December 2014

Framing the Policy Debate: Competing Portrayals of Technology in Online Content Regulation and Lessons from Science and Technology Studies

Jeremy John Mauger
University of Wisconsin-Milwaukee

FRAMING THE POLICY DEBATE: COMPETING PORTRAYALS OF TECHNOLOGY IN ONLINE CONTENT REGULATION AND LESSONS FROM SCIENCE AND TECHNOLOGY STUDIES

by

Jeremy Mauger

A Dissertation Submitted in

Partial Fulfillment of the

Requirements for the Degree of

Doctor of Philosophy

in Information Studies

at

The University of Wisconsin-Milwaukee

December 2014

ABSTRACT
FRAMING THE POLICY DEBATE: COMPETING PORTRAYALS OF TECHNOLOGY IN ONLINE CONTENT REGULATION AND LESSONS FROM SCIENCE AND TECHNOLOGY STUDIES

by

Jeremy Mauger

The University of Wisconsin-Milwaukee, 2014
Under the Supervision of Professor Michael Zimmer, Ph.D.

In an effort to control access to certain online content, the U.S. Congress has repeatedly mandated the use of powerful regulatory technologies such as Domain Name System blocking, Internet Service Provider filtering, age verification systems, and commercial filtering software. The application of these enforcement mechanisms may have serious implications for constitutional rights, individual freedom, and autonomy. This research will show that policies including the Communications Decency Act, the Child Online Protection Act, the Children's Internet Protection Act, the Stop Online Piracy Act, and the PROTECT Intellectual Property Act all have the potential to negatively impact these rights. Although the motivations for these policies differ, each requires the use of technologies that legislators have often portrayed as instrumentally useful tools. The primary question at the core of this project is to ask how Congress may have misunderstood these mechanisms and may have failed to recognize the political and constitutional impact they can have. By understanding how lawmakers have portrayed technology, it will be possible to offer recommendations for injecting a more critical understanding of these regulatory technologies within the policy process. This understanding relies on core concepts from Science and Technology Studies.

This dissertation is dedicated to my wife Angela and our son Jacob who have inspired me to work hard and have fun doing it. I love you both.

I would also like to thank my parents, John and Karen Mauger, who helped me pursue my education and taught me to love learning.

TABLE OF CONTENTS

Chapter 1: Introduction

- Introduction– p. 1
- Introduction to the CDA, COPA, CIPA, SOPA, and PIPA – p. 4
- Identifying Frames and the Theoretical Lens – p. 7
- Normative Framework – p. 15
- Summary – p. 17

Chapter 2: Theoretical Framework: Science and Technology Studies

- Introduction – p. 19
- Technology is Political and Non-Neutral – p. 20
- Technological Ordering – p. 22
- Advocacy and Local Knowledge – p. 24
- Governance – p. 27
- Alternative Models of Internet Governance – p. 30
- Technical Rationality and Political Design – p. 35
- Affordances – p. 40
- Hegemony – p. 42
- Conclusion – p. 46

Chapter 3: Methodology

- Methodological Framework: Frame Analysis – p. 48
- Frame Analysis Accommodates the Theoretical Lens of STS – p. 61
- Research Questions – p. 64
- Data Selection – p. 67
- Coding Scheme – p. 70
- Data Coding and Analysis – p. 73
- Delimitations – p. 78
- Summary – p. 79

Chapter 4: The Communications Decency

- Introduction – p. 81
- Part I – Legislative Master Frames – p. 82
- Part II – Oppositional Master Frames – p. 93
- Part III – Legislative Diagnostic Frames – p. 101
- Part IV – Oppositional Diagnostic Frames – p. 109
- Part V – Legislative Prognostic Frames – p. 120

- Part VI – Oppositional Prognostic Frames – p. 126
- Part VII – Judicial Opinion – p. 132
- Communications Decency Act Documentation Index – p. 145

Chapter 5: The Child Online Protection Act

- Introduction – p. 147
- Part I – Legislative Master Frames – p. 148
- Part II – Oppositional Master Frames – p. 157
- Part III – Legislative Diagnostic Frames – p. 169
- Part IV – Oppositional Diagnostic Frames – p. 175
- Part V – Legislative Prognostic Frames – p. 182
- Part VI – Oppositional Prognostic Frames – p. 187
- Part VII – Judicial Opinion – p. 194
- Child Online Protection Act Documentation Index – p. 205

Chapter 6: The Children's Internet Protection Act

- Introduction – p. 207
- Part I – Legislative Master Frames – p. 208
- Part II – Oppositional Master Frames – p. 219
- Part III – Legislative Diagnostic Frames – p. 230
- Part IV – Oppositional Diagnostic Frames – p. 237
- Part V – Legislative Prognostic Frames – p. 246
- Part VI – Oppositional Prognostic Frames – p. 254
- Part VII – Judicial Opinion – p. 262
- Children's Internet Protection Act Documentation Index – p. 274

Chapter 7: The Stop Online Piracy Act and PROTECT Intellectual Property Act

- Introduction – p. 277
- Part I – Legislative Master Frames – p. 278
- Part II – Oppositional Master Frames – p. 288
- Part III – Legislative Diagnostic Frames – p. 297
- Part IV – Oppositional Diagnostic Frames – p. 306
- Part V – Legislative Prognostic Frames – p. 316
- Part VI – Oppositional Prognostic Frames – p. 322
- Stop Online Piracy Act Documentation Index – p. 330

Chapter 8: Theoretical Discussion and Conclusion

- Introduction – p. 332
- Technical Rationality – p. 334

- Technological Affordances – p. 342
- Neutrality, Subjectivity, and Bias – p. 346
- Technology is Political – Liberty – p. 349
- Technology is Political – Autonomy – p. 351
- Hegemony – p. 357
- Non-Democratic Power Relations – p. 363
- Technological Ordering – p. 367
- The Legislative Relationship to Technology – p. 370
- Recommendations and Conclusion – p. 374

References – p. 379

Curriculum Vitae – p. 390

LIST OF FIGURES

- Figure 1: Coding Scheme – p. 72
- Figure 2: COPA Commission Scattergram – p. 176

LIST OF TABLES

- Table 1: Legislative and Oppositional Documents Collected – p. 69
- Table 2: Primary Oppositional Groups Represented – p. 70
- Table 3: Sample Code Indicators – p. 74
- Table 4: Coding Totals – p. 77
- Table 5: Communications Decency Act Frame Analysis Summary – p. 144
- Table 6: Child Online Protection Act Frame Analysis Summary – p. 204
- Table 7: Children's Internet Protection Act Frame Analysis Summary – p. 273
- Table 8: Stop Online Piracy Act/PROTECT IP Act Frame Analysis Summary – p. 329

ACKNOWLEDGMENTS

I would like to thank my dissertation committee for their continued support and guidance throughout this process. Dr. Michael Zimmer has been my mentor from the start, constantly going the extra mile to guide me through seminars, research projects, and even creating courses when none existed. Dr. Nadine Kozak who introduced me to the finer points of Science and Technology Studies and always had one more book to recommend. Dr. Charles Ess who has provided encouragement, friendship, and opportunities abroad. Dr. Maria Haigh who helped shape this dissertation as it worked its way through the proposal phase. Finally, Dr. Grace Chikoto who taught me how to approach policy studies and generously agreed to serve on a committee that was way outside of her department. Thank you all.

Chapter 1 – Introduction

Introduction

Jim Exon did not use the Internet much.[1] Like many people in the mid-1990s he did not truly understand what it was or how it worked but he did recognize the World Wide Web as having the potential to "rival the invention of the printing press and broadcasting in terms of how it will affect our daily lives" (Exon, 1995). Unfortunately, along with this potential he saw the Internet as a threat, a threat to decency, and a threat to vulnerable children who might stumble across pornographic pictures and videos, predators and perverts. After all, dangerous and indecent content was only "a few click-click-clicks away from any child" when they ventured online (141 Cong. Rec. S8088, 1995). The Internet, for all its revolutionary implications, was a dangerous frontier that required regulation. Exon knew that online speech was important, knew that it often qualified for constitutional protection, but like many concerned parents, he did not believe the First Amendment was "so sacrosanct that we must stand idly by while our children are inundated with pornography and smut on the Internet" (Id). Although he did not know much about it or use it himself, Mr. Exon knew that the Internet was a problem that Congress must fix before it could harm innocent children. What set him apart from others with similar concerns was that, as the Democratic Senator from Nebraska, Mr. Exon was in a unique position to do something about it.

If the problem was endemic to this new technological medium of the Internet, it seemed self-apparent that technology might also provide the solution. As the co-sponsor

[1] As noted by Cannon (1996, pp. 72-73), "At no time did Senator Exon ever profess personal experience on the Internet. His staff indicated that he had no first-hand Internet experience. The material that Senator Exon presented from the Internet to the Senate was always downloaded by someone other than himself."

of the Communications Decency Act (CDA) of 1996, this is exactly what Exon and other legislators proposed. By using age verification systems and Internet service providers themselves to police content, the federal government could accomplish the online equivalent of confining adult bookstores to the seedier part of town. As Exon put it, "Just as we have laws against dumping garbage on the interstate, we ought to have similar laws for the information superhighway" (Id). Regardless, in their haste to protect children from this "garbage," Senator Exon and most of Congress failed to realize just how seriously the technological "solutions" they were proposing would constrain access to constitutionally protected speech.

