as a modern-day version of Plato's guardians, complete with the "noble lie."[563] Hackers hold both the power of society and the key to the myth. In this case, the noble lie is not a creation myth but a myth concerning knowledge—hackers perpetuate the myth that people are unable to understand technological systems. In the Hacking For Girliez hack of the *New York Times*, the idea that the average person is incapable of examining code is reinforced. "The Conscience of a Hacker" explains that the hacker is not like other people—they are vastly more intelligent and skilled. But the key difference between Plato's guardians and hackers is that the guardians understood that the noble lie was a myth. For hackers, the myth has become reified to the extent that hackers now believe the myth too. In order to break the hold of this myth on society, we must "desacralize technique."[564]

But the process of demystifying technology is easier said than done. Our technological systems seem to favor a "black box" aesthetic, concealing the inner workings in the name of convenience and ease of use. Langdon Winner argues that this is

---

[562] For more on Touraine's notion of citizenship and its place in democracy, see Touraine, *What Is Democracy?* 64-73.
[563] For more on Plato's use of the noble lie as a way to keep the masses in order, see Plato, "Republic," 414c-415c.
[564] See Ellul, "Technology and Democracy," 48.

by design: "One does not want to bother with its structure or the principles of its internal workings. One simply wants the technical thing to be present in its utility. . . . Technology, then, allows us to ignore our own works. It is a license to forget."[565] In other words, it seems that individuals *want* technology to remain obscured. Winner explains that "the desire for access to the 'black boxes' produced by technology, therefore, does not imply a desire for access to the inner workings of the technology itself. One becomes accustomed to the idea that systems are too large, too complex, and too distant to permit all but experts an inside view."[566] It is not only hackers who believe that the common person is ill equipped to handle technology—the common person believes this as well.

That this sentiment is held by both technologists / hackers and the population at large does not bode well for the prospects of a technologically enhanced democratic society. Individuals need to have at least a basic understanding of the technologies used to enhance democratic activities. For example, certain voting machines have been called into question because of possible system insecurities and the ability for hackers to modify the vote tallies.[567] Without an understanding of the limitations of these machines, citizens are ill-equipped to make decisions concerning the adoption of a particular machine, or if machines should be adopted at all.

---

[565] Langdon Winner, *Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought* (Cambridge, MA: MIT Press, 1977), 315.
[566] Ibid., 288.
[567] See Michael A. Carrier, "Vote Counting, Technology, and Unintended Consequences," *St. John's Law Review* 79, no. 3 (2005): 645-87; Zachary Goldfarb, "As Elections near, Officials Challenge Balloting Security; in Controlled Test, Results Are Manipulated in Florida System," *The Washington Post*, January 22, 2006; Marc L Songini, "Maryland House Votes to Oust Diebold Machines," *Computerworld*, March 13, 2006.

The prognosis for a technological democracy may seem bleak. Hackers view the masses as technological idiots, incapable of understanding even basic technologies. More importantly, hackers are not interested in informing the masses. Hackers seem to see themselves as not only more intelligent, but better than the rest of society. This is not a question of what would happen if the hackers ruled the cyberworld—they already do. This is the core reason that society as a whole cannot look to cyberspace for liberation. The analog world exists with a power structure built on class and economic status. In the digital world, the power structure is built on technological knowledge. Those who wield power in the analog world will continue to enjoy access to knowledge for a period of time but their time of power is waning. If the current trend continues unchecked, we may soon witness the eclipse of their power because hackers do not require the same resources as those necessary in the analog world.

But the notion that hackers will rule the digital world is not entirely deterministic because innovation is not exclusive to hackers. People have a knack for creating unintended uses for technology. An old adage goes, “when the only tool you have is a hammer, all of your problems look like nails.” The converse is also true—when all your problems are nails, every tool looks like a hammer. Many of us have used a wrench or a screwdriver as a hammer. Although this may seem trivial, it illustrates the point that people are not tied to particular uses of technology. People use technologies to meet their needs in ways unanticipated by the inventor, producer, or marketer. For example, Marjorie Kibby and Brigid Costello describe how individuals use CU-SeeMe, originally developed at Cornell University as a video conferencing program, to create private

networks of interactive sexual entertainment.[568] Technology is not simply the program or the technological artifact. Ellul uses the term *technique*, which includes not only the artifacts but the ways in which they are used.[569] Because innovation is not exclusive to the technologists or to the hackers, society may yet succeed in demystifying technology. What may save society from the hackers is that all of us, in some small way, share some hacker tendencies.

New Means of Protest

Innovations in technique tend to spread and this is also the case in social movement protest activities.[570] With the widespread use of the Internet, new forms of protest and political action are emerging. These forms are being used by social movement activists and institutionalized political parties. For example, the Dean for America campaign made extensive use of blogs as a way to disseminate their message and rally support.[571] Other developments include wardriving, message boards, newsgroups, and datamining for political causes.[572] Bakardjieva explains that "citizens seem to want their voices heard and taken into account now through the new functionalities of the Internet.

---

[568] Marjorie Kibby and Brigid Costello, "Between the Image and the Act: Interactive Sex Entertainment on the Internet," *Sexualities* 4, no. 3 (2001): 353-69.
[569] For more on Ellul's conception of technique, see Jacques Ellul, *The Technological Society*, trans. John Wilkinson (New York: Vintage Books, 1964), 13-22.
[570] See Doug McAdam and Dieter Rucht, "The Cross-National Diffusion of Movement Ideas," *The Annals of the American Academy of Political and Social Science* 528 (1993): 56-74.
[571] See Matthew R. Kerbel and Joel David Bloom, "Blog for America and Civic Involvement," *Harvard International Journal of Press/Politics* 10, no. 4 (2005): 3-27.
[572] See Jenine Abboushi Dallal, "Hizballah's Virtual Civil Society," *Television & New Media* 2, no. 4 (2001): 367-72; Howard, "Deep Democracy, Thin Citizenship: The Impact of Digital Media in Political Campaign Strategy"; Kahn and Kellner, "New Media and Internet Activism: From the 'Battle of Seattle' to Blogging."

This suggests that there is indeed a democratic potential in the Internet—its capacity to galvanize response and to conduct it back to previously one-way transmitters of powerful discourse. However, in order for that potential to start materializing, innovative social and political interfaces between citizens and political institutions should be imagined and implemented to match the technical interface already in place."[573]

Many of these strategies seem to be little more than new ways of enacting traditional means of protest. Hacktivist groups such as the electrohippies refer to denial of service attacks as "virtual sit-ins" and database integration and datamining seems similar to J. Michael Hogan's description of the New Right's direct mailing campaign to defeat the Panama Canal treaties using Richard Viguerie's refined, specialized mailing lists.[574] Although these techniques build on old strategies, the core difference seems to be a matter of scale. With the advent of new communication technologies, Viguerie's database of 30 million Americans seems almost paltry. In one security breach alone, CardSystems, a credit card processing company, improperly kept data, resulting in 40 million credit card numbers being compromised.[575] In the information age, not only mailing lists, but credit information, personal financial transactions, viewing habits, and personal data are compiled, bought, sold, and used.

These information systems can be used for many ends and not all of them encourage democratic practice. More pervasive information systems do not inevitably

---

[573] Bakardjieva, *Internet Society: The Internet in Everyday Life*, 128.
[574] See J. Michael Hogan, *The Panama Canal in American Politics: Domestic Advocacy and the Evolution of Policy* (Carbondale: Southern Illinois University Press, 1986), 120-126.
[575] See Dash, "Lost Credit Data Improperly Kept, Company Admits"; Sutton, "Security Breach Exposes Holes in Credit Card System."

lead to more freedom. James Martin argues that "America has generally had the world's best telecommunications. Totalitarian governments have generally had the worst. To maximize the chance of freedom tomorrow, we should build the greatest diversity of information channels today."[576] But John Negroponte points out that "for a long time, decentralization was plausible as a concept but not possible as an implementation. The effect of fax machines on Tiananmen Square is an ironic example, because newly popular and decentralized tools were invoked precisely when the government was trying to reassert its elite and centralized control. The Internet provides a worldwide channel of communication that flies in the face of any censorship and thrives especially in places like Singapore, where freedom of the press is marginal and networking ubiquitous."[577]

There is still democratic potential in these technologies—but this potential can be realized only through the human element rather than though the technologies themselves. Bakardjieva states, "Naïve hopes for a technologically mediated direct democracy aside, it can still be argued that there is room for more imaginative forms of two-way communication between citizens and institutions. A whole new practice of Internet-based *participatory public relations* can be imagined if citizens' interests, and not solely institutional agenda, are taken as cues."[578] But who determines citizen interests? Bakardjieva seems to believe that the Internet can somehow overcome the agenda-setting

---

[576] Martin, *The Wired Society*, 248.
[577] Negroponte, *Being Digital*, 158.
[578] Bakardjieva, *Internet Society: The Internet in Everyday Life*, 194.

function of the mass media, even as the Internet becomes more integrated with traditional forms of mass media.[579]

The real democratic potential for new media seems to lie not in the ability to transcend corporate or institutional agenda-setting, but through a more fundamental transformation of the public sphere. In her study of chat room discourse, Bakardjieva found that "what was actually happening in this [chat room] environment was that people were meeting previously anonymous strangers and treating them as someone 'like myself,' someone who could laugh at the same jokes, talk about the same topics of interest and then walk away and go on with his or her own life."[580] Sennett argues that we live in a culture of intimacy, in which we must know the character of the person. This short circuits the ability to function in public as if we were strangers, making men and women, not measures, the guiding concern. For Sennett, "The extent to which people can learn to pursue aggressively their interests in society is the extent to which they learn to act impersonally."[581] Jürgen Habermas noted that although this ideal public sphere was not necessarily realized, it was, nevertheless, the ideal.[582] This is the great promise of information technologies such as the Internet—the ability to transcend corporeality and judge one another on the merits of the ideas presented. In other words, through new communication technologies we can make the ideal public sphere a reality.

---

[579] For more on the agenda setting function of the mass media, see McCombs and Shaw, "The Agenda-Setting Function of Mass Media."
[580] Bakardjieva, *Internet Society: The Internet in Everyday Life*, 175.
[581] Sennett, *The Fall of Public Man*, 349.
[582] Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*, 36.

But Sennett points out that this potential for a mediated public sphere must be considered in the context of our culture of intimacy: "The mass media infinitely heighten the knowledge people have of what transpires in the society, and they infinitely inhibit the capacity of people to convert that knowledge into political action."[583] Simply putting technological structures in place will not invigorate the public sphere without a change in culture. Current research in mediated identities suggests that this cultural shift may be taking place.[584]

The population is changing and there is potential for a new public sphere modeled on the ideals set forth by Habermas and Sennett. Still, one is left with the question, "if these technologies simply build on previous strategies, what is new in digital protest?" Of the recent attempts to bridge technology, protest, and democratic practice, vote swapping and the formation of "smart mobs" seem particularly noteworthy.