In fact, the CDA prompted an almost instantaneous legal challenge from the American Civil Liberties Union. Based on the requirements of the law and the technological conditions under which Congress regulated content, the ACLU and others argued that the limits imposed on protected speech by the CDA generally and its technological mechanisms of enforcement specifically were unacceptable within the framework of U.S. Constitutional guarantees. The ACLU recognized that "because of the nature of online communications, a substantial number of content providers…simply have no technologically or economically feasible way of screening out minors; the CDA thus becomes a total criminalization of constitutionally protected 'indecent' or 'patently offensive' speech" (ACLU Plaintiffs' Post-Trial Brief in Support of Their Motion for a Preliminary Injunction, 1996). The Supreme Court would unanimously find in favor of the ACLU in the landmark case, *Reno v. ACLU*. The Court underlined the ACLU's point that there was no way for the technological arrangement required by the law to function constitutionally within the context of the legislation.

At the heart of this case lay Senator Exon and Congress' fundamental misunderstanding of the Internet and the technological mechanisms of enforcement necessitated by the CDA. Although there is a distinct possibility that Senator Exon "fundamentally misunderstood the medium which he sought to regulate", the more pressing issue is "how a senator with no technical knowledge of the [Internet] can draft language which regulates it" (Cannon 1996, pp. 72-73). Particularly in a circumstance where Congress applied more technology to fix the perceived problem, it may have been inevitable that Exon and other lawmakers equally unfamiliar with such systems failed to recognize just how deeply those systems could affect individual rights. Congress could not begin to assess the implications of what they proposed without a critical understanding of the Internet and the technological mechanisms of enforcement that they imposed to regulate it. This is a recurring theme in recent legislative history where lawmakers have attempted to regulate the Internet at the national level. In addition to the CDA, the Child Online Protection Act (COPA), the Children's Internet Protection Act (CIPA), the Stop Online Piracy Act (SOPA) and the PROTECT Intellectual Property Act (PIPA) exemplify this phenomenon. To date, these have been the major federal attempts to manage online content in the United States. In each case, Congress has mandated the use of powerful regulatory technologies often vaguely described as "technology protection measures" (see CIPA) and individual rights have consistently been implicated as a result. Below is a more detailed introduction to these policies and their key requirements.

Introduction to the CDA, COPA, CIPA, SOPA, and PIPA

With passage of the Communications Decency Act (CDA) in 1996, the United States took its first steps to construct policy designed to regulate Internet content on a national scale. Legislators intended the CDA to address the issue of minors' access to indecent and pornographic content on the Internet. As the means to address this problem, Congress offered two primary solutions. The first required that any online content producer or provider implement age verification systems in order to ensure that children would not be able to proceed to the harmful content beyond the verification screen. The primary surrogate for proof of age would be credit or debit card information and/or the creation of an online identification. Second, the Internet service and network providers that controlled access for customers would be obligated to screen for indecent content on their systems. The CDA would afford these service providers with legal immunity for all such blocking and filtering actions taken in good faith for the protection of children. Several oppositional groups led by the American Civil Liberties Union (ACLU) would oppose these policies both publicly and in the courts. The substance of the argument was that the CDA's broad definitions of indecency and the technological enforcement mechanisms it required placed too severe a burden on constitutionally protected speech. As will be described, the Supreme Court eventually struck down this Act on these grounds in the case of *Reno v. ACLU* (1997).

The Child Online Protection Act (COPA) of 1998 was the immediate successor to the CDA and lawmakers had a similar desire to protect children from online pornography. In an effort to address the Supreme Court's concerns (and, by inference, the concerns of the opposition), Congress shifted the scope and target of enforcement.

Specifically, while COPA would continue to require the implementation of age verification systems as the primary mechanism of enforcement, Congress would narrow the breadth of enforcement from all content providers to only commercial outlets. Despite the adaptations embedded within this policy, it too faced strong opposition from a number of groups. Again, the ACLU and other organizations such as the Center for Democracy and Technology (CDT) argued that this policy was overly broad and unduly burdensome for protected speech. In particular, even the limited use of age verification systems was onerous for adult access and did not accommodate First Amendment protections. This challenge led to a temporary injunction barring enforcement of the Act and, after a lengthy legal battle over this policy and its technological provisions, the courts imposed a permanent injunction.

Following the defeat of both the CDA and COPA, Congress passed the Children's Internet Protection Act (CIPA) of 2000. For the third time, Congress attempted to protect children from potentially harmful material on the Internet and relied on technological solutions to accomplish its goal. In this case, however, legislators proposed a drastic shift from either of the policies that had preceded CIPA. Specifically, CIPA narrowed the focus of enforcement even further, limiting regulation only to public schools and public libraries. In addition to confining the policy to these venues, legislators called for the use of commercial filtering software as the primary regulatory system. This differed significantly from the broad application of age verification systems at the level of Internet speakers and, instead, limited access only at the level of recipients. Again, despite this regulatory adaptation, oppositional groups took issue with the constitutionality of CIPA and commercial filters. Led by the American Library

Association (ALA), the opposition argued that this policy and this technology unduly limited access to a considerable amount of protected speech and that it harmed the ability of adult library patrons to seek out protected speech within a public institution. Like the CDA and COPA before it, CIPA would face a Supreme Court challenge. What sets CIPA apart is that the Court did not find either the policy or its technological mandate to be significantly burdensome for adult access to protected speech and the policy remains in force today. Despite this, and as will be discussed, the application of CIPA has been problematic and has led to additional legal challenges.

With CIPA Congress was finally able to implement policy that addressed the goal of protecting children from indecent material online. In addition to this, legislators have since pursued content regulation schemes in other policy domains as well. For example, in 2011 Congress proposed the Stop Online Piracy Act (SOPA) in order to halt the theft of intellectual property on the Internet. The Senate introduced the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of (PROTECT IP Act or PIPA) almost simultaneously to SOPA. The goals of both SOPA and PIPA were identical and each proposed that technological mechanisms must address the problem of online piracy including Domain Name System (DNS) blocking of allegedly infringing sites and the adulteration of search engine results to halt the flow of traffic to these sites. Oppositional groups took issue with these policies as well and argued that the law would affect a number of legitimate websites and entangle a great deal of protected speech in the state's regulatory scheme. Due to the public and political unpopularity of these Acts, neither would reach a vote in Congress.

Identifying Frames and the Theoretical Lens

Throughout all of these examples, the primary question at the core of this dissertation asks how federal legislators may have misunderstood technology and may have misused technological systems in an attempt to "fix" the Internet by regulating content online. Specifically, have lawmakers applied these systems without a critical understanding of how regulatory technologies can impact individual rights, freedom, and autonomy? This potential for misapprehension of regulatory technology leads to important and novel research questions that will be the focus of this dissertation. Broadly put, have lawmakers misunderstood technology and misapplied it as a tool to effect policy? If so, where in the policy process are these conceptual errors most prevalent? By understanding how lawmakers might have (mis)portrayed technology and where in the policy process these mistakes have occurred, it will be possible to offer recommendations for injecting a more critical understanding of technology within that process.

In order to address these broad questions, this research will first identify the initial motivations for these policies (e.g. protecting children, protecting intellectual property and protecting national security) and will describe how those justifications have or have not included a simplistic assessment of technology. Next, this research will isolate moments within the policy process where lawmakers chose to portray aspects of the Internet as problems that required intervention through policy and where they chose to employ technological systems as the means to address those problems. This research is necessary and novel in that it will identify instances within the legislative process where this potentially naïve portrayal of technology may have manifested. Understanding where and how this occurs will help to demonstrate why these policies have consistently

met with constitutional difficulties and will pinpoint where a more critical view of technology might fit within the process of policy formulation, negotiation, or even implementation. This dissertation will argue that inserting a critical assessment of technology into the policy process at these points will help to remedy the constitutional and ethical difficulties that these laws have so consistently caused.

In order to isolate how and where these kinds of misunderstandings about technology manifest, the policy process itself will be organized into discrete segments in order to locate instances where Congress has failed to recognize that technology is not simply a neutral tool free from ideological and political bias (see Friedman & Nissenbaum, 1996) and that regulatory technologies are not simply expedient policy instruments (Brey, 2006, p. 360). To accomplish this, each of the policies listed above will be broken down into frames and a "frame analysis" (Goffman, 1974) will be conducted. These frames can be divided into three categories: first are the "master frames" (Williams & Benford, 2000, p. 134) that describe the initial motivations and justifications for these policies; next are the "diagnostic frames" (Benford & Snow, 2000, p. 615) that illustrate how lawmakers have rhetorically defined aspects of the Internet as "problems" that require federal intervention; and third are the "prognostic frames" (Id) that demonstrate how lawmakers have proposed to solve the perceived problem through policy and through regulatory technologies. Across all of these frames, it will be necessary to examine how legislators are portraying technology. It is crucial that this analysis categorize policies into these frames in order to locate precisely Congress may have inaccurately portrayed technology as a neutral object and how it is being misapplied in a way that implicates individual rights. Locating these instances also serves to isolate

points in the process where a more critical view of technology can and should be included.

For example, as federal legislators, Exon and other supporters of the CDA recognized the need to protect children from "smut" (Exon, 1995), identified the Internet as a "unique medium" (Id) that offered unprecedented access to this kind of harmful content and proposed a unique solution to the problem in the form of regulatory technologies that would essentially zone this material to the dark corners of the Web. What Exon and others may have failed to do at any point within these frames was adequately recognize that the technological fix they were proposing could impose its own ideology on citizens and unduly limit access to protected speech. The philosophy of those designing regulatory technologies and the systems that actually made filtering decisions on behalf of Internet service providers were not themselves impartial. As social science and technology scholar Wiebe Bijker has argued, technologies, including these systems, are shaped by social processes and value judgments, political perspectives and normative rationales (1997, p. 281). By their very nature, these technological enforcement mechanisms restrict access and impose points of view on the individual user that may be as distasteful to them as pornography was to Senator Exon. What is required in these instances and what this dissertation will demonstrate is that Congress must examine the political, constitutional and ethical implications of regulatory technologies when formulating broad "information policies" (Trauth, 1986, p. 41) such as these. Examining how these systems can impact rights and freedoms when mandated by federal law is a prerequisite for crafting sound policy and this research will dissected each of the laws identified above into frames in order to illustrate this point. Lawmakers must

scrutinize the design of regulatory technologies, the potential biases of these systems, and the implications they have for constitutional rights. Describing the legislative portrayal of technology within all of these policies and identifying specific instances in the policy process that would benefit from a critical understanding of technology is one of the primary scholarly contributions of this dissertation. The principal data set for this portion of the research includes direct documentary evidence taken from the legislative process. In addition to the policies themselves, this analysis will include legislative histories, congressional reports, press releases, and other public statements of key legislators. This documentation most thoroughly articulates the fundamental frames employed by lawmakers.

Parallel to this investigation of the legislative process, this dissertation will demonstrate how oppositional groups have already used these critical points of view to redefine these kinds of information policies and their associated regulatory technologies. For example, in the case of the CDA, the American Civil Liberties Union provided a much more nuanced discussion of the nature of these systems and the potential harm they could cause to individual rights. As mentioned above, the Supreme Court's unanimous opinion in *Reno v. ACLU* validated the critical analysis of technology presented by the ACLU. This validation strongly suggests that Congress could benefit from this kind of critical understanding and, if it were to be included in the policy process from the outset, legislators could address many of the legal and constitutional difficulties these laws have faced prior to implementation. In addition to isolating points in the legislative process where this critical perspective can be most usefully inserted, this dissertation will identify instances where oppositional frameworks have employed exactly this kind of critique.

Again, it will be necessary to break down the oppositional process into key frames in order to locate those moments. The identification of master, diagnostic, and prognostic frames are crucial for this analysis as well and will provide a novel contribution to the study of oppositional movements in the context of information policies such as the CDA, COPA, CIPA, SOPA, and PIPA.

Additionally, this research will demonstrate how the judiciary has taken up the critical view of technology used by these oppositional groups. Court rulings are used here as the benchmark for the validity of these critical perspectives because they provide the final judgment of how these policies and their technological mechanisms of enforcement impact the constitutional rights and civil liberties of the populace within the context of the U.S. political system. Several of the policies analyzed throughout this dissertation have come before the Supreme Court and, because of the arguments put forward by oppositional groups, have either been struck down as unconstitutional or have been heavily modified to ensure that the regulatory systems they require function constitutionally in application. Based on the frames presented by the opposition, the Court has consistently recognized that these technologies function politically in the sense that they deeply impact individual rights.

Furthermore, because various courts have found these policies to be constitutionally unsound, these laws have had to evolve and shift. After the Supreme Court struck down the CDA, Congress attempted to narrow the scope of the law and its enforcement mechanisms in order to address this constitutional infirmity. Due to the more technologically nuanced arguments put forward by the opposition and the endorsement of those arguments by the Court, the law shifted slightly resulting in passage

of the Child Online Protection Act. When the Court struck down COPA for many of the same reasons as the CDA, Congress tried yet again to pass similar legislation. When the Children's Internet Protection Act became federal law in 2000, legislators had again narrowed the scope of enforcement, this time strictly to minors in certain controlled locales, thereby shifting the focus of the policy and its technological enforcement. Although challenged on similar grounds, the Court eventually found CIPA to be constitutional as long as Congress placed significant limits on the filtering mechanisms required by the law. Despite this, it is possible that legislators again failed to consider the political nature of the technologies they were proposing and CIPA may yet face additional constitutional hurdles (see *Bradburn v. NCRL* and *PFLAG v. Camdenton).* One of the goals of this dissertation is to examine whether or not these shifts in policy relate directly to the opposition's competing framework. Again, these competing oppositional frameworks often include the assertion that a critical view of technology must be included within the structure of the policy's enforcement. As long as this critical view is absent from the policy process, information policies such as these will continue to face constitutional obstacles.

Although a wide array of individuals and organizations have opposed these policies in a variety of ways, this dissertation will focus on those groups that were most active in challenging these laws, the most vocal in their criticism and that most effectively employed a critical understanding of the Internet and associated regulatory technologies. Particularly in the examples of the CDA, COPA, and CIPA, those organizations primarily responsible for articulating and advancing the opposition were those that pursued legal action against the policies on constitutional grounds. While

several organizations may have spoken publicly on issues related to these laws, only a few were active in the judicial process (and had the financial clout to pursue such challenges). These primary oppositional actors are, for the most part, the named plaintiffs in these actions. These groups filed the initial complaints and various court documents that will be part of the fundamental documentary evidence for this research. Additionally, this research will analyze the amicus briefs, expert reports, press releases, and other public statements made by these groups as they relate to key frames and to technology.

Although identifying key frames within direct documentary evidence is crucial to this research, it is not enough to chide the legislative branch for its apparent misunderstanding of technology or its failure to recognize the impact regulatory technologies can have on individual rights. It is also insufficient to compliment oppositional groups for the clarity of their argument. Equally, isolating instances in the policy process where critical perspectives can be included is useful but incomplete. In order for this research to provide a more meaningful contribution to policy research, in order to enrich the methodology of frame analysis and to explain what, exactly, a critical view of technology looks like, it is necessary to provide a specific lens for the consideration of frames. The theoretical framework that most thoroughly critiques the political nature of technology, technological systems, and their impact on individual rights, freedom and autonomy is Science and Technology Studies (STS). Additional work from the philosophy of technology (such as Andrew Feenberg's critical theory of technology and Philip Brey's disclosive ethics) will be considered as well but perspectives from STS provide the fundamental structure necessary to guide the analysis

of both legislative and oppositional frames and can offer a roadmap of sorts for lawmakers when considering information policies of this kind in the future. By including perspectives from STS, this research can more adequately address why a critical assessment of technology needs to be part of the policy process and how oppositional groups have already advanced such viewpoints so successfully. As will be explained more thoroughly in Chapter 2, STS as a field of study is fundamentally concerned with the socially constructed nature of technology and the ideological biases that the design process can embed within it. As STS pioneer Langdon Winner has argued, one of the core theoretical assumptions of STS literature is that the technologies used to implement and enforce social policy are not merely tools. Instead, "What appear to be nothing more than useful instruments are…enduring frameworks of social and political action" (Winner, 1986, p. x).

Contrary to this more nuanced view, there appears to be a pervasive attitude in policy circles implying that regulatory technologies are intrinsically impartial and unbiased. This perspective holds that "tools and technical systems are inherently ideologically neutral. Individuals with particular axes to grind may employ a tool to achieve their ends, but this does not make the tool itself ideological" (Pitt, 2000, p. 72). The rationalist underpinnings of science and the perceived nature of the technological design process leads some legislators to believe that these "tools" are apolitical. From this point of view, technology has no values of its own or ideology embedded within it through the course of its development (Feenberg, 1991, p. 5). This "neutrality thesis" (Brey, 2010, p. 43) suggests that technological artifacts can be applied in any number of ways without consequence. In contrast, as technological ethicist Deborah Johnson has

argued, "It is now well-accepted…that technology…is value-laden…that technologies are developed in a social context that pushes and pulls and shapes its development" (Johnson, 1997, p. 20).

Normative Framework

It is important to note that this dissertation and this author proceed from the normative position that access to information is a benefit to the individual and to democratic society. This principle ensures that "those resources and circumstances necessary for living a minimally good life" (Nickel, 2007) remain unrestricted. The ability to read, write, speak, and listen without undue constraint from the state is crucial to the ability of the citizen to exercise individual autonomy and for the state to function for the benefit of its citizens. As Philip Brey has noted, individual autonomy is a good in itself because "it ensures that human beings are able to draw out their own life plans that reflect, as much as possible, values and needs of their own, instead of those of the government or of other citizens" (1998, p. 2). Therefore, access to information serves both individual interests and the interests of a democratic state. This supports the suggestion that, "A minimally good human life is not possible without access to a rich array of expressions and to knowledge for both practical ends and intrinsic benefits to the human spirit" (Mathiesen, 2008).