Howard Rheingold describes how individuals can be brought together as "smart mobs" through a mixture of technologies such as mobile phones, wireless Internet, text messaging systems, and blogging. According to Rheingold, "Smart mobs consist of people who are able to act in concert even if they don't know each other. The people who make up smart mobs cooperate in ways never before possible because they carry devices that possess both communication and computing capabilities."[585] In one striking

---

[583] Sennett, *The Fall of Public Man*, 283.

[584] See Costello, Lenholt, and Stryker, "Using Blackboard in Library Instruction: Addressing the Learning Styles of Generations X and Y"; Leung, "Impacts of Net-Generation Attributes, Seductive Properties of the Internet, and Gratifications-Obtained on Internet Use"; Leung, "Net-Generation Attributes and Seductive Properties of the Internet as Predictors of Online Activities and Internet Addiction"; Tapscott, *Growing up Digital: The Rise of the Net Generation*; Weiler, "Information-Seeking Behavior in Generation Y Students: Motivation, Critical Thinking, and Learning Theory."

[585] Howard Rheingold, *Smart Mobs: The Next Social Revolution* (Cambridge, MA: Perseus, 2002), xii.

example, Rheingold describes President Joseph Estrada of the Philippines, who had just had his impeachment proceedings abruptly stopped by supporters, as "the first head of state in history to lose power to a smart mob. . . . Tens of thousands of Filipinos converged on Epifanio de los Santas Avenue, known as 'Edsa,' within an hour of the first text message volleys: 'Go 2EDSA, Wear blck.' Over four days, more than a million citizens showed up, mostly dressed in black. Estrada fell. The legend of 'Generation Txt' was born."[586] The diffusion of mobile technologies such as cellular phones, wireless internet, text message systems (SMS) and interconnected devices such as personal digital assistants (PDA) and global positioning system (GPS) units allow groups to function as united bodies, especially when combined with websites generating RSS (Really Simple Syndication) feeds which provide constantly updated information from a centralized location.

These technologies are important when opposing a militarized police force equipped with tactical communication systems. Using these technologies, protestors could employ the following scenario. A website announces the site of a protest, but this news is also spread through social networks via phone or SMS. When protestors arrive at the protest, they receive RSS feeds from a centralized computer, advising them of conditions. Laptop users onsite update this RSS feed in real time, based on changing conditions. If police are launching tear gas grenades, depending on the tactics of the protest, the feed could advise protestors to avoid that area or to swarm the area and

---

[586] Ibid., 157-158.

retaliate. Protestors would document the action through video cameras and video devices on their cellular phones, which are then uploaded in real time to a central computer.

Although the end result of such a scenario—physical protest—is similar to previous social movement action, the means by which it is conducted and organized have become more efficient, more tactical. These technologies present great potential for social movement activities. But the technology is not only shaping the means by which protest is conducted, it is changing the protestors: "Online activist subcultures have materialized as a vital new space of politics and culture in which a wide diversity of individuals and groups have used emergent technologies in order to help to produce new social relations and forms of political possibility."[587] As technological activist subcultures evolve, there is a greater possibility for technological innovation and more inventive strategies of protest.

Vote swapping is another innovation that shows promise, allowing individual citizens to protest within institutionally accepted structures. When Al Gore lost the 2000 presidential election, some Democrats blamed the supporters of Ralph Nader. Nader's goal was not to become president, but to gain five percent of the popular vote in order for the Green Party to receive federal matching funds for their election activities. These Nader voters would have likely voted for Gore instead of Bush, and in some states, the race was very close. Nader supporters did not want Bush to win, but also wanted Nader to gain five percent of the popular vote. The solution was a novel one—a Gore supporter in a state where Gore was projected to easily win promised to vote for Nader in their

---

[587] Kahn and Kellner, "New Media and Internet Activism: From the 'Battle of Seattle' to Blogging," 94.

elections if a Nader supporter in a "battleground" state voted for Gore. Marc Randazza explains that this strategy is nothing new in politics: "On Capitol Hill, members of Congress routinely support their colleagues' bills in exchange for support for their own. This coalition building was never before a practical issue in presidential electoral politics because of the logistical impossibility of creating a citizen vote-swap on a scale that could have any significant impact. Enter the Internet, and enter the freak circumstances of the 2000 presidential race."[588] Government officials stepped in and shut down some of the vote swapping websites, which created a chilling effect for similar sites.[589] The vote swapping phenomenon resurfaced during the 2004 presidential campaign.

Although vote swapping has not gained widespread popularity in the United States, this strategy has gained traction in the United Kingdom and has been credited with altering the outcomes of parliamentary elections:

> So did it work? Again, like most aspects of voter research it's impossible to be definitive; but tactical voting enthusiasts do point to two outcomes with particular glee. In Cheadle, Cheshire, www.tacticalvoter.net received 47 vote-swapping pledges from voters and the Conservative MP lost by 33 votes; in Dorset South 185 vote-swapping pledges were received and the sitting Conservative lost by 153. None of which proves anything but the fact that the Conservative party filed complaints against tactical voting sites both to the data protection commissioner

---

[588] Marc J. Randazza, "The Forgotten Electoral Controversy," *Intermedia* 29, no. 2 (2001): 34.
[589] See Lynda Gledhill, "California Shuts Down Vote-Trader Web Site / Secretary of State Calls Such Swaps Illegal," *San Francisco Chronicle*, October 31, 2000; Randazza, "The Forgotten Electoral Controversy."

and the electoral commission indicates that they at least were far from sanguine about the process.[590]

Both of these strategies illustrate the potential for technology to enable innovation in social movement activities and democratic practice but citizen activity is still required. Vote swapping does nothing for a citizen who does not vote. New communication technologies do little for protestors who cannot afford them. Technology alone cannot overcome citizen apathy or material constraints. Even so, these innovations demonstrate some of the ways that activists and citizens have helped shape the current landscape of democratic practice.

The Potential Efficacy of Hacktivism

In his discussion of Critical Art Ensemble, Wray states, "Electronic Civil Disobedience is seen as imperative by these writers, not only because of the proliferation and importance of computer technology, but also because traditional forms of civil disobedience have become less and less effective. The streets, they say, have become the location of dead capital. To seriously confront capital in its current mobile, electronic form, resistance must take place in the location where capital now exists in greatest concentrations, namely in cyberspace."[591] But how effective is electronic civil disobedience as a method of inducing democratic practice? Wray explains, "If the desired goal of ECD is to draw attention to particular issues by engaging in actions that are

---

[590] Ivor Gabe, "New Media: E-Lection Gets the Vote: Almost Three Million People Used Email or the Internet to Join in the General Election Campaign," *The Guardian*, July 30, 2001.
[591] Wray, "On Electronic Civil Disobedience," 109.

unusual and will attract some degree of media coverage, then these actions have a high degree of effectiveness. If, however, effectiveness is measured by assessing the action's ability to catalyze a more profound mobilization of people, then probably these new techniques are not effective. . . . Electronic civil disobedience is not likely to be an organizing tool, and the end result of the ECD is not likely to be an increase in the ranks of the disaffected. Rather ECD appears to be a means to augment or supplement existing organizing efforts, a way to make some noise and focus attention."[592]

Although it may be a way to gain attention, electronic civil disobedience is not necessarily an effective way to keep attention. In 1998, the Electronic Disturbance Theater used a program called Floodnet to engage in politically motivated denial of service attacks on behalf of the Zapatista movement in Mexico.[593] Although the Zapatista movement is still functioning and online, other concerns have eclipsed their cause in the public mind. Other actions, such as the hack of the *New York Times*, may have gained attention, but it seemed to do little to further the goals of the "Free Kevin Mitnick" campaign.

For hacktivism to be effective, it needs to have some kind of resonance for both the public and the media. More importantly, it must have an analogue counterpart. The Filipino protests that drove Joseph Estrada out of the presidency would not have had the same effect had text messaging simply been used to denounce the president. A denial of service attack on government servers may prove temporarily effective in attracting media attention, but it is too easy to denounce the action as the work of terrorists or "the

---

[592] Ibid., 110.
[593] Ibid.

enemies of freedom" or to dismiss the action as the work of a few individuals. In contrast, the physical assembly of millions of citizens sends an unmistakable message that the movement is supported by a large number of citizens.

The ephemeral nature of the Internet necessarily constrains the duration of social movement actions: websites move, domain names change, servers can be added to combat denial of service attacks. The electrohippies may have temporarily overwhelmed the WTO's servers, rendering their website inaccessible, but this result was short lived. Moreover, the effect was not very dramatic because the denial of service attack created an absence, rather than a *presence*. As such, there was little to remain in the collective memory concerning the event. The public has forgotten the denial of service attack, but they still remember anarchists breaking windows and the violence that erupted. When virtual protests work in tandem with physical protest, the physical aspects will likely overshadow the virtual ones.

That which is used by protest activities can often be co-opted by the state and corporate interests or used for criminal activities. With enough properly configured servers, any organization could avoid the denial of service attacks that the electrohippies successfully implemented against the WTO's servers. Organizations are not immune from similar attacks, but such attacks are taking place by different means and for different ends. For example, some hackers have begun threatening online gambling websites with denial of service attacks unless the owner pays for protection.[594] In these

---

[594] See "Gamblers Get $1.9 Million in Winnings in One Case as Hackers Scam Net Casinos," *Wall Street Journal*, September 11, 2001; Jon Swartz, "Online Betting Sites Fight Cyberextortion; Owners Hope Tightened Security Thwarts Hackers," *USA TODAY*, March 9, 2004.

cases of "hackstortion," hackers amass large "zombie networks" through the use of spyware that allows for remote control of the machine.[595] If needed, the hacker calls upon this legion of unwitting accomplices and targets the site. Architecturally, this is similar to the electrohippies' distributed denial of service attacks, but with an important difference—the participants may never know that they had taken place in attacking an online casino or other website.

Hacktivism may become an integral part of future social movement activities, but it seems unlikely until hacktivists find a way to make actions relevant and memorable to the general public. The electrohippies' attempt to make hacktivism more participatory and democratic is a step in the right direction. By making hacktivist techniques available to the general public, the electrohippies provide a way for individuals to actively participate in protest action without leaving their homes and dispel some fear of the hacker by allowing non-hackers to use the tools of the hacker for a noble purpose. By allowing common citizens to take part in a hacktivist action, the electrohippies weaken the us/them distinction often found in hacker discourse and the news media. This bridge between "us" and "them" is an essential component for making hacktivism relevant to the general public.

---

[595] Spyware is often bundled with other programs. For example, a person could download a program that displays current weather information on their desktop, but included in the installation of the program are several other programs that the user has not chosen to install. These "hidden" programs may track the user's Internet surfing or gather other data about the user. This information is then transmitted to a server and retrieved by the company or person that manages the program. Often, the end user does not realize that his or her computer is infected with spyware. Keyloggers are programs that have the ability to record every keystroke that the user makes, which can reveal such things as passwords and credit card numbers. Tracking programs gather a detailed history of the user's Internet surfing, recording, for example, sites that the user has visited and for how long.