The exercise of individual autonomy is dependent on a number of freedoms including the freedom to speak, listen, and access the information necessary to make decisions that reflect the person's motivations, values, and goals (Brey, 1998, p. 2). This is equally true when considering access to the vast informational resource and democratic forum that the Internet has become. From this perspective, any policy or technology that

Congress implements to restrict access online requires thoughtful analysis prior to its application. In the U.S. constitutional context, the First Amendment increases the state's responsibility to its citizens in this regard and demands that policy preserve adult access to protected speech. If we accept the idea that access to information is a basic right and a boon to society, then Congress bears the burden of proving that the policies they choose to implement and the technologies they choose to employ do not illegitimately damage this fundamental good. The normative framework for this dissertation is fundamentally based on John Stuart Mill's assertion that there "ought to exist the fullest liberty of professing and discussing, as a matter of ethical conviction, any doctrine, however immoral it may be considered" by the state (1859/2008, p.26). Embedded within this assumption is the ideal that discussion is meaningless without access. If the individual is unable to hear and speak or is otherwise restricted from participating in the conversation, then a basic right has been illegitimately constrained.

That being said, there are and should continue to be some constraints on the exercise of free speech. Lawful restraints on individual speech and the First Amendment are not mutually exclusive. As First Amendment advocate Alexander Meiklejohn has suggested, "When self-governing men demand freedom of speech…They do not declare that any man may talk as he pleases, when he pleases, about what he pleases, about whom he pleases, to whom he pleases" (1948/2004, p. 24). Democratic societies can and should restrict speech and access when, for example, the welfare of a child is at risk. This is equally true when speech directly incites violence or causes injury. The problem with this and the question taken up by this dissertation is; how do we enforce any "exceptions to the presumption of free speech [and access] in such a way that consistent

application of the principle doesn't permit less desirable censorship" (Warburton, 2009, p. 4)? The normative framework presented here suggests that the application of technological barriers to access, as mandated by the CDA, COPA, CIPA, SOPA, and PIPA, directly causes undesirable censorship. The motivations of policymakers in these examples may superficially appear to qualify as valid restraints on access and speech because lawmakers desire to protect children from indecent content, protect property rights, and defend national security. Despite this, a careful analysis of the enforcement mechanisms used to accomplish these seemingly worthwhile goals demonstrates that a great deal of legitimate speech is subject to the state's regulatory zeal. Particularly when the state sets limits on adult access to speech it deems controversial, this damages the constitutional foundations of democratic society and the ability of the individual to decide what constitutes information that is right, proper, and necessary.

Summary

By employing an STS framework to unpack legislative frames, this research can identify instances where lawmakers have failed to consider technology critically. STS also provides a means for addressing how oppositional frames have used a more nuanced argument that includes this technological critique to great effect. This research will also illustrate how judicial rulings have incorporated oppositional frames dealing with technology as well as how those frames and judicial opinions may have forced an incremental shift in the scope and technological enforcement of these policies. Finally, by showing how STS can improve the formulation of these kinds of laws and where in the policy process STS can be included to the greatest benefit, this research can provide a set of coherent recommendations. This dissertation will demonstrate that the inclusion of

STS perspectives within key frames can result in better outcomes for lawmakers and a better, more thoughtful use of regulatory technologies. By improving the policy process and ameliorating constitutional deficiencies prior to implementation, Congress can better preserve the rights and autonomy of individual citizens.

Following the literature review and methodology sections in Chapters 2 and 3, this dissertation will proceed with a frame analysis of the CDA (Chapter 4), COPA (Chapter 5), CIPA (Chapter 6), and SOPA/PIPA (Chapter 7). Each of these chapters will describe these policies in depth and will detail the master, diagnostic and prognostic frames for each. Chapter 8 will provide a theoretical discussion analyzing several core concepts from Science and Technology Studies alongside this descriptive frame analysis. Finally, this dissertation will conclude by offering some recommendations for including these critical perspectives from STS within the policy process so that lawmakers may create more sound policy going forward.

Chapter 2 – Theoretical Framework: Science and Technology Studies (STS)

Introduction

In order to undertake the research described above, perspectives from Science and Technology Studies (STS) will help describe the frames of both legislative and oppositional groups. STS will be the theoretical lens employed in conjunction with the frame analysis methodology because, as Richard Sclove's work on democracy and technology suggests, it recognizes that "all government policies involving technology need to be reevaluated from the standpoint of their implications for achieving a more democratic technological order" (1995, p. 224). The intersection of policy, technology and democratic rights relates directly to the fundamental principles of STS research making this discipline the most appropriate for addressing policies that attempt to regulate online content including the CDA, COPA, CIPA, SOPA and PIPA. This is particularly true in the context of this research where specific moments within the policy process are to be unpacked and described. As communications studies researcher and STS contributor John Monberg suggests, STS can help provide a "rich analysis of the complex and tentative nature of policies" and can "identify multiple points of intervention" within policy deliberations "that can expand the democratic potential of the Internet" (2005, p. 283). One of the primary goals of this dissertation is to provide that kind of analysis to the policies listed above and to help both policymakers and oppositional groups realize this democratic potential.

While frame analysis provides an organizational tool for isolating how groups portray technology within key frames and points within the policy process where misunderstandings may occur, STS explains how technology functions politically and

how it can constrain individual rights. Broadly stated, STS is "an interdisciplinary field that is creating integrative understanding of the origins, dynamics and consequences of science and technology…STS scholars engage activists, scientists, doctors, decision makers, engineers and other stakeholders on matters of equity, policy, politics, social change, national developments and economic transformation" (Hackett, et al., 2008, p. 1). STS can also critically examine the use of regulatory technologies, the scientific expertise that underpins them, and how that expertise is "produced, maintained, stabilised, closed, contested or negotiated" (Guggenheim & Nowotny, 2003, p. 242). This is particularly useful in the context of entrenched political institutions and the oppositional groups that have arisen to contest policies that depend on instrumental understandings of policy and technological enforcement. The scope and intent of STS research can address the frames employed by both legislators and oppositional movements and can describe their varying portrayals of technology as well as technology's place in policy. Some core concepts from STS can help describe these processes and may offer insight into the implications they may have for democratic society.

Technology is Political and Non-Neutral

This is particularly true in an environment where policymakers may not be aware of the political ramifications of the technologies they are employing to solve social problems. Policies such as those addressed in this dissertation mandate the imposition of technological systems to regulate the terms and conditions under which individuals may access information online. Not only is the use of technology in these instances a political decision, but it is also increasingly the manner in which policy goals are accomplished (Winner, 1977, p. 323). STS researchers Emilie Gomart and Maarten Hajer suggest that

STS as a field acknowledges this, provides the tools necessary for critically evaluating technology in such a situation and "STS has a long tradition of warning [against] 'technological fixes'" (2003, p. 55). Specifically, some STS scholars have recognized that "Politics…takes the form of a general concern about which political systems, institutions, and understandings; which participants with what qualifications, roles, and responsibilities; and which kinds of civil society would be most democratic while preserving the benefits of scientific and technical expertise" (Hackett, et al., 2008, p. 3).

STS research can also help to explain how and why some legislators may have failed to address the regulatory technologies they have mandated through policy. Specifically, it is possible that lawmakers have proceeded from the position that age verification systems, DNS blocking and even commercial filtering software are apolitical instruments of action. From this view, as political theorist Yaron Ezrahi has noted, technology and the scientific processes that underpin its design seem above reproach. As the products of scientific reasoning, technological artifacts appear "non-arbitrary, impersonal and therefore rarely contestable" from a legislative point of view (Ezrahi, 2003, p. 64). These tools, then, provide a means to exercise governmental force without the appearance of bias and with complete viewpoint neutrality. The scientific method and the mechanisms it creates appear to stand apart from the social and political processes that define policy and some legislators have demonstrated a keen "willingness to privilege science based technologies as neutral modes of action" (Id). This reifies "expert" knowledge and allows those in Congress to apply seemingly neutral technological objects without first exploring their implications for rights and autonomy.

Why should the state investigate such a possibility if scientific rationality and the technical design process have already stripped these objects of any values or biases?

Technological Ordering

Legislative action, then, requires these technological mechanisms to "appear distinct from political authority" (Ezrahi, 2003, p. 64). Congress may portray such "tools" as the best means to accomplish the instrumental ends of policy. Despite this, as STS has recognized, this fails to account for the socially constructed and contingent nature of technological design. This perspective also obscures the kinds of power relationships that may result from broad application of these regulatory systems. As anthropologist and political scientist James Scott has suggested in his work on technocratic ordering by the state, these uncritical political processes can demonstrate "the dangers of dismembering an exceptionally complex and poorly understood set of relations and processes in order to isolate a single element of instrumental value" (1998, p. 21). As will be described in the examples of the CDA, COPA, CIPA, SOPA, and PIPA, these policies drastically altered the complex relationships of those speaking and listening on the Internet through the application of apparently neutral tools. In Scott's view, this technological exercise by the state exemplifies "high modernism" (Id, p. 90). High modernism demonstrates a tendency within government to apply the "benefits of technical and scientific progress" uncritically across a wide variety of actions (Id). While the intent of these policies may be benevolent, by employing technology in this way, lawmakers can strip the individual of his or her rights and basic freedoms because they have failed to account for the impact these systems may have on the complex speaker/listener relationships that constitute Internet-based discourse.

Specifically, the goal of the high modern state is to engineer a society according to rationalist scientific and technological principles. This eliminates the ambiguity of societal practice dictated by "custom and historical accident" and allows the state to order the activities of the individual according to "conscious, rational, scientific criteria" (Id, p. 92). From this view, the exercise of rights and the implementation of technocratic policy appear to be distinct and separate phenomena. If the state is applying the fruits of science and technology for the benefit of its citizens and if technological policy instruments are apolitical due to the neutrality of the design process, this does not implicate the freedom and autonomy of the individual. Despite this, the relationships dictated by the use of regulatory technologies at the policy level and the individual activities constrained by those systems lead to the opposite conclusion. As STS researcher Sheila Jasanoff has argued, instead of standing apart from technology or "lying in an altogether separate normative domain," the rights and freedoms of the citizen are "being constituted in significant part through technology" (2003, p. 164).

Legislative supporters of those policies at issue here appear to have been oblivious to the assertion that individual rights may become subordinate to the political nature of technological mechanisms of enforcement. The use of these technologies can be constitutive in the context of freedom and autonomy due to the affordances they provide (or lack) (Brey, 1998, p. 2). As Internet law scholar Lawrence Lessig (1999) has argued, this may be especially true in a technological environment such as the Internet where access and choice may be entirely subservient to technological architecture and code. This does not imply technological determinism - quite the opposite. The high modern society has chosen to construct a technological regulatory environment where

Congress applies artifacts like commercial filtering software uncritically. Equally, scientists and technologists have designed systems that embed, reflect, and advance a distinct set of norms and values. The Internet also embeds values and ideology and, as Tim Berners-Lee (the Web's original designer) has suggested, from the beginning designers intended the Internet to allow for the broad dissemination and receipt of information without prioritizing messages based on their content (2010). When policy demands the imposition of technological barriers to access that impede this design principle, something is lost. Again, this diminishment of the Internet's communicative potential is unacceptable if the state applies such systems without some critical understanding of their nature. Nevertheless, these choices are completely within our control. Exposing both technology and policy to critical review allows us to unpack these contradictions and implications. As historian and STS scholar Gabrielle Hecht (1998) has argued, "Opening the black boxes of culture and technology *simultaneously* can…give us insight into how technologies constitute a terrain for transforming, enacting, or protesting power relations within the social fabric. Taking politics [and technology] seriously as objects of analysis greatly deepens our understanding" of both (p. 10, emphasis in original).

Advocacy and Local Knowledge

The problem here, then, is to identify when those policy choices and design practices clash with democratic rights, constitutional guarantees, and individual agency. As instruments of federal policy, these technological barriers to access, and the values they embody, have the significant ability to determine the boundaries of behavior and the borders of access. Essentially, lawmakers have imbued these technologies with

"constitutional force" and, as such, that force "should be explicitly authorized" (Jasanoff, 2003, p. 175). Without such authorization, these systems have received governmental approval in the absence of thoughtful deliberation. It is no wonder, then, that poorly understood technologies hinder rights when the state delegates its police power to them. This is entirely unacceptable in the context of U.S. constitutional guarantees and is particularly tragic considering the potential of the Internet as a vast democratic forum. Rather than being constrained, these freedoms could and should be magnified and enhanced by technology. Again, this is not to suggest that these technologies determine the actions of individuals but instead, as sociologist and STS scholar Chandra Mukerji has argued, these artifacts shape the material conditions within which politics and dissent may be exercised (Mukerji, 2007). As Jasanoff has suggested, "For good or for ill, science and technology are important aids to human self-expression, not merely iron cages within which a passive humanity languishes imprisoned by forces beyond its control" (2003, p. 174). Therefore, if we allow it through ignorance or indifference, poorly understood regulatory technologies become the means for illegitimate control rather than empowerment.

In addition to recognizing this condition of the high modern society, it is important to treat "expert" scientific and technical knowledge with a degree of skepticism. By accepting the efficacy and neutrality of regulatory systems as a given, some legislators may have been far too credulous and, in the process, may have failed to address the importance of practice and local knowledge (Gomart & Hajer, 2003, p. 36). Without this recognition, the circumstances created by policies that depend so heavily on technology often bear "only a schematic resemblance to the lived realities of those being

governed" (Jasanoff, 2003, p. 172). This local knowledge, although often ignored, is consistently a powerful force in defining and contesting the limits of what policies and technologies can do (see Mukerji, 2009). As the oppositional groups discussed throughout this dissertation have shown, legislators disregard the influence and importance of local knowledge at their own peril. In the context of this research, activist and professional organizations often represent local knowledge and the ideological commitment of those groups to technological regulation and positivist policymaking are minimal at best. Instead, these groups rely on the lived experience of those who would be regulated and focus on the protection of rights instead of the exercise of technocratic government. This struggle is also exemplified by institutions such as public libraries that have often argued that the application of regulatory systems to delineate "community standards" should instead be defined by local practitioners rather than distant legislators or technologies designed with other criteria in mind. Fashioning their opposition around constitutional guarantees and local norms of practice, these groups have taken what some in STS would describe as a "democratic approach to science and technology" that, in part, is intended "to criticize scientific experts' [and policymakers'] reluctance to include local knowledges and stakeholders" within policy debates (Gomart & Hajer, 2003, p. 36).

STS, then, as part of its research agenda attempts to describe these "subpolitical" groups that construct themselves "outside the domain of formal politics" (Id). As will be described, this extra-institutional political phenomena manifested most clearly during the debate over SOPA where grassroots organizations, individuals and websites that were in no way traditional advocates banded together to contest the policy being imposed upon them. Rather than remain subservient to the vagaries of political representation in a high

modern state, these groups used their shared experience within various Internet communities as a counterargument to the rationalist assumptions of those who supported SOPA in Congress. As Gomart and Hajer (2003) have observed, this exemplifies "a reversal of the political order" where oppositional groups, assembled around a common complaint, have employed their local knowledge of a technological circumstance to challenge the "classical-modernist order of politics" (p. 43). Again, STS is uniquely suited to address "both important intellectual questions" surrounding politics and technology while advancing "an activist agenda aimed at improving society" (Monberg, 2005, p. 283). Even more specifically in the context of Internet research, and in alignment with this dissertation, STS helps to provide "a critique of specific Internet public policy choices including privacy, censorship, access, and intellectual property [all of which] offer myriad scholarly and advocacy opportunities" (Id).

Governance

In addition to case-specific opportunities for advocacy, STS research provides insight into the workings of government in general and Internet governance in particular. As communications scholar Mikkel Flyverbom (2011) has argued, in any new technological arrangement it is almost inevitable that artifacts like regulatory systems become "sites of contestation" (p. viii). In any such contest over the legitimacy of these objects "questions about governance and power move to the fore: who does this space belong to, what rules and forms of governance should apply, and who should set and enforce them?" (Id). The questions addressed throughout this dissertation align with this research agenda and the conflicts between legislative and oppositional groups demonstrate the contested nature of these spaces and technological systems. Specifically,

in online spaces, what limits is the state authorized to place on access to information? When and by what means? Does such a thing as a "community standard" exist online? Does the federal regulation of "indecent" content implicate the right of adult access? When Congress requires the use of technological barriers to mediate access, are those barriers appropriate? As will be described, all of these questions have been central to the debates around the CDA, COPA, CIPA, SOPA, and PIPA.

Furthermore, oppositional groups have demonstrated significant power in these debates and have been able to shape both policy and the technological conditions of Internet access in the United States. This validates the assertions of telecommunications scholars Peter Cowhey and Milton Mueller that Internet governance is increasingly a site for new kinds of struggles where "Changes in the rules of decision making and the forms of stakeholder participation will drive outcomes in novel directions even if the parameters of choice still remain under the control of governments" (2009, p. 193). In cases such as these, oppositional groups have demonstrated the ability to mobilize quickly and coherently to address what they often see as a misuse of power and a misapplication of technological mechanisms of enforcement. It is possible that the ability of these groups to assemble rapidly and affect policy initiatives so drastically represents an example of political scientist Bruce Bimber's "accelerated pluralism" (1998). Such a phenomenon demonstrates that these groups coalesce around issues that are *about* the Internet and, in some cases, are so effective because they organize *on* the Internet. As Bimber suggests, the Internet may be "accelerating the process of issue group formation and action, leaving the structure of political power in the U.S. altered" (p. 136). Again, the examples of SOPA and PIPA, and the array of groups that organized online to oppose these policies,

demonstrate this possibility most clearly. These groups were primarily Internet communities who used their online "spaces" as sites of protest against restrictive policy and technology.