The Potential for Democratic Practice in an Information Society

It is possible to identify some of the overarching trends that have manifested themselves in the quarter century since the advent of personal computers became widely available and significantly altered the American social landscape. The question at hand remains: How can technology help to enable a more democratic society? Technology is not the determining factor here—rather, it is merely an enabling factor. As Lynn White Jr. eloquently writes, "A new device merely opens a door; it does not compel one to enter."[596] Technology cannot create a more or less democratic society; people create a more or less democratic society.

The answer to the question of how technology can help to enable a more democratic society can be found in how citizens view technology and their relationship to the state, other institutions, and each other. The advent of the information age may seem to have opened Pandora's Box, but the concerns surrounding democratic practice in an information society are as old as civilization. Issues of ownership, self-determination, and information access compete with public good, government control, and privacy. Such tensions will not magically disappear with technological advances because human nature lies at the heart of these problems. Rather than eliminate these tensions, technology brings them to the forefront. For example, the recording industry laments the explosion of music piracy through the use of peer-to-peer software. But piracy is nothing new—it is just more obvious now. Technologies and their use reflect core values within our society.

---

[596] Lynn White, Jr., *Medieval Technology and Social Change* (Oxford: Clarendon Press, 1962), 28.

This study examines only one side of the equation concerning how technology may influence democratic practice. On one side, there are the values and beliefs held by the creators of the technology. On the other side, there are the values and beliefs of those who use the technology. The values held by the individual users of technology are varied, but it is possible to note some of the larger trends as society evolves. For instance, widespread piracy through peer-to-peer software and disregard for copyright laws display how society's view of information may be shifting. A large percentage of the population may not recognize the relevance of copyright. This has been facilitated by the mass media. When we turn on our television set, our radio, or connect to the Internet, we expect to see or hear content that is free. When I worked for Excite@Home, the strategy for the Excite side was to bring people to the site for the personalized content in order to boost advertisement revenue. Even on the @Home side, where I worked, we created and licensed content to demonstrate the value of a broadband Internet connection. In other words, the content wasn't what you paid for—instead, you paid for the medium by which you got the content. On the Excite side, the content is what brought "eyeballs" to the site, which allowed for increased advertising dollars. On both sides of the business—the strictly web-based and the hardware based—content was given away for free. Radio and television follow a similar model, where content is given away mainly through the support of advertisers. A hit show brings in the largest quantity of potential consumers. People are now accustomed to receiving content for free—if only we could eliminate the commercials! The current model has gone on for so long that the whole mechanism has been reified—the connection between commercials and free content has been forgotten. New technologies such as peer-to-peer and TiVo allow people to hear the other songs on

the album instead of just the single that was released for radio airplay and watch television at their leisure without commercial interruption. People still buy compact discs and DVDs, but it is the packaging of the content rather than the content itself that they purchase.

The direction that society seems to be heading in its view of information is demonstrated by the ideas of access and privacy. This is one of the fundamental paradoxes in the information society: people want both access to information (even about other people, such as celebrities) *and* privacy. Privacy and access to information are both core elements of our conception of democracy, but the information required for citizens should be public information. Sennett explains that in the current culture of intimacy, citizens feel that they need to know about the person that they vote for; in other words, individuals believe that they need private information in order to make public decisions.[597] But this surveillance goes both ways—while citizens are watching their leaders, leaders are watching the citizens. Martin points out that "the problem with 'privacy' is its conflict with other social values, such as competent government, a free press, protection against crime, health care, provision of services, collection of taxes, social and medical research, and the development of community living environments. The authority providing each of these wants to decide what it should know about us and when it should be told. We, on the other hand, resent the intruding official eye."[598] Yaman Akdeniz also illustrates the tension between individual and government views of anonymity. Akdeniz argues that although law enforcement agencies often frame

---

[597] Sennett, *The Fall of Public Man*, 284-287.
[598] Martin, *The Wired Society*, 250.

anonymity as a way to protect criminal activity, anonymity is an essential component for free speech, allowing for open expression of ideas and such activities as allowing dissidents to speak out concerning human rights abuses in oppressive regimes.[599] This is consistent with Richard Sennett's argument that one reason the public sphere has diminished is because citizens are no longer able to interact *as strangers* concerning public issues.[600]

Governments have made concessions, recognizing that there can, and must, be a middle ground between the interests of the state and the interests of the citizen. One example of this is the doctrine of fair use in copyright law. TyAnna Herrington explains that there is a relationship between fair use, the First Amendment and freedom of expression, noting that the free expression of ideas is essential in order to have a functioning democracy. She argues that "the interdependent nature of fair use and free speech makes strong fair use protections necessary to a healthy First Amendment."[601] Even so, since her article was written, legislation such as the Digital Millennium Copyright Act (DMCA) and the Copyright Term Extension Act has continued to erode the public domain and fair use. Here we can see the emergence of another form of individual rights with the rise of the transnational corporation. Although such legislation ostensibly protects artists and copyright holders, many citizens do not realize that the majority of intellectual property is not controlled by those who create the information, but

---

[599] Akdeniz, "Anonymity, Democracy, and Cyberspace."
[600] Sennett, *The Fall of Public Man*.
[601] TyAnna K. Herrington, "The Interdependency of Fair Use and the First Amendment," *Computers and Composition* 15, no. 2 (1998): 141.

by corporations. In this way the state can provide the illusion of protecting individual freedoms while simultaneously eliminating other freedoms.

The relationship between the state, corporate interests, non-governmental organizations, and individual citizens is one that has yet to be completely resolved. Although technology complicates these relationships even further, it has a role to play in the future of democratic practice. To understand where technology is driving us, we must recognize that living, breathing human beings are behind the wheel. Many of these individuals are hackers, and the collective identity of the hacker movement is by and large incongruent with the tenets of democracy. But this does not doom technology to a future of reproducing the values of elitism and division. Individuals have an uncanny knack for finding unintended uses of technologies and some of these uses have great potential to promote democratic practice, especially when used in the context of social movement protest. The great hope for a technologically enhanced democracy is not the hacker with the tools of hacktivism. Rather, hope seems to come from common citizens who adapt technology to political ends in new and inventive ways that the technologists had not anticipated. This is possible because everyone has some of the core tendencies of the hacker—curiosity, a passion for an elegant solution, and the will to push the limits just a bit further. So long as society embraces the uncertainty inherent in such behavior and resists the urge to resort to the certainty of order and conformity, our technological creations may yet prove to be the salvation of our most precious social creation: democracy.

Bibliography

2600. December 29, 1996. "The Air Force: Hacked Webpage." http://www.2600.com/hackedphiles/airforce/hacked_af/www_af_mil.html (accessed February 3, 2006).

2600. September 14, 1998. "2600 | Slashdot." http://www.2600.com/hackedphiles/slashdot/ (accessed March 27, 2006).

2600. April 1, 2005. 2600 Meetings Today - Formal Attire Required. http://www.2600.com/news/view/article/2200 (accessed March 27, 2006).

Abbott, Edwin Abbott. *Flatland: A Romance of Many Dimensions*. 5th , rev. ed. New York: Barnes & Noble, 1963.

Akdeniz, Yaman. "Anonymity, Democracy, and Cyberspace." *Social Research* 69, no. 1 (2002): 223-37.

Albin, Leslie, and Jester Sluggo. "Centrex Renaissance: 'The Regulations.'" *Phrack* 1, no. 4 (March 13, 1986): phile 7.

Aljalian, Natasha N. "Fourteenth Amendment Personhood: Fact or Fiction?" *St. John's Law Review* 73, no. 2 (1999): 495-540.

Allen, Rod, and Nod Miller. "Panaceas and Promises of Democratic Participation: Reactions to New Channels, from the Wireless to the World Wide Web." In *Technology and in/Equality: Questioning the Information Society*, edited by Sally Wyatt, Flis Henwood, Nod Miller and Peter Senker, 46-60. London: Routledge, 2000.

Althusser, Louis. *Lenin and Philosophy and Other Essays*. Translated by Ben Brewster. New York: Monthly Review Press, 1971.

Andersen, Hans Christian. "The Emperor's New Suit." In *The Complete Hans Christian Andersen Fairy Tales*, edited by Hans Christian Andersen and Lily Owens, 438-41. New York: Chatham River Press, 1984.

Anderson, Jon W. "New Media, New Publics: Reconfiguring the Public Sphere of Islam." *Social Research* 70, no. 3 (2003): 887-906.

Applbaum, Arthur Isak. "Failure in the Cybermarketplace of Ideas." In *Governance.Com: Democracy in the Information Age*, edited by Elaine Ciulla Kamarck and Joseph S. Nye, 17-31. Washington, DC: Brookings Institution Press, 2002.

Aristotle. “Politics.” In *The Complete Works of Aristotle: The Revised Oxford Translation*, edited by Jonathan Barnes, 1986-2129. Princeton: Princeton University Press, 1984.

Asen, Robert. “A Discourse Theory of Citizenship.” *The Quarterly Journal of Speech* 90, no. 2 (2004): 189-211.

Babcock, Brian. *Cyborgs and Nomads: A Vision of Identity for the Information Age*. Stanford, CA: Humanities Honors Program, Stanford University, 2001.

Bakardjieva, Maria. *Internet Society: The Internet in Everyday Life*. London: Sage, 2005.

Bandura, Albert. “Social Cognitive Theory of Mass Communication.” In *Media Effects: Advances in Theory and Research*, edited by Jennings Bryant and Dolf Zillmann, 121-53. Mahwah, NJ: Lawrence Erlbaum Associates, 2002.

Barlow, John Perry. 1996. “A Declaration of the Independence of Cyberspace.” http://homes.eff.org/~barlow/Declaration-Final.html (accessed July 26, 2005).

Barnlund, Dean C., and Franklyn Saul Haiman. *The Dynamics of Discussion*. Boston: Houghton Mifflin, 1960.

Barnouw, Erik. “New Look.” In *Conglomerates and the Media*, edited by Patricia Aufderheide, Erik Barnouw, Richard M. Cohen, Thomas Frank, Todd Gitlin, David Lieberman, Mark Crispin Miller, Gene Roberts and Thomas Schatz, 15-29. New York: New Press, 1997.

Baudrillard, Jean. *Simulacra and Simulation*. Translated by Sheila Faria Glaser. Ann Arbor: University of Michigan Press, 1994.

Bekkers, Victor J. J. M., and Hein P. M. Van Duivenboden. “Democracy and Datacoupling.” In *Orwell in Athens: A Perspective on Informatization and Democracy*, edited by Wim B. H. J. van de Donk, I. Th M. Snellen and P. W. Tops, 213-23. Amsterdam: IOS Press, 1995.

Bell, Al. “Blue Box Is Linked to Phone Call Fraud.” *Youth International Party Line*, July 1971, 1.

Bell, Daniel. *The Coming of Post-Industrial Society: A Venture in Social Forecasting*. Special anniversary ed. New York: Basic Books, 1999.

Benford, Robert D, and David A Snow. “Framing Processes and Social Movements: An Overview and Assessment.” *Annual Review of Sociology* 26 (2000): 611-39.

Benford, Robert D. “Frame Disputes within the Nuclear Disarmament Movement.” *Social Forces* 71, no. 3 (1993): 677-701.