Exercising force over the material and technological conditions embedded within the architecture of the Internet is hugely important when determining the contours of Internet governance. As mentioned above, Lawrence Lessig's work in this area demonstrates the principle that code is law in the online environment and, if we are to preserve the open nature of the Internet's original architecture, we must exercise caution when confronted with mechanisms designed to control and regulate without consideration for rights or autonomy (1999, p. 6). Age verification systems, DNS blocking, search result adulteration and commercial filtering software epitomize these architectural barriers to freedom and access and should be closely examined accordingly. Some researchers within STS have made observations similar to Lessig's and have tied the shape of network architecture to "the shaping of user rights" (Musiani, 2013). STS scholar Laura DeNardis has been particularly eloquent on this subject and has repeatedly warned that the "Technologies of Internet governance increasingly mediate civil liberties such as freedom of expression" (2014, p. 1) and we ignore this possibility to our own detriment. DeNardis also warns us that the kinds of technological mechanisms of control described throughout this dissertation demand critical reassessment because they are nothing less than "expressions of mediation over societal values such as security, individual liberty, innovation policy, and intellectual property rights" (Id, p. 2). The regulatory technologies mandated by the CDA, COPA, CIPA, SOPA, and PIPA require such careful analysis because they have the potential to redefine the scope and variety of

speech on the Internet. Without meaningful review of the technological barriers to access required by these policies, we allow the unchecked "technical mediation of the public sphere and the privatization of conditions of civil liberties" (Id, p. 242). This dissertation, and the STS framework it employs, can reexamine the implications of the technical mediation that legislators may have applied uncritically.

Alternative Models of Internet Governance

In relation to questions of governance, it is important to note here that the initial rise of the Internet as the key platform for the global dissemination and receipt of information has resulted in several theories about how to regulate that platform. Most notably, Cyberlibertarianism and exceptionalism typified some of the earliest conceptions about policymaking online. Oppositional groups and grassroots campaigns that fought against the CDA, COPA, CIPA, SOPA and PIPA all, to some extent, share the basic ideology of these movements. This ideology includes the concept that the Internet functions best when left largely unregulated and that those who participate online should formulate a normative and regulatory framework tailored to their own needs. As noted by legal scholar Lawrence Solum, this typifies the Internet governance "model of cyberspace and spontaneous ordering" that "is premised on the idea that the Internet is a self-governing realm of individual liberty, beyond the reach of government control" (2008, p. 57). Centralized regulation and the imposition of technological barriers to access runs counter to this framework and many of the opposition's arguments across all of these cases typify this perspective. For example, early Internet scholars and activists including John Perry Barlow (founder of the Electronic Frontier Foundation) argued that the Internet required no regulation. Barlow believed that the Internet was a unique

domain that would suffer under the imposition of traditional legal constraints. Barlow's "Declaration of the Independence of Cyberspace" (1996) repudiated all of the sovereign territorial claims necessary for regulatory legitimacy and the Internet, in his view, was not subject to legitimate regulation by states bounded by physical borders. Those in "cyberspace" constituted a new citizenship that did not need or wish to consent to the will of these states. Regulation imposed by those who did not participate in this new medium or those who did not understand the technological conditions that define online speech was, by definition, harmful to this citizenship.

Barlow was one of the first to question the right of territorial governments to dictate regulations in a medium that allowed individuals to receive or distribute information anywhere in the world. Barlow argued that laws did not engage the consent of those online if states geographically removed from the subject implemented national laws hindering access. As Barlow noted, if considered a coherent citizenry, those in cyberspace had not agreed to be governed. Other scholars took Barlow's claims quite seriously and began to articulate a new conception of how to regulate cyberspace.

Perhaps the best articulation of this new "exceptionalism" came from legal scholars David Johnson and David Post. Johnson and Post suggested that new legal structures would need to be defined – structures independent of national borders. Since online space constituted its own territorial boundaries, the idea of physical sovereignty had, in their opinion, to be reexamined. Precisely because cyberspace was a disembodied medium, new laws would need to be formulated and these new regulations would have to acknowledge that traditional enforcement mechanisms were no longer adequate. Johnson and Post point out that, in order to create meaningful law, some sort of coercion is

necessary as a threat for noncompliance. Lacking the ability to physically punish or incarcerate an online actor outside their borders, states no longer possessed the means to effectively coerce individuals to obey the law (1997, p. 5). Johnson and Post's solution to regulating this borderless world was to conceptualize the Internet as its own unique territory - an independent sovereign in its own right that would formulate, enforce, and adjudicate its own laws. Simply participating in the online space granted rights akin to citizenship to those individuals. Consent of the governed would come from those participants and the borders separating the physical from the virtual defined this regulatory terrain. Rather than being forced to negotiate a confusing and contradictory set of guidelines, online citizens would operate under a unified system whereby cyberspace was independent of any national policy but its own (Id, p. 13). Like Barlow, Johnson and Post proposed nothing less than a declaration of independence from traditional legal processes.

There are many similarities between these early regulatory approaches and the approach taken by many of the oppositional groups described here. However, the key difference between the two and the difference that informs all of the opposition's arguments against these policies is that regulatory systems became the coercive mechanism by which the state could enforce its policy. Age verification systems, filtering software, DNS blocking and other technologies undercut the argument that physical states did not have the ability to regulate effectively. While many of the oppositional groups described throughout this dissertation have argued that the Internet works best when left alone, they were also forced to contend with enforcement technologies that were unanticipated by Barlow, Johnson or Post. Due directly to the

state's demonstrated ability to coerce behavior online, the opposition was less concerned with the issue of sovereignty and more disturbed by the potential for regulatory systems to harm the constitutional rights of users within U.S. borders. Although sympathetic to many of the cyberlibertarian arguments for global informational rights, as will be described, the opposition's arguments tend to favor the protection of domestic liberties and the preservation of access to protected speech according to U.S. constitutional principles.

The countervailing principle that guided Senator Exon and others as they attempted to reconcile the challenges posed by the new medium of the Internet is analogous to the "law of the horse." As legal scholar and eventual Appellate Court Judge Frank Easterbrook suggested, there should not be two legal systems competing with one another where the first applies only to the physical world while the second applies only for the Internet. As Easterbrook argued in his analogy, simply because issues of ownership or injury were related directly to a horse, these cases should reflect traditional and unifying precedent that recognizes these instances as representative of property and torts law generally rather than some unique law related only and specifically to horses. Equally, when seemingly novel implications of new technology such as the Internet confronted legislators, they should not rush to institute laws separated from the long and proven history of legislation applied to the physical world. As Easterbrook would suggest, "Error in legislation is common, and never more so than when the technology is galloping forward. Let us not struggle to match an imperfect legal system to an evolving world that we understand poorly. Let us instead do what is essential to permit the participants in this evolving world to make their own decisions" and "make rules clear"

(1996, p. 5). Exon's regulatory approach to the problem of online pornography through the CDA was emblematic of this approach and his reliance on traditional regulatory history as well as his argument that regulations such as physical zoning laws have "been in effect and been approved constitutional with regard to pornography…We're not out in no-man's land…We're trying to expand that as best we can to the Internet" (Exon, 1995, p. 2) demonstrates this. This coincides with another model of Internet governance that relies on "national governments and law" and is "based on the idea that as the Internet grows in importance fundamental regulatory decisions will be made by national governments through legal regulation" (Solum, 2008, pp. 57-58). That being said, the law of the horse remains more grounded in legislative precedent than the model of national governments Solum describes.

Interestingly, as the opposition would find and as all of the policies described throughout this dissertation demonstrate, neither the cyberlibertarian model nor the more traditional law of the horse would dominate the debate. Instead, each side would find itself arguing for or against a much different conception of Internet governance. In contrast to the more utopian ideals of self-governance free of national regulation or even the historically proven models of traditional legislation, these debates would focus on a third model of governance. Specifically, both sides had to confront the idea that technological enforcement mechanisms could dictate the substance of online content and the direction of online behavior. This reflects Solum's "model of code and Internet architecture" that is "based on the notion that many regulatory decisions are made by the communications protocols and other software that determine how the Internet operates (Id, p. 57).

Technical Rationality and Political Design

Despite this, the imposition of technology at the legislative level may quash exactly this kind of mobilization by its very nature. As noted above, because technological artifacts represent scientific rationalism and technical expertise they may appear beyond the realm of legitimate debate (Winner, 1977, p. 324). Several social theorists have noted this aspect of technology including Jurgen Habermas, Helmut Schelsky, Jacques Ellul, and Max Horkheimer all of whom have argued that the apparent logic and rationality of technology "cannot be easily criticized in a democratic political arena" (Brey, 2006, p. 361). Legislators and ordinary citizens may not be inclined to question the use of technology or dispute its ability to resolve social problems because of this. Yet, as Andrew Feenberg's critical theory of technology suggests:

> "A good society should enlarge the personal freedom of its members while enabling them to participate effectively in a widening range of public activities. At the highest level, public life involves choices about what it means to be human. Today these choices are increasingly mediated by technical decisions. What human beings are and will become is decided in the shape of our tools no less than in the action of statesmen and political movements. The design [and use] of technology is thus an ontological decision fraught with political consequences" (1991, p. 3).

Investigating how lawmakers portray the use of technology to implement policy can demonstrate how and where they have neglected to examine or understand its political nature and are practicing, as Winner suggests, the kind of "somnambulism that characterizes technological politics" (1977, p. 324). Exploring how oppositional groups have exploited that somnambulism and employed contradicting frames to portray technology is an important means for understanding how various publics have re-opened the debate. STS provides the foundation necessary to accomplish both of these tasks and

can go beyond this descriptive function to offer specific and nuanced recommendations at crucial points within the policy process (Monberg, 2005, p. 283).

A wide cross-section of STS research provides the background necessary to examine the political nature of technology, how the design and implementation of these systems function politically, and how to ameliorate negative effects on individual rights. One possibility within this view suggests that political outcomes are an intentional design feature of technology. Therefore, as science and technology scholar Bryan Pfaffenberger argues, those responsible for creating these systems "have created technological artifacts with technical characteristics specifically designed to exercise force, that is, to coerce obedience and suppress deviance" (1992, p. 283). This can include the design and construction of large-scale, public structures that serve the function of reinforcing the social and political order. The famous example provided by Winner is that of the parkway overpasses on Long Island. In order to prevent lower income minorities from crossing the bridges via public transportation, Winner asserts that city planners intentionally designed the overpasses to be too low to allow buses to pass through. This was a conscious choice on the part of the designer to "achieve a particular social effect" (1986, p. 23). This demonstrates that technological artifacts can indeed have politics as Winner suggested. While the bridge itself is simply concrete and steel, its design can accomplish political goals within its specific historical and societal context.

Many other examples of this phenomenon exist within the STS literature and each demonstrates the political aspects of what superficially appear to be neutral artifacts. Each instance illustrates not only intentional design choices that have social consequences but also how the decision to implement these technologies can reflect

political ends. As Bryan Pfaffenberger has noted, the "elite, the supposedly 'traditional' values, and the technological artifacts [of a society] are reciprocally and recursively constructed in interaction with each other, producing an outcome that ideally generates both political authority and a technological system" (1992, p. 290). To illustrate his point, Pfaffenberger describes the deployment of irrigation technology by the Sri Lankan government. Although seemingly neutral, the state implemented this technological structure in a manner that entrenched the property rights and political authority of the Ceylonese majority while marginalizing the Tamil minority. In this way, "Sri Lankan irrigation technology may have succeeded in its political aims of legitimating the elite's status, discouraging industrial development, and packing the landless [minority] off to the settlements, where they could do no harm" (Id, p. 289). Again, the context of the technology's use may be equally as important as the purpose of its design.

Technology can uphold social hierarchy and entrenched power relations in a similar manner. For example, Pfaffenberger relates how the placement of benches in the hallways of aristocratic homes during the Victorian era served to reinforce class differences between servant and master. While a bench may seem somewhat unsophisticated in a technological sense, it functioned exceptionally well in fulfilling the purpose for which it was designed and implemented. These benches emphasized "Profound decorum standards [that] called for members of the master's class to be admitted straightaway into the interior of the house, while members of the servant's class were seated on the bench, signifying their inferiority" (Id, p. 294). Yet Pfaffenberger cautions that while artifacts have the potential to function politically, they must be employed within a specific social and historical context to do so.

This reminder can serve to caution legislators that technological artifacts are socially constructed and can function politically within the precise social and historical milieu in which they are created (Bijker, 1997, p. 281). This context becomes important, especially when the interpretation of objects is contested (Pfaffenberger, 1992, p. 284). Specifically, "a proper analysis of such political changes requires that an important role is also assigned to social factors, and particularly to the way users and others interpret and represent the technology" (Brey, 2005, p. 66). For instance, as Philip Brey relates, at one time seatbelts in cars were mandatory in that the vehicle would not start unless passengers buckled their belts. Although designed as a safety precaution, this kind of "behavior-steering technology" (2006, p. 357) has moral implications related to freedom, democracy and personal responsibility. Even technology intended to save lives has political implications when those forced to use it take issue with its effects on their rights and autonomy. As this example demonstrates, "behavior-steering technologies are sometimes controversial. U.S. car drivers did not appreciate being mechanically forced to wear their seat belts…Some people even mounted a court challenge: they felt that the coercive mechanism in place went against their civil liberties" (Id). Within the political and social context of the United States, this kind of technological imposition had implications that were not immediately apparent and those sponsoring the law may not have adequately recognized this in their haste to implement the regulatory system.

This observation leads to a second conclusion that not all technology is specifically designed with a political purpose in mind but may have political implications nonetheless. Richard Sclove goes further to suggest that, even without intention, the implementation of technological artifacts through policy can undermine democratic

practices and democratic societal frameworks. In the case of Ibieca, a Spanish village, Sclove argues that the villagers found the introduction of technology (in this case, indoor plumbing) to be a disruption of the community. Instead of gathering at a communal water source, villagers found themselves isolated by the new system thus upsetting a traditional social relationship and introducing a new structure (1995, p. 11). Where democratic society is concerned, technology may be problematic in that it can function to coerce the compliance of the individual at the expense of freedom and autonomy (see Noble, 1986 and Barker & Downing, 1985). Just as Brey's behavior-steering technologies have moral implications, so too do regulatory systems when "in contemporary society [technological processes] have become the equivalent of a form of law – that is, an authoritative or binding expression of social norms and values from which the individual or group may have no immediate recourse" (Carroll, 1977 in Sclove, 1995, p. 11). The imposition of regulatory technologies by policymakers within a representative democracy such as the United States must be examined prior to implementation if, as Brey, Sclove, Carrol, Winner and others suggest, the potential for harm to individual rights exists. Whether designed intentionally or not, employed deliberately or not, technologies are political and not simply neutral tools that serve a useful function. STS provides the vocabulary for exploring the political implications of technology and strongly requires that lawmakers explore those implications as part of the political process. STS "has as its central thesis that better technology is arrived at through a democratization of the process of development and implementation. Better technology is attained if more stakeholders (social groups or actors that have a stake in the way the technology is developed and implemented) have had a say in these

processes" (Brey, 1998, p. 65). Inserting these kinds of critiques into the policy process prior to passage of laws such as the CDA, COPA, CIPA, SOPA and PIPA can help achieve more beneficial and democratic outcomes.

Affordances

Furthermore, technological artifacts, whether they are bridges, irrigation systems, seatbelts, or software filtering programs, can function politically because they afford the user only specifically prescribed activities. Generally speaking, affordances make some actions possible while limiting others. As design engineer William Gaver explains, through these affordances, individuals can and cannot interact with their environment (1991, p. 80). From this perspective, the concept of affordances "encourages us [i.e. designers] to consider devices, technologies and media in terms of the actions they make possible and obvious. It can guide us in designing artifacts which emphasize desired affordances and deemphasize undesired ones. Perhaps most important, it allows us to focus not on technologies or users alone, but on fundamental interactions between the two" (Id, p. 83). As Bruno Latour (1992) has argued through his sociology of science, this aspect of technology can guide and limit a user's range of available actions and constrain a variety of possibilities. Therefore, technological affordances are "a perceived property of an artifact that suggests how it should be used" (Pfaffenberger, 1992, p. 284). The political implications of affordances become obvious when considered in the context of democratic rights for those forced to operate under technological systems. When those systems constrain the exercise of individual autonomy, when those constraints are not immediately apparent to the user, and when access to constitutionally protected content is limited, this harms democratic rights. It is clear that the affordances present (and absent)

within those regulatory technologies mandated by the policies at issue here constrain rights in this manner and the political implications of these systems may not have been adequately addressed at the legislative level.

When legislation requires the use of regulatory technologies such as age verification systems, domain name blocking at the ISP level or Internet filtering software, the actions afforded to the user by the system become fundamentally important. If the system "discourages or prevents a user from behaving in certain ways while using an artifact" (Brey, 2006, p. 73), the rights of the individual are implicated. Within the context of liberty, autonomy and democratic rights, such affordances and constraints may affect the user in two ways. First, this may hinder the negative rights of the user. As described by legal philosopher Isaiah Berlin, questions related to negative liberty ask, "What is the area within which the subject - a person or group of persons - is or should be left to do or be what he is able to do or be, without interference by other persons?" (1969, p. 2). Within the context of the research described here, lawmakers should ask this question when considering the implications of the constraints imposed by regulatory technologies. Failing to address such issues at the policy level can harm negative liberty. In the examples used throughout this dissertation it seems to be the oppositional groups, through critical analysis of the technology, who have recognized that "If I am prevented by others from doing what I could otherwise do, I am to that degree unfree; and if this area is contracted by other men beyond a certain minimum, I can be described as being coerced, or, it may be, enslaved" (Id, p. 3). Questions of positive liberty are equally important when addressing affordances and technological constraints because they ask "What, or who, is the source of control or interference that can determine someone to do,

or be, this rather than that?" (Id, p. 2). When the source of that control is technological in nature and mandated directly by policy, individuals must ask if that interference is legitimate. Legislators should not mediate the ability of the individual to pursue personal goals and access desired information through technology unless they have thoroughly explored that mediation prior to implementation. Again, STS provides the foundation for pursuing these issues and for guiding the policy process.