Benson, Thomas W. “Rhetoric as a Way of Being.” In *American Rhetoric: Context and Criticism*, edited by Thomas W. Benson, 293-322. Carbondale: Southern Illinois University Press, 1989.

Benson, Thomas W., and Bonnie Johnson. “The Rhetoric of Resistance: Confrontation with the Warmakers, Washington D.C., October 1967.” *Today’s Speech*, 16 (September 1968): 35-42.

Bentham, Jeremy. *Panopticon; or, the Inspection-House: Containing the Idea of a New Principle of Construction Applicable to Any Sort of Establishment, in Which Persons of Any Description Are to Be Kept under Inspection: And in Particular to Penitentiary-Houses, Prisons, Houses of Industry ... And Schools: With a Plan of Management Adapted to the Principle: In a Series of Letters, Written in the Year 1787*. London: T. Payne, 1791.

Berger, Peter L., and Thomas Luckmann. *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*. New York: Anchor Books, 1966.

Berman, Jerry, and Daniel J Weitzner. “Technology and Democracy.” *Social Research* 64, no. 3 (1997): 1313-19.

Bernays, Edward L. *Propaganda*. Brooklyn, NY: Ig Publishing, 2005.

Bernd, Joseph L., and Lynwood M. Holland. “Recent Restrictions Upon Negro Suffrage: The Case of Georgia.” *The Journal of Politics* 21, no. 3 (1959): 487-513.

Beveren, John Van. “A Conceptual Model of Hacker Development and Motivations.” *Journal of E-Business* 1, no. 2 (2001): 1-9.

Bijker, Wiebe E., Thomas Parke Hughes, and T. J. Pinch, eds. *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Cambridge, MA: MIT Press, 1987.

Bimber, Bruce A. *Information and American Democracy: Technology in the Evolution of Political Power*. Cambridge: Cambridge University Press, 2003.

Black, Edwin. “The Second Persona.” *Quarterly Journal of Speech* 56 (1970): 109-19.

Blackwell, Rob. “Treasury Exec: Banks Face New Cyber Enemies.” *American Banker*, September 9, 2004, 3.

Bloodaxe, Erik. “Introduction.” *Phrack* 4, no. 42 (March 1, 1993): file 1.

Bogard, William. *The Simulation of Surveillance: Hypercontrol in Telematic Societies*. New York: Cambridge University Press, 1996.

Booth, Wayne C. *The Rhetoric of Fiction*. Chicago: University of Chicago Press, 1961.

Bosmajian, Haig A. "Defining the 'American Indian': A Case Study in the Language of Suppression." *The Speech Teacher* 21, no. 2 (1973).

———. "Freedom of Speech and the Heckler." *Western Speech* 36, no. 4 (1972): 218-32.

———. "Obscenity and Protest." *Today's Speech* 18 (1970): 9-14.

Bowden, Mike (Agenta Aka Agent 005). "An Interview with Agent Steal." *Phrack* 4, no. 44 (November 17, 1993): file 16.

Braman, Sandra, and Stephanie Roberts. "Advantage ISP: Terms of Service as Media Law." *New Media & Society* 5, no. 3 (2003): 422-48.

Branwyn, Gareth. "Introduction: Hackers: Heroes or Villians?" In *Secrets of a Super Hacker* by The Knightmare, i-vi. Port Townsend, WA: Loompanics Unlimited, 1994.

Bray, Anne. "The Community Is Watching, and Replying: Art in Public Places and Spaces." *Leonardo* 35, no. 1 (2002): 15-21.

Brokaw, Tom. "The Laws Governing Credit Card Fraud." *Phrack*, no. 16 (September 19, 1987): file 5.

Burgess, Parke G. "The Rhetoric of Moral Conflict: Two Critical Dimensions." *Quarterly Journal of Speech* 56, no. 2 (1970): 120-30.

Calhoun, Craig. "Social Theory and the Politics of Identity." In *Social Theory and the Politics of Identity*, edited by Craig J. Calhoun, 9-36. Oxford: Blackwell, 1994.

Campbell, John Edward, and Matt Carlson. "Panopticon.Com: Online Surveillance and the Commodification of Privacy." *Journal of Broadcasting & Electronic Media* 46, no. 4 (2002): 586-606.

Carrier, Michael A. "Vote Counting, Technology, and Unintended Consequences." *St. John's Law Review* 79, no. 3 (2005): 645-87.

Castells, Manuel. *The Internet Galaxy: Reflections on the Internet, Business, and Society*. Oxford: Oxford University Press, 2001.

———. *The Rise of the Network Society*. 2nd ed. Oxford: Blackwell Publishers, 2000.

Cathcart, Robert S. "New Approaches to the Study of Movements: Defining Movements Rhetorically." *Western Speech* 36 (1972): 82-88.

Charland, Maurice. "Constitutive Rhetoric: The Case of the *Peuple Quebecois*." *Quarterly Journal of Speech* 73, no. 2 (1987): 133-50.

ChicagoLand, Thumpr Of. "Big Brother Online." *Phrack* 2, no. 23 (June 6, 1988): file 10.

Chomsky, Noam. *Media Control: The Spectacular Achievements of Propaganda*. New York: Seven Stories Press, 1997.

Clark, John, and Nuno Themudo. "The Age of Protest: Internet-Based "Dot-Causes" and the "Anti-Globalization" Movement." In *Globalizing Civic Engagement: Civil Society and Transnational Action*, edited by John Clark, 109-26. London: Earthscan Publications, 2003.

Clift, Steven. "An Internet of Democracy." *Communications of the ACM* 43, no. 11 (2000): 31-32.

Club, Chaos Computer. May 10, 2003. "CCC Summary: What Is the CCC?" http://www.ccc.de/club/?language=en (accessed January 27, 2006).

Company, The New York Times. 2006. "Circulation Data." *The New York Times Company*, http://www.nytco.com/investors-nyt-circulation.html (accessed February 13, 2006).

Conley, John. "Outwitting Cybercriminals." *Risk Management* 47, no. 7 (2000): 18-26.

Conway, Maura. "Hackers as Terrorists? Why It Doesn't Compute." *Computer Fraud & Security* 2003, no. 12 (2003): 10-13.

Corporation, Symantec. "Norton Personal Firewall: Product Overview." 2006. http://www.symantec.com/home_homeoffice/products/internet_security/npf2006/index.html (accessed March 10, 2006).

Costello, Barbara, Robert Lenholt, and Judson Stryker. "Using Blackboard in Library Instruction: Addressing the Learning Styles of Generations X and Y." *The Journal of Academic Librarianship* 30, no. 6 (2004): 452-60.

Cowboy, Datastream. "Phrack World News." *Phrack* 6, no. 47 (April 15, 1995): file 22.

Crandell, S. Judson. “The Beginnings of a Methodology for Social Control Studies in Public Address.” *Quarterly Journal of Speech* 33, no. 1 (1947): 36-39.

Cress, Daniel M., and David A. Snow. “The Outcomes of Homeless Mobilization: The Influence of Organization, Disruption, Political Mediation, and Framing.” *American Journal of Sociology* 105, no. 4 (2000): 1063-104.

Dallal, Jenine Abboushi. “Hizballah’s Virtual Civil Society.” *Television & New Media* 2, no. 4 (2001): 367-72.

Danet, Brenda , Lucia Ruedenberg-Wright, and Yehudit Rosenbaum-Tamari. “Hmmm . . . Where’s That Smoke Coming From?: Writing, Play and Performance on Internet Relay Chat.” *Journal of Computer-Mediated Communication* 2, no. 4 (1997), http://jcmc.indiana.edu/vol2/issue4/danet.html.

Davison, W. Phillips. “The Third-Person Effect in Communication.” *Public Opinion Quarterly* 47, no. 1 (1983): 1-15.

DeLuca, Kevin Michael, and Jennifer Peeples. “From Public Sphere to Public Screen: Democracy, Activism, and the ‘Violence’ of Seattle.” *Critical Studies in Media Communication* 19, no. 2 (2002): 125-51.

Derville, Tiffany. “Radical Activist Tactics: Overturning Public Relations Conceptualizations.” *Public Relations Review* 31 (2005): 527-33.

Dewey, John. *The Public and Its Problems*. Athens, OH: Swallow Press, 1991.

Diani, Mario. “Social Movement Networks Virtual and Real.” *Information Communication & Society* 3, no. 3 (2000): 386-401.

Dibbell, Julian. “A Rape in Cyberspace.” In *Cyberreader*, edited by Victor J. Vitanza, 454-72. Boston: Allyn and Bacon, 1999.

Dickinson, Greg. “Selling Democracy: Consumer Culture and Citizenship in the Wake of September 11.” *The Southern Communication Journal* 70, no. 4 (2005): 271-84.

Dietrich, Dawn. “Refashioning the Techno-Erotic Woman: Gender and Textuality in the Cybercultural Matrix.” In *Virtual Culture: Identity and Communication in Cybersociety*, edited by Steve Jones, 169-84. London: Sage Publications, 1997.

“Disenfranchisement by Means of the Poll Tax.” *Harvard Law Review* 53, no. 4 (1940): 645-52.

Disorder. “Phrack World News.” *Phrack* 8, no. 53 (July 8, 1998): article 14.

DJNZ, and the Action Tool Development Group of the electrohippies collective. February, 2000. “Occasional Paper No. 1: Client-Side Distributed Denial-of-Service: Valid Campaign Tactic or Terrorist Act?” the electrohippies collective, http://www.fraw.org.uk/ehippies/papers/op1.pdf (accessed January 30, 2006).

Doolittle, Robert J. “Riots as Symbolic: A Criticism and Approach.” *Central States Speech Journal* 27 (1976): 310-17.

Downs, Anthony. *An Economic Theory of Democracy*. New York: Harper, 1957.

Drucker, Susan J., and Gary Gumpert. “Cybercrime and Punishment.” *Critical Studies in Media Communication* 17, no. 2 (2000): 133-58.

Dyens, Ollivier. *Metal and Flesh: The Evolution of Man: Technology Takes Over*. Cambridge, MA: MIT Press, 2001.

Earth, Hackers of Planet. “Social Engineering.” In *Information Warfare: Cyberterrorism--Protecting Your Personal Security in the Electronic Age*, edited by Winn Schwartau, 360-66. New York: Thunder’s Mouth Press, 1996.

Edwards, Jan, and Alis Valencia. “Corporate Personhood and the ‘Right’ to Harm the Environment.” *Peace and Freedom* 62, no. 3 (2002): 10.

Ellul, Jacques. *Propaganda: The Formation of Men’s Attitudes*. Translated by Konrad Kellen and Jean Lerner. New York: Knopf, 1965.

———. *The Technological Society*. Translated by John Wilkinson. New York: Vintage Books, 1964.

———. “Technology and Democracy.” In *Democracy in a Technological Society*, edited by Langdon Winner, 35-50. Dordrecht: Kluwer, 1992.

Elmer, Greg. “A Diagram of Panoptic Surveillance.” *New Media & Society* 5, no. 2 (2003): 231-47.

Embar-Seddon, Ayn. “Cyberterrorism: Are We under Siege?” *The American Behavioral Scientist* 45, no. 6 (2002): 1033-43.

Engineering, Air Force Satellite Control Network System Program Office for Sustaining. “The Hacker Threat.” Washington, DC: Air Force Satellite Control Network System Program Office for Sustaining Engineering, 1989.

Erickson, Jon. *Hacking: The Art of Exploitation*. San Francisco: No Starch Press, 2003.

Fernback, Jan. “The Individual within the Collective: Virtual Ideology and the Realization of Collective Principles.” In *Virtual Culture: Identity and Communication in Cybersociety*, edited by Steve Jones, 36-54. London: Sage Publications, 1997.

Fortunati, Leopoldina. “The Human Body: Natural and Artificial Technology.” In *Machines That Become Us: The Social Context of Personal Communication Technology*, edited by James Everett Katz, 71-87. New Brunswick, NJ: Transaction Publishers, 2003.

Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. Translated by Alan Sheridan. 2nd Vintage Books ed. New York: Vintage Books, 1995.

Foucault, Michel, and James D. Faubion. *Power*. Translated by Robert Hurley. New York: New Press, 1994.

Frand, Jason L. “The Information Age Mindset: Changes in Students and Implications for Higher Education.” *Educause Review*, September/October 2000, 14-24.

Frank III, Arthur W. “Reality Construction in Interaction.” *Annual Review of Sociology* 5 (1979): 167-91.

Frantzich, Stephen E. *Cyberage Politics 101: Mobility, Technology and Democracy*. New York: Peter Lang, 2002.

Friedland, Lewis A. “Electronic Democracy and the New Citizenship.” *Media, Culture & Society* 18, no. 2 (1996): 185-212.

Furnell, Steven. *Cybercrime: Vandalizing the Information Society*. Boston: Addison-Wesley, 2002.

Furnell, Steven M., Paul S. Dowland, and Peter W. Sanders. “Dissecting the ‘Hacker Manifesto.’” *Information Management & Computer Security* 7, no. 2 (1999): 69-75.

Gerbner, George, Larry Gross, Michael Morgan, Nancy Signorielli, and James Shanahan. “Growing up with Television: Cultivation Processes.” In *Media Effects: Advances in Theory and Research*, edited by Jennings Bryant and Dolf Zillmann, 43-68. Mahwah, NJ: Lawrence Erlbaum Associates, 2002.

Gerhards, Jurgen, and Dieter Rucht. “Mesomobilization: Organizing and Framing in Two Protest Campaigns in West Germany.” *American Journal of Sociology* 98, no. 3 (1992): 555-96.

Gladstein, Deborah L., and Nora P. Reilly. “Group Decision Making under Threat: The Tycoon Game.” *Academy of Management Journal* 28, no. 3 (1985): 613-27.

Goffman, Erving. *Encounters: Two Studies in the Sociology of Interaction*. Indianapolis: Bobbs-Merrill, 1961.

———. *Frame Analysis: An Essay on the Organization of Experience*. Cambridge, MA: Harvard University Press, 1974.

———. *The Presentation of Self in Everyday Life*. Garden City, NY: Doubleday, 1959.

Goody, Jack. *The Domestication of the Savage Mind*. Cambridge: Cambridge University Press, 1977.

———. *The Power of the Written Tradition*. Washington, DC: Smithsonian Institution Press, 2000.

Gordon, Carol, and Asher Arian. “Threat and Decision Making.” *The Journal of Conflict Resolution* 45, no. 2 (2001): 196-215.

Gordon, Don E. *Electronic Warfare: Element of Strategy and Multiplier of Combat Power*. New York: Pergamon Press, 1981.

“Government Secrecy Continued to Rise in 2004.” *Newsletter on Intellectual Freedom* 54, no. 3 (2005): 100-01.

Graham, Fred P., and VaxCat. “Can You Find out If Your Telephone Is Tapped? ‘It Depends on Who You Ask.’” *Phrack* 2, no. 23 (December 30, 1988): file 9.

Green, Stephen. “A Plague on the Panopticon: Surveillance and Power in the Global Information Economy.” *Information Communication & Society* 2, no. 1 (1999): 26-44.

Gregg, Richard B. “The Ego-Function of the Rhetoric of Protest.” *Philosophy and Rhetoric* 4 (1971): 71-91.

Griffin, Leland M. “The Rhetoric of Historical Movements.” *Quarterly Journal of Speech* 38, no. 2 (1952): 184-88.

———. “The Rhetorical Structure of the Antimasonic Movement.” In *The Rhetorical Idiom*, edited by Donald Bryant, 145-60. Ithaca, NY: Cornell University Press, 1958.

Guerra, Sandra. “Voting Rights and the Constitution: The Disenfranchisement of Non-English Speaking Citizens.” *The Yale Law Journal* 97, no. 7 (1988): 1419-37.

Gunderson, Robert G. "'The Calamity Howlers.'" *Quarterly Journal of Speech* 26, no. 3 (1940): 401-11.

Gunkel, David J. *Hacking Cyberspace*. Boulder, CO: Westview Press, 2001.

H4G1S. September 14, 1998. RoTSHB. http://www.2600.com/hackedphiles/slashdot/hacked/ (accessed March 27, 2006).

Habermas, Jürgen. *Moral Consciousness and Communicative Action*. Translated by Christian Lenhardt and Shierry Weber Nicholsen. Cambridge, MA: MIT Press, 1990.

———. *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. Translated by Thomas Burger. Cambridge, MA: MIT Press, 1989.

Hacking For Girliez. September 13, 1998. "HFG Owns Mah Dumb Azz." *2600,* http://www.2600.com/hackedphiles/nytimes/hacked/ (accessed February 3, 2006).

Hacktivismo, and Cult of the Dead Cow. July 4, 2001. "The Hacktivismo Declaration." *Hacktivismo*, http://www.hacktivismo.com/public/declarations/en.php (accessed January 27, 2006).

Hafner, Katie, and John Markoff. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Simon & Schuster, 1991.

Hague, Barry N., and Brian Loader. "Digital Democracy: An Introduction." In *Digital Democracy: Discourse and Decision Making in the Information Age*, edited by Barry N. Hague and Brian Loader, 3-22. London: Routledge, 1999.

Haiman, Franklyn S. "The Rhetoric of the Streets: Some Legal and Ethical Considerations." *Quarterly Journal of Speech* 53 (1967): 99-114.

Halbert, Debora. "Discourses of Danger and the Computer Hacker." *Information Society* 13, no. 4 (1997): 361-74.

Harold, Christine. "Pranking Rhetoric: 'Culture Jamming' as Media Activism." *Critical Studies in Media Communication* 21, no. 3 (2004): 189-211.

Havelock, Eric Alfred. *The Muse Learns to Write: Reflections on Orality and Literacy from Antiquity to the Present*. New Haven: Yale University Press, 1986.

———. *Preface to Plato*. Cambridge: Belknap Press, 1963.

Herman, Edward S., and Noam Chomsky. *Manufacturing Consent: The Political Economy of the Mass Media*. New York: Pantheon Books, 1988.

Hermanowicz, Joseph C., and Harriet P. Morgan. "Ritualizing the Routine: Collective Identity Affirmation." *Sociological Forum* 14, no. 2 (1999): 197-214.

Herrington, TyAnna K. "The Interdependency of Fair Use and the First Amendment." *Computers and Composition* 15, no. 2 (1998): 125-43.

Hesseldahl, Arik. "After the Hack." *Columbia Journalism Review* 37, no. 5 (1999): 14.

———. All the News That's Fit to Hack. *Wired News*, http://www.wired.com/news/politics/0,1283,14990,00.html (accessed April 29, 2003).

Hogan, J. Michael. *The Panama Canal in American Politics: Domestic Advocacy and the Evolution of Policy*. Carbondale: Southern Illinois University Press, 1986.

House Committee on the Judiciary. *Administration's Draft Anti-Terrorism Act of 2001: Hearing before the House Committee on the Judiciary*, 107th Cong., 1, 2001.

House Select Committee on Homeland Security. *H.R. 5005, the Homeland Security Act of 2002, Days 1 and 2: Hearing before the House Select Committee on Homeland Security*, 107th Cong., 2, July 15-16, 2002.

House Select Committee on Homeland Security. *Transforming the Federal Government to Protect America from Terrorism: Hearing before the House Select Committee on Homeland Security*, 107th Cong., 2, July 11, 2002.

Howard, Philip N. "Deep Democracy, Thin Citizenship: The Impact of Digital Media in Political Campaign Strategy." *The Annals of The American Academy Of Political And Social Science* 597, no. 1 (2005): 153-70.

Huseby, Sverre H. *Innocent Code: A Security Wake-up Call for Web Programmers*. New York: John Wiley & Sons, 2004.

Hyland, James L. *Democratic Theory: The Philosophical Foundations*. Manchester: Manchester University Press, 1995.

Jamieson, Kathleen Hall. *Eloquence in an Electronic Age: The Transformation of Political Speechmaking*. New York: Oxford University Press, 1988.

Jefferson, Thomas. "To Edward Carrington." In *Thomas Jefferson, Political Writings*, edited by Joyce Oldham Appleby and Terence Ball, 152-54. New York: Cambridge University Press, 1999.

Jenkins, Henry, and David Thorburn. “Introduction: The Digital Revolution, the Informed Citizen, and the Culture of Democracy.” In *Democracy and New Media*, edited by Henry Jenkins, David Thorburn and Brad Seawell, 1-17. Cambridge, MA: MIT Press, 2003.

Jewkes, Yvonne, and Keith Sharp. “Crime, Deviance and the Disembodied Self: Transcending the Dangers of Corporeality.” In *Dot.Cons*, edited by Yvonne Jewkes, 1-14. Portland, OR: Willan Publishing, 2002.

Jockey, The Disk. “Getting Caught - Legal Procedures.” *Phrack* 3, no. 26 (March 24, 1989): file 3.

Johnson, Jeff. “The Information Superhighway: A Worst-Case Scenario.” *Communications of the ACM* 39, no. 2 (1996): 15-17.

Jones, Steve. “The Internet and Its Social Landscape.” In *Virtual Culture: Identity and Communication in Cybersociety*, edited by Steve Jones, 7-35. London: Sage Publications, 1997.

Jordan, Tim. *Cyberpower: The Culture and Politics of Cyberspace and the Internet*. London: Routledge, 1999.

Jordan, Tim, and Paul A. Taylor. *Hacktivism and Cyberwars: Rebels with a Cause?* New York, NY: Routledge, 2004.

Juris, Jeffrey S. “The New Digital Media and Activist Networking within Anti-Corporate Globalization Movements.” *The Annals of The American Academy Of Political And Social Science* 597, no. 1 (2005): 189-208.

Kahn, Richard, and Douglas Kellner. “New Media and Internet Activism: From the `Battle of Seattle’ to Blogging.” *New Media & Society* 6, no. 1 (2004): 87-95.

Kates, Jim, Stephen Nickson, Mark Greisiger, and Peter R Taffea. “The Reality of Hackers.” *Risk Management* 48, no. 7 (2001): 50-57.