Hegemony

Additionally, an STS critique should be included at necessary points within the policy debate because the technologies at issue may have hegemonic attributes. Control, power, and illegitimate hierarchical relationships relate directly to the issue of hegemony. Broadly defined, "hegemony is a form of domination so deeply rooted in social life that it seems natural to those it dominates. One might also define it as that aspect of the distribution of social power which has the force of culture behind it" (Feenberg, 1992, p. 7). Those in power can reinforce this kind of domination through the endorsement of technological systems. By mandating their use, policymakers are imposing technologies that "shape aspects of social roles and relations by requiring, fostering, enhancing, discouraging, eliminating or modifying certain social behaviors and patterns of social interaction, or by changing or fostering certain perceptions of social status or the criteria by which people agree to the assignment of certain statuses or roles" (Brey, 2006, p. 75). Regulatory technologies can steer behavior and implicate positive and negative rights through technological affordances but first those in power must approve and institutionalize these technologies. In order to reach the level of legislative implementation, technologies, both large scale and small, must have the imprimatur of

the state. Put another way, "The principle dimensions of such culture institutionalization are the state, which articulates its interests through political codes, technology and its technical codes…an effective hegemony is characterized by a cultural unity traversing the domains of economics, technology, and politics" (Feenberg, 1991, p. 135). Through policy, the state can institutionalize hegemonic technologies that can detrimentally impact individual rights.

If regulatory technologies are not neutral tools and if they are socially constructed artifacts with embedded values of their own, the hegemonic dominance of those values may become pervasive. Particularly if those values remain undetected at the policy level, by default, they may impose a certain point of view on those forced to operate under them. If lawmakers implement regulatory technologies without a critical understanding of the values they embody, those forced to implement these systems may be tacitly endorsing these values (Johnson, 1997, p. 22). This possibility is reminiscent of Marxian political theorist Antonio Gramsci's conception of cultural hegemony. Gramsci argued that this phenomenon is comprised of the "consent given by the great masses of the population to the general direction imposed on social life by the dominant fundamental group" (Gramsci, 1971/2005, p. 12). While Gramsci's analysis deals primarily with the power afforded to those in control of the means of production, this concept applies equally to those with the power to impose artifacts specifically designed to enforce a set of prescribed norms and quash behavior deemed to be outside of those norms (Pfaffenberger, 1992, p. 283). In addition, Gramsci emphasizes that hegemony and the exercise of power requires, to some extent, the consent of those who acquiesce to the cultural norms of what constitutes acceptable behavior, what is deviant and the

mechanisms used to mediate both. In Gramsci's estimation "consent and force nearly always coexist, though one or the other predominates" and those in power rule "primarily through domination – that is, by monopolizing the instruments of coercion" (Lears, 1985, p. 568). In the examples discussed throughout this dissertation, those instruments mandated by policy may coercively limit access to a range of constitutionally protected speech.

The policies at issue in this dissertation all deal with some coercive instrument that disallows the free flow of information. Yet those with legislative authority, in some measure, have surrendered their power in that they have employed these technologies without an adequate understanding of how the objects themselves mediate access and exercise power over the individual. In these instances, policymakers have handed over some hegemonic authority to the technical specifications of regulatory systems and, by inference, to those who designed those systems. As philosopher Martin Heidegger has suggested, based on a strong belief in scientific expertise, rationality, technical knowledge and the certainty that technological problems can only be remedied by technological solutions, power is delegated to those mechanisms (1977, p. 3). This compromises the power of the individual in that their consent is now dependent on accepting the terms of access placed upon them by technology. If they do so without question, individuals have, in a sense, given up the power inherent in their consent by trusting that elected representatives, the policies they impose and the instruments employed to accomplish policy goals are the only rational solution to perceived social problems. Again, this demonstrates a hegemonic relationship if the "social power which has the force of culture behind it" (Feenberg, 1992, p. 7) is granted to regulatory systems

without a critical analysis of those systems. As philosopher Michel Foucault has suggested, if power "only exists in action" and manifests as the "way in which relations of forces are deployed and given in concrete expression" (1976/1980, pp. 89-90), then regulatory technologies assume the power granted to them by the state that employs them and the citizens who accept them if that power is delegated without first understanding how it will be exercised. When we blindly accept low bridges that refuse entry to minorities or filtering software that refuses access to constitutionally protected content, we are forfeiting our power to artifacts we may not understand and systems that make political decisions on our behalf. The power of individual consent is meaningless if our relationship to technology allows no room for solutions other than those that are technological.

In this sense, the true danger of technology and technocratic policy is that it can restrict how we may choose to address social problems (Dreyfus, 1995, p. 99). By conceiving of technology as the only viable solution, legislators may restrict themselves to only those options when formulating policy. As sociologist Todd Gitlin argues, this too becomes a "hegemonic ideology" that subsumes our world view and "meshes with the 'common sense' through which people make the world seem intelligible" (2003, p. 10). Yet, even when presented as "common sense" and outside the realm of controversy, it is possible to oppose hegemonic ideology. The oppositional movements described within this dissertation have framed the debates surrounding these policies in a way designed to "stretch, dispute, and…transform the hegemonic ideology" (Id, p. 11). These groups may have recognized that a different relationship with technology is possible and that powerful counterarguments to its use as regulatory mechanisms exist. Within the social

and historical context of these artifacts and within the political environment they have been deployed, oppositional groups have recognized that "the dominant ideology" includes contradictions that position democratic values against state control and the tyranny of rationalism against informed and legitimate debate (Id). By exploiting these contradictions, these groups have found a means for once again exercising the power of their consent and reinvigorating the debate over the objectivity and neutrality of technological systems. Questioning hegemonic ideology as it relates to technological policy instruments may once again bring these issues, as political communications scholar Daniel Hallin argues, within a "sphere of legitimate controversy" (1989, p. 116) that is recognized by legislators and the courts as worthy of debate and critical discourse.

Conclusion

STS provides the tools necessary to address all of the technological issues addressed above including the possibility that legislators have assumed that regulatory systems, as the end result of a rational design process, are neutral and apolitical policy instruments. This analysis will provide insight into the potential for these systems to function politically due to the values and bias that the design process may embed within them. Additionally, this research will describe how these regulatory technologies may have functioned politically constraining individual rights, local autonomy, and constitutional liberty in the process. This potential extends to unintended consequences resulting from these policy actions including the formation of anti-democratic power relationships and the exercise of hegemonic power. In the context of Internet research, it is hoped that the "payoff" of using STS as a theoretical lens will be to provide an enlightening "exploration of the political consequences of technologies seemingly most

apolitical" (Monberg, 2005, p. 284). By isolating these policy moments and analyzing them within an STS framework, this dissertation provides a novel contribution to both frame analysis and to information policy studies. Structurally, frame analysis locates where to apply a critical understanding of technology within the policy process but, without STS, there would be no way to discern what that critical view should encompass. If lawmakers have neglected the implications of these technologies, STS can help explain why these policies have met with such difficulties and how to ameliorate concerns as Congress negotiates future policies. Bijker has called for STS to take up the kind of empirical work that this dissertation will attempt to accomplish while embracing rich theoretical perspectives that encompass both policy and technology (1997, pp. 289-290). By combining a descriptive account of the CDA, COPA, CIPA, SOPA and PIPA with the theoretical lens provided by STS, this research is intended to, as Bijker has suggested, "strengthen the links between academic STS studies and politically relevant action" (Id). By conducting this analysis, and by examining lawmakers' actions in the context of these important concepts, it is possible that more democratic outcomes may result.

Chapter 3 – Methodology

Methodological Framework: Frame Analysis

Frame analysis provides the methodological grounding necessary to organize and understand both the legislative and oppositional processes at issue within these policies. It allows these policies to be broken down into functional units that relate to the portrayal of technology and technological mechanisms of enforcement. Coupled with the use of an STS lens, frames provide a structural mechanism for parsing out moments in time where the policy process and its oppositional counterparts have or have not employed some critical view of technology. Locating those moments will isolate where lawmakers may have failed to examine the implications of regulatory systems and where oppositional groups have used arguments similar to those provided by STS to the greatest advantage. Furthermore, by identifying those points in the policy process it will then be possible to make recommendations as to where legislators can most beneficially employ a more critical analysis. This research suggests that including an STS critique within the legislative process can result in better, more nuanced information policies and frame analysis provides the entry point necessary to accomplish this.

Frame analysis began as a sociological instrument for studying representation and meaning (Fisher, 1997). Sociologist Erving Goffman (1974) suggested that frames provide a structure through which individuals and groups can make sense of their physical surroundings as well as their social context and, through frame analysis, "what would otherwise be a meaningless aspect of the scene [becomes] something that is meaningful" (p. 21). This dissertation will explore the context of both policymakers and oppositional groups frame analysis will provide a method for coherently organizing the

themes that emerge. Frame analysis will help explain the motivations of these groups and will offer a structural and organizational point of reference to describe how stakeholders understand these issues and present alternatives (Zald, 1996, p. 265). Frame analysis will allow this research to isolate crucial moments within the policy process where a better, more thorough understanding of technology can and should be included.

Specifically, this methodology provides insight into the policy process and the movements that oppose those policies by "offering a point of comparison, or a conceptual structure, through which people can digest information" (Fisher, 1997). The "conceptual structure" of frame analysis can take two primary forms: cognitive representation and discourse related to the subject. The cognitive approach defines frames as an individual interpretive scheme for understanding and representing situations based on prior practice, successful experience, and cultural foundations (Johnston, 1995, p