Kauffman, L. A. “The Anti-Politics of Identity.” *Socialist Review* 20, no. 1 (1990): 67-80.

Kerbel, Matthew R., and Joel David Bloom. “Blog for America and Civic Involvement.” *Harvard International Journal of Press/Politics* 10, no. 4 (2005): 3-27.

Keum, Heejo, Narayan Devanathan, Sameer Deshpande, Michelle R. Nelson, and Dhavan V. Shah. “The Citizen-Consumer: Media Effects at the Intersection of Consumer and Civic Culture.” *Political Communication* 21, no. 3 (2004): 369-91.

Kibby, Marjorie, and Brigid Costello. “Between the Image and the Act: Interactive Sex Entertainment on the Internet.” *Sexualities* 4, no. 3 (2001): 353-69.

King, Taran. “Introduction.” *Phrack* 1, no. 1 (November 17, 1985): phile 1.

———. “Introduction.” *Phrack* 1, no. 7 (September 25, 1986): phile 1.

———. “Introduction.” *Phrack* 1, no. 9 (December 1, 1986): phile 1.

———. “Phrack Pro-Phile XXIII: The Mentor,” *Phrack* 2, no. 23 (January 18, 1989): file 2.

Klumpp, James F. “Challenge of Radical Rhetoric: Radicalization at Columbia.” *Western Speech* 37, no. 3 (1973): 146-56.

Kovacich, Gerald L. “Hackers: Freedom Fighters of the 21st Century.” *Computers & Security* 18, no. 7 (1999): 573-76.

Kraut, Robert, Sara Kiesler, Bonka Boneva, Jonathan Cummings, Vicki Helgeson, and Anne Crawford. “Internet Paradox Revisited.” *The Journal of Social Issues* 58, no. 1 (2002): 49-74.

Kraut, Robert, Michael Patterson, Vicki Lundmark, Sara Kiesler, Tridas Mukopadhyay, and William Scherlis. “Internet Paradox: A Social Technology That Reduces Social Involvement and Psychological Well-Being?” *The American Psychologist* 53, no. 9 (1998): 1017-31.

Lane, Jill. “Digital Zapatistas.” *TDR: The Drama Review* 47, no. 2 (2003): 129-44.

Lea, Graham. September 14, 1998. “New York Times Hacked.” *The Register*, http://www.theregister.co.uk/1998/09/14/new_york_times_hacked/ (accessed February 13, 2006).

Lessig, Lawrence. *Code and Other Laws of Cyberspace*. New York: Basic Books, 1999.

———. “The Zones of Cyberspace.” *Stanford Law Review* 48, no. 5 (1996): 1403-11.

Leung, Louis. “Impacts of Net-Generation Attributes, Seductive Properties of the Internet, and Gratifications-Obtained on Internet Use.” *Telematics and Informatics* 20, no. 2 (2003): 107-29.

———. “Net-Generation Attributes and Seductive Properties of the Internet as Predictors of Online Activities and Internet Addiction.” *CyberPsychology & Behavior* 7, no. 3 (2004): 333-48.

Levy, Stephen. *Hackers: Heroes of the Computer Revolution*. New York: Penguin, 1984.

Lightning, Knight. "Introduction." *Phrack* 2, no. 14 (July 28, 1987): phile 1.

———. "Phrack World News." *Phrack* 2, no. 23 (January 25, 1989): file 11.

Lightning, Knight, and Taran King. "Phrack World News." *Phrack* 2, no. 22 (December 23, 1988): file 9.

Lijphart, Arend. *Patterns of Democracy: Government Forms and Performance in Thirty-Six Countries*. New Haven, CT: Yale University Press, 1999.

Lippmann, Walter. *Public Opinion*. 1st Free Press pbks. ed. New York: Free Press Paperbacks, 1997.

Lovecraft, Howard Phillips. "Supernatural Horror in Literature." In *Dagon, and Other Macabre Tales*, edited by S. T. Joshi, 365-436. Sauk City, WI: Arkham House, 1965.

Lucas, Stephen E. "Coming to Terms with Movement Studies." *Central States Speech Journal* 31, no. 4 (1980): 255-66.

Lyon, Janet. *Manifestoes: Provocations of the Modern*. Ithaca, NY: Cornell University Press, 1999.

MacKinnon, Richard. "Virtual Rape." *Journal of Computer-Mediated Communication* 2, no. 4 (1997), http://jcmc.indiana.edu/vol2/issue4/mackinnon.html.

Madison, James. "To W. T. Barry, August 4, 1822." In *Letters and Other Writings of James Madison*, 3:276-81. Philadelphia: J. B. Lippincott & co., 1865.

Madsen, Wayne. "Carnivore Documents Reveal Enhanced Tapping Abilities." *Network Security* 2001, no. 1 (2001): 5.

Magaziner, Ira, and Benjamin Barber. "Democracy and Cyberspace: First Principles." In *Democracy and New Media*, edited by Henry Jenkins, David Thorburn and Brad Seawell, 113-31. Cambridge, MA: MIT Press, 2003.

Manning, Rita C. "Corporate Responsibility and Corporate Personhood." *Journal of Business Ethics* 3, no. 1 (1984): 77-84.

Margolis, Michael, and David Resnick. *Politics as Usual: The Cyberspace "Revolution."* Thousand Oaks, CA: Sage Publications, 2000.

Martin, Hugh J. 2000. “Hacktivism: The New Protest Movement?” *Spark-Online*, http://www.spark-online.com/april00/trends/martin.html (accessed April 27, 2003).

Martin, James. *The Wired Society*. Englewood Cliffs, N.J.: Prentice-Hall, 1978.

Marx, Karl, and Friedrich Engels. “The Poverty of Philosophy.” In *Karl Marx, Frederick Engels: Collected Works*, 6:105-212. Moscow: Progress Publishers, 1975.

Mawson, Anthony R. “Understanding Mass Panic and Other Collective Responses to Threat and Disaster.” *Psychiatry* 68, no. 2 (2005): 95-113.

McAdam, Doug, and Dieter Rucht. “The Cross-National Diffusion of Movement Ideas.” *The Annals of the American Academy of Political and Social Science* 528 (1993): 56-74.

McCarthy, John D., and Mayer N. Zald. “Resource Mobilization and Social Movements: A Partial Theory.” *American Journal of Sociology* 82, no. 6 (1977): 1212-41.

McChesney, Robert Waterman. *Corporate Media and the Threat to Democracy*. New York: Seven Stories Press, 1997.

McCombs, Maxwell E., and Donald L. Shaw. “The Agenda-Setting Function of Mass Media.” *Public Opinion Quarterly* 36, no. 2 (1972): 176-87.

McGee, Michael C. “In Search of ‘the People’: A Rhetorical Alternative.” *Quarterly Journal of Speech* 61, no. 3 (1975): 235-49.

McGee, Michael Calvin. “‘Social Movement’: Phenomenon or Meaning?” *Central States Speech Journal* 31, no. 4 (1980): 233-44.

———. “Text, Context, and the Fragmentation of Contemporary Culture.” *Western Journal of Communication* 54, no. 3 (1990): 274-89.

McKenzie, John. “!Nt3rh4ckt!V!Ty.” *Style* 33, no. 2 (1999): 283-99.

McLuhan, Marshall. *Understanding Media: The Extensions of Man*. 1st MIT Press ed. Cambridge, MA: MIT Press, 1994.

McLuhan, Marshall, Quentin Fiore, and Jerome Agel. *The Medium Is the Massage: An Inventory of Effects*. San Francisco, CA: HardWired, 1996.

Meeks, Brock N. “Better Democracy through Technology.” *Communications of the ACM* 40, no. 2 (1997): 75-78.

Meinel, Carolyn. January 4, 1999. “Happy Hacker Digest.” http://happyhacker.org/hhlist/inside1_4.shtml (accessed February 6, 2006).

———. September 25, 1998. “Happy Hacker Digest.” http://happyhacker.org/hhlist/digest49.shtml (accessed February 6, 2006).

Melucci, Alberto. *Challenging Codes: Collective Action in the Information Age*. Cambridge: Cambridge University Press, 1996.

Mentor, The. “The Conscience of a Hacker.” *Phrack* 1, no. 7 (1986): phile 3.

———. “Crashing Dec-10’s.” *Phrack* 1, no. 4 (March 13, 1986): phile 6.

Mill, James. “Liberty of the Press.” In *Essays on Government, Jurisprudence, Liberty of the Press and Law of Nations*, 1-34. New York: A. M. Kelley, 1967.

Millar, Melanie Stewart. *Cracking the Gender Code: Who Rules the Wired World?* Toronto: Second Story Press, 1998.

Milone, Mark G. “Hacktivism: Securing the National Infratructure.” *The Business Lawyer* 58, no. 1 (2002): 383-413.

Mitnick, Kevin D., and William L. Simon. *The Art of Deception: Controlling the Human Element of Security*. Indianapolis: Wiley, 2002.

Molina, Alejandro. “Cyberspace: The “Color Line” of the 21st Century.” *Social Justice* 30, no. 2 (2003): 143-49.

Molly, Hatchet. “Hacking: What’s Legal and What’s Not.” *Phrack* 3, no. 25 (March 8, 1989): file 8.

Moore, Richard K. “Democracy and Cyberspace.” In *Digital Democracy: Discourse and Decision Making in the Information Age*, edited by Barry N. Hague and Brian Loader, 39-59. London: Routledge, 1999.

Morris, Dick. “The Future of Political Campaigning: The American Example.” *Journal of Public Affairs* 3, no. 1 (2003): 14-20.

Mosco, Vincent. “Computers and Democracy.” In *The Information Society: Evolving Landscapes*, edited by Jacques Berleur, Andrew Clement, Richard Sizer and Diane Whitehouse, 215-31. New York: Springer-Verlag, 1990.

Nabbali, Talitha, and Mark Perry. “Going for the Throat: Carnivore in an Echelon World - Part I.” *Computer Law & Security Report* 19, no. 6 (2003): 456-67.

———. “Going for the Throat: Carnivore in an Echelon World - Part II.” *Computer Law & Security Report* 20, no. 2 (2004): 84-97.

Negroponte, Nicholas. *Being Digital*. New York: Knopf, 1995.

———. “Beyond Digital.” *Wired*, December 1998, 288.

Nelson, Diane M. “Maya Hackers and the Cyberspatialized Nation-State: Modernity, Ethnostalgia, and a Lizard Queen in Guatemala.” *Cultural Anthropology* 11, no. 3 (1996): 287-308.

Network, Cable News. September 13, 1998. “Hackers Break into N.Y. Times Web Site.” *CNN.com*, http://www.cnn.com/TECH/computing/9809/13/nyt.hacked/ (accessed February 13, 2006).

Noack, David. “Hack Attack Sends Chill through News Web Sites.” *Editor & Publisher*, September 19, 1998, 14.

Nunziato, Dawn C. “Freedom of Expression, Democratic Norms, and Internet Governance.” *Emory Law Journal* 52, no. 1 (2003): 187-279.

Office, Government Accountability. “Energy Task Force: Process Used to Develop the National Energy Policy.” Washington, DC: Government Accountability Office, 2003.

Ong, Walter J. *Orality and Literacy: The Technologizing of the Word*. London: Methuen, 1982.

Owens, Lynn, and L. Kendall Palmer. “Making the News: Anarchist Counter-Public Relations on the World Wide Web.” *Critical Studies in Media Communication* 20, no. 4 (2003): 335-61.

P.H.A.i.T. November 22, 1997. “Hacked Timor.” *2600*, http://www.2600.com/hackedphiles/timor010198/indo/ (accessed February 3, 2006).

Papacharissi, Zizi. “The Virtual Sphere: The Internet as a Public Sphere.” *New Media & Society* 4, no. 1 (2002): 9-27.

Park, Hyun Soon. “Case Study: Public Consensus Building on the Internet.” *CyberPsychology & Behavior* 5, no. 3 (2002): 233-39.

Penenberg, Adam L. April 5, 1999. “Mitnick Speaks!” *Forbes.com*, http://www.forbes.com/1999/04/05/feat.html (accessed April 29, 2003).

Perloff, Richard M. “The Third Person Effect in Media Effects.” In *Media Effects: Advances in Theory and Research*, edited by Jennings Bryant and Dolf Zillmann, 489-506. Mahwah, NJ: Lawrence Elbaum Associates, 2002.

Phreak_Accident. “Phrack World News.” *Phrack* 3, no. 31 (May 28, 1990): phile 8.

Pichardo, Nelson A. “New Social Movements: A Critical Review.” *Annual Review of Sociology* 23 (1997): 411-30.

Plato. “Laws.” In *The Collected Dialogues of Plato, Including the Letters*, edited by Edith Hamilton and Huntington Cairns, 1225-513. Princeton, NJ: Princeton University Press, 1961.

———. “Republic.” In *The Collected Dialogues of Plato, Including the Letters*, edited by Edith Hamilton and Huntington Cairns, 575-844. Princeton, NJ: Princeton University Press, 1961.

Poulsen, Kevin. January 14, 2005. “FBI Retires Its Carnivore.” *SecurityFocus*, http://www.securityfocus.com/news/10307 (accessed February 22, 2006).

———. September 16, 1998. “Grassroots Hacktivism.” *G4 Media Inc*., http://www.g4tv.com/techtvvault/features/3292/Grassroots_Hacktivism.html (accessed February 13, 2006).

Powers, Francis Gary. *Fair Use: The Story of the Letter U and the Numeral 2*. Concord, CA: Seeland, 1995.

Qrin, Elf. July 31, 2000. “Elf Qrin Interviews the Mentor.” http://www.elfqrin.com/docs/hakref/interviews/eq-i-mentor.html (accessed March 28, 2006).

Radio Broadcast. May, 1922. Quoted in Erik Barnouw, “New Look.” In *Conglomerates and the Media*, edited by Patricia Aufderheide, Erik Barnouw, Richard M. Cohen, Thomas Frank, Todd Gitlin, David Lieberman, Mark Crispin Miller, Gene Roberts and Thomas Schatz, 15-29. New York: New Press, 1997.

Rafalko, Robert J. “Corporate Punishment: A Proposal.” *Journal of Business Ethics* 8, no. 12 (1989): 917-28.

Randall, Neil. *The Soul of the Internet*. London: Thompson Publishing Inc., 1997.

Randazza, Marc J. “The Forgotten Electoral Controversy.” *Intermedia* 29, no. 2 (2001): 33-37.

Randolph, Sal. “Free Words to Free Manifesta: Some Experiments in Art as Gift.” *Ethics & the Environment* 8, no. 1 (2003): 61-73.

Rayl, A. J. S. “Secrets of the Cyberculture.” *Omni*, November 1992, 58-67.

Raymond, Eric S. *The Cathedral & the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary*. Cambridge, MA: O’Reilly, 1999.

“Remember the Blue Box?” *Youth International Party Line* October, 1971, 1.

Rheingold, Howard. *Smart Mobs: The Next Social Revolution*. Cambridge, MA: Perseus, 2002.

Rogue, Space. September 17, 2004. “Lets Set the Record Straight.” *Slashdot*, http://it.slashdot.org/comments.pl?sid=122222&threshold=1&commentsort=0&mode=thread&cid=10280841 (accessed February 14, 2006).

Romano, Mike. “The Politics of Hacking.” *Spin*, November 1999, 168-74.

Roskos-Ewoldsen, David R., Beverly Roskos-Ewoldsen, and Francesca R. Dillman Carpentier. “Media Priming: A Synthesis.” In *Media Effects: Advances in Theory and Research*, edited by Jennings Bryant and Dolf Zillmann, 97-120. Mahwah, NJ: Lawrence Erlbaum Associates, 2002.

Ruffin, Oxblood. March 28, 2004. “Hacktivism, from Here to There.” Cult of the Dead Cow, http://www.cultdeadcow.com/cDc_files/cDc-0384.html (accessed February 1, 2006).

———. July 17, 2000. “Hacktivismo.” *Cult of the Dead Cow*, http://www.cultdeadcow.com/archives/2000/07/hacktivismo_by_oxblo.php3 (accessed January 30, 2006).

Ruffin, Oxblood, A Dwarf Named Warren, and Little Marie. 2000-2001. “The Hacktivismo FAQ v1.0.” *Cult of the Dead Cow*, http://www.cultdeadcow.com/cDc_files/HacktivismoFAQ.html (accessed January 30, 2006).

Ryan, Charlotte. “Framing, the News Media, and Collective Action.” *Journal of Broadcasting & Electronic Media* 45, no. 1 (2001): 175-82.

Saco, Diana. *Cybering Democracy: Public Space and the Internet*. Minneapolis: University of Minnesota Press, 2002.

Salus, Peter H. *Casting the Net: From Arpanet to Internet and Beyond*. Reading, MA: Addison-Wesley, 1995.

Scammell, Margaret. “The Internet and Civic Engagement: The Age of the Citizen-Consumer.” *Political Communication* 17, no. 4 (2000): 351-55.

Schement, Jorge Reina. “Democracy Digitized.” *Broadcasting & Cable* 131, no. 15 (2001): 77.

———. “An Etymological Exploration of the Links between Information and Communication.” In *Between Communication & Information*, edited by Brent D. Ruben and Jorge Reina Schement, 173-87. New Brunswick, NJ: Transaction Publishers, 1993.

———. “The Origins of the Information Society in the United States: Competing Visions.” In *The Information Society: Economic, Social, and Structural Issues*, edited by Jerry Lee Salvaggio, 29-50. Hillsdale, NJ: Lawrence Erlbaum Associates, 1989.

Schement, Jorge Reina, and Terry Curtis. *Tendencies and Tensions of the Information Age: The Production and Distribution of Information in the United States*. New Brunswick, NJ: Transaction Publishers, 1997.

Schiller, Herbert I., and Bernard Miège. “Communication of Knowledge in an Information Society.” In *The Information Society: Evolving Landscapes*, edited by Jacques Berleur, Andrew Clement, Richard Sizer and Diane Whitehouse, 161-67. New York: Springer-Verlag, 1990.

Schleher, D. Curtis. *Electronic Warfare in the Information Age*. Boston: Artech House, 1999.

Schlosberg, David, and John S. Dryzek. “Digital Democracy: Authentic or Virtual?” *Organization & Environment* 15, no. 3 (2002): 332-35.

Schudson, Michael. *The Good Citizen: A History of American Civic Life*. New York: Martin Kessler Books, 1998.

Schumpeter, Joseph Alois. *Capitalism, Socialism, and Democracy*. 4th ed. London: Allen & Unwin, 1954.

Schwartau, Winn. “Cyber Christ Bites the Big Apple - Hope - Hackers on Planet Earth, New York City - August 13-14, 1994.” *Phrack* 5, no. 46 (September 20, 1994): file 23.

———. *Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Destruction*. New York: Thunder’s Mouth Press, 2000.

Schwartz, Bernard. “The Negro and the Law in the United States.” *The Modern Law Review* 14, no. 4 (1951): 446-61.

Scott, Alan. *Ideology and the New Social Movements*. London: Unwin Hyman, 1990.

Scott, Robert L. “The Conservative Voice in Radical Rhetoric: A Common Response to Division.” *Speech Monographs* 40 (1973): 123-35.

Scott, Robert L., and Donald K. Smith. “The Rhetoric of Confrontation.” *Quarterly Journal of Speech* 55 (1969): 1-8.

Segaller, Stephen. *Nerds 2.0.1: A Brief History of the Internet*. New York: TV Books, 1998.

Senate Governmental Affairs Committee. May 19, 1998. “Weak Computer Security in the Government: Is the Public at Risk?” *Senate Governmental Affairs Committee*, http://www. senate.gov/~govt-aff/051998_summary.htm (accessed February 13, 2006).

Sennett, Richard. *The Fall of Public Man*. New York: W.W. Norton, 1996.

Shark, Shooting. “Phrack XV Intro.” *Phrack* 2, no. 15 (August 7, 1987): file 1.

Shimomura, Tsutomu, and John Markoff. *Take-Down: The Pursuit and Capture of Kevin Mitnick, America’s Most Wanted Computer Outlaw--by the Man Who Did It*. New York: Hyperion, 1996.

Siani, Kenneth. “Kenneth Siani Speaks out About Kevin Mitnick.” *Phrack* 3, no. 27 (June 20, 1989): file 10.

Sillars, Malcolm O. “Defining Social Movements Rhetorically: Casting the Widest Net.” *Southern Speech Communication Journal* (1980): 17-32.

Simons, Herbert W. “On Terms, Definitions and Theoretical Distinctiveness: Comments on Papers by Mcgee and Zarefsky.” *Central States Speech Journal* 31, no. 4 (1980): 306-15.

Sivakumaran, Sandesh. “Male/Male Rape and the “Taint” of Homosexuality.” *Human Rights Quarterly* 27, no. 4 (2005): 1274-306.

Smelser, Neil J. *Theory of Collective Behavior*. New York: Free Press, 1962.

Smith, Edward E. *Children of the Lens*. Reading, PA: Fantasy Press, 1954.

———. *First Lensman*. Reading, PA: Fantasy Press, 1950.

Smuggler, The. “Phrack World News.” *Phrack* 2, no. 17 (February 1, 1988): file 11.

Snow, David A., E. Burke Rochford, Jr., Steven K. Worden, and Robert D. Benford. "Frame Alignment Processes, Micromobilization, and Movement Participation." *American Sociological Review* 51, no. 4 (1986): 464-81.

Sobchack, Vivian. "Beating the Meat/Surviving the Text, or How to Get out of This Century Alive." In *Cyberspace/Cyberbodies/Cyberpunk: Cultures of Technological Embodiment*, edited by Mike Featherstone and Roger Burrows, 205-14. London: Sage, 1995.

Solomon, Norman. "Hiding out in Cyberspace." *The Humanist* 61, no. 4 (2001): 17.

Songini, Marc L. "Maryland House Votes to Oust Diebold Machines." *Computerworld*, March 13, 2006, 14.

Sorcerer, Dark. May 9, 2005. "Operation Sundevil... 15 Years Later." *Cult of the Dead Cow*, http://www.cultdeadcow.com/archives/2005/05/operation_sundevil_1.php3 (accessed March 21, 2006).

———. April 22, 2005. "A Short Requiem for _Phrack_ . . . Life Sucking in the Middle East." *Cult of the Dead Cow*, http://www.cultdeadcow.com/archives/2005/04/a_short_requiem_for_.php3 (accessed March 21, 2006).

Sprigman, Chris. March 5, 2002. "The Mouse That Ate the Public Domain: Disney, the Copyright Term Extension Act, and Eldred V. Ashcroft." *FindLaw*, http://writ.news.findlaw.com/commentary/20020305_sprigman.html (accessed September 1, 2005).

Sprouse, Martin. *Sabotage in the American Workplace: Anecdotes of Dissatisfaction, Mischief, and Revenge*. San Francisco: Pressure Drop Press, 1992.

Staff, Attrition. "Negation: The End." *Attrition*, http://attrition.org/errata/charlatan/negation/ (accessed February 13, 2006).

Staff, Phrack. "Phrack Editorial." *Phrack* 6, no. 47 (April 15, 1995): file 2a.

Stanley, Jay, and Barry Steinhardt. "Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society." *American Civil Liberties Union*, http://www.aclu.org/FilesPDFs/aclu_report_bigger_monster_weaker_chains.pdf (accessed April 18, 2006).

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

Stewart, Charles J. “Championing the Rights of Others and Challenging Evil: The Ego Function in the Rhetoric of Other-Directed Social Movements.” *Southern Communication Journal* 64, no. 2 (1999): 91-105.

Stewart, Charles J., Craig Allen Smith, and Robert E. Denton. *Persuasion and Social Movements*. 4th ed. Prospect Heights, IL: Waveland Press, 2001.

Stock, Gregory. *Metaman: The Merging of Humans and Machines into a Global Superorganism*. New York: Simon & Schuster, 1993.

Subcommittee on Commerce, Trade, and Consumer Protection of the Committee on Energy and Commerce. *Cyber Security: Private-Sector Efforts Addressing Cyber Threats*, 107th Cong., 1, November 15, 2001.

Sunstein, Cass R. *Republic.Com*. Princeton, NJ: Princeton University Press, 2001.

Sussman, Gerald. *Communication, Technology, and Politics in the Information Age*. Thousand Oaks, CA: Sage Publications, 1997.

Sutton, Neil. “Security Breach Exposes Holes in Credit Card System.” *Computing Canada* 31, no. 10 (2005): 1, 12.

Tapscott, Don. *Growing up Digital: The Rise of the Net Generation*. New York: McGraw-Hill, 1998.

Taylor, Paul A. *Hackers: Crime in the Digital Sublime*. London: Routledge, 1999.

———. “Maestros or Misogynists? Gender and the Social Construction of Hacking.” In *Dot.Cons*, edited by Yvonne Jewkes, 126-46. Portland, OR: Willan Publishing, 2003.

Terranova, Tiziana. “Communication Beyond Meaning: On the Cultural Politics of Information.” *Social Text* 22, no. 3 (2004): 51-73.

Terrorism, National Commission on. 2000. “Countering the Changing Threat of International Terrorism.” *National Commission on Terrorism*, http://www.gpo.gov/nct/nct3.pdf (accessed February 21, 2006).

Tesh, Sylvia N. “The Internet and the Grass Roots.” *Organization & Environment* 15, no. 3 (2002): 336-39.

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

Thomas, Graham, and Sally Wyatt. “Access Is Not the Only Problem: Using and Controlling the Internet.” In *Technology and in/Equality: Questioning the*

Information Society, edited by Sally Wyatt, Flis Henwood, Nod Miller and Peter Senker, 21-45. London: Routledge, 2000.

Toffler, Alvin. *The Third Wave*. New York: William Morrow and Company, 1980.

Toffler, Alvin, and Heidi Toffler. *Creating a New Civilization: The Politics of the Third Wave*. Atlanta: Turner Pub., 1995.

Touraine, Alain. *What Is Democracy?* Translated by David Macey. Boulder, CO: WestviewPress, 1997.

Trammel. February 14, 2006. "Modern Love." *Cult of the Dead Cow*, http://www .cultdeadcow. com/cDc_files/cDc-0403.php (accessed March 22, 2006).

Turkle, Sherry. *Life on the Screen: Identity in the Age of the Internet*. New York: Simon & Schuster, 1995.

———. *The Second Self: Computers and the Human Spirit*. New York: Simon and Schuster, 1984.

Turtle, Tippy. 1987. "Ted and Dave's Animal Fun: Session I: Bunny Lust." *Cult of the Dead Cow*, http://www.cultdeadcow.com/cDc_files/cDc-0018.php (accessed March 22, 2006).

Union, American Civil Liberties. October 4, 2001. "Despite Significant Improvements, ACLU Says House Bill Fails to Protect Liberty." *American Civil Liberties Union*, http://www. aclu.org/NationalSecurity/NationalSecurity.cfm?ID=9782&c=24 (accessed December 13, 2003).

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001. Public Law 107–56. 107th Cong. 1st sess., October 26, 2001.

Uslaner, Eric M. "Trust, Civic Engagement, and the Internet." *Political Communication* 21, no. 2 (2004): 223-42.

Vakin, Sergei A., Lev N. Shustov, and Robert H. Dunwell. *Fundamentals of Electronic Warfare*. Boston: Artech House, 2001.

Van Aelst, Peter, and Stefaan Walgrave. "New Media, New Movements? The Role of the Internet in Shaping the Anti-Globalization Movement." *Information Communication & Society* 5, no. 4 (2002): 465-93.

Vanderburg, Willem. "Political Imagination in a Technical Age." In *Democratic Theory and Technological Society*, edited by Richard B. Day, Ronald Beiner and Joseph Masciulli, 3-35. Armonk, NY: M.E. Sharpe, 1988.

Vegh, Sandor. "Hacktivists or Cyberterrorists? The Changing Media Discourse on Hacking." *First Monday* 7, no. 10 (2002), http://www.firstmonday.org/issues/issue7_10/vegh/index.html.

Verton, Dan. *The Hacker Diaries: Confessions of Teenage Hackers*. New York: McGraw-Hill/Osborne, 2002.

Waites, Matthew. *The Age of Consent: Young People, Sexuality, and Citizenship*. New York: Palgrave Macmillan, 2005.

Watzlawick, Paul, Janet Beavin Bavelas, and Don D. Jackson. *Pragmatics of Human Communication; A Study of Interactional Patterns, Pathologies, and Paradoxes*. New York: Norton, 1967.

Weiler, Angela. "Information-Seeking Behavior in Generation Y Students: Motivation, Critical Thinking, and Learning Theory." *The Journal of Academic Librarianship* 31, no. 1 (2005): 46-53.

Wellen, Alex. September 16, 1998. "Delving into the Source." *G4 Media, Inc*., http://www.g4tv.com/techtvvault/features/4720/Delving_Into_the_Source.html (accessed January 23, 2006).

"While Progress Has Been Made, Managers and Employees Are Still Susceptible to Social Engineering Techniques." Washington, DC: Department of the Treasury, 2005.

"White House Phone Directory." *2600*, January, 1984, 5.

White, Lynn, Jr. *Medieval Technology and Social Change*. Oxford: Clarendon Press, 1962.

"White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63." Washington, DC, 1998.

Whorf, Benjamin Lee. *Language, Thought, and Reality: Selected Writings*. Cambridge, MA: M.I.T. Press, 1956.

Wilkinson, Charles A. "A Rhetorical Definition of Movements." *Central States Speech Journal* 27 (1976): 88-94.

Williams, Matthew. “Virtually Criminal: Discourse, Deviance and Anxiety within Virtual Communities.” *International Review of Law, Computers & Technology* 14, no. 1 (2000): 95-104.

Wilson, P. Eddy. “Corporations, Minors, and Other Innocents - a Reply from R. E. Ewin.” *Journal of Business Ethics* 13, no. 10 (1994): 761-74.

Windt, Theodore Otto, Jr. “The Diatribe: Last Resort for Protest.” *Quarterly Journal of Speech* 58 (1972): 1-14.

Winner, Langdon. *Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought*. Cambridge, MA: MIT Press, 1977.

———. “Technologies as Forms of Life.” In *Technology and Values*, edited by K. S. Shrader-Frechette and Laura Westra, 55-69. Lanham, MD: Rowman & Littlefield, 1997.

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

Wray, Stefan. “On Electronic Civil Disobedience.” *Peace Review* 11, no. 1 (1999): 107-11.

Yar, Majid. “Computer Hacking: Just Another Case of Juvenile Delinquency?” *The Howard Journal of Criminal Justice* 44, no. 4 (2005): 387-99.

Young, Iris Marion. *Inclusion and Democracy*. Oxford: Oxford University Press, 2000.

Yourdon, Edward. *Byte Wars: The Impact of September 11 on Information Technology*. Upper Saddle River, NJ: Prentice Hall PTR, 2002.

Zaretsky, Eli. “Identity Theory, Identity Politics: Psychoanalysis, Marxism, Post-Structuralism.” In *Social Theory and the Politics of Identity*, edited by Craig J. Calhoun, 198-215. Oxford: Blackwell, 1994.

VITA

Brett Lance Lunceford

Ph.D. Communication Arts and Sciences, The Pennsylvania State University, expected December, 2006
M.A. Speech Communication, California State University, Hayward, 2003
B.S. Speech Communication, Oregon State University, 1998

Selected Conference Presentations

Lunceford, Brett. "Building a Collective Identity One Text Phile at a Time: Reading *Phrack*." Presented to the Rhetoric Society of America, 2006.
———. "Evading the Panoptic Gaze as Terrorist Act: The Rhetorical Construction of the Hacker as Terrorist." Presented to the Human Communication Technology Division of the National Communication Association, 2005.
———. "Pornographic Spam and the Rhetorical Construction of Male and Female Sexualities." Presented to the Media Studies interest group of the Western States Communication Association, 2005.
———. "What the Ancients Already Knew: The Art and Science of Orality." Presented to the Media Studies and Language and Social Interaction interest groups of the Western States Communication Association, 2005.
———. "J00 uR 0wN3D: The Rhetorical Dimensions of Hacking." Presented to the Rhetoric Society of America, 2004.
———. "Entering the World of the Hacker: A Close Textual Analysis of 'The Conscience of a Hacker.'" Presented to the Human Information Technologies interest group of the Eastern Communication Association, 2004.
———. "Toward a Clearer Differentiation Between Propaganda and Rhetoric." Presented to the Rhetoric and Public Address interest group of the Eastern Communication Association, 2004.

Selected Awards and Honors

2005, Institute for the Arts and Humanities Dissertation Release Fellowship, The Pennsylvania State University
2002, Department Service Award, California State University, Hayward

Selected Service

Faculty Advisor, Students Organizing Multiple Arts (SOMA), Spring 2005-Current, The Pennsylvania State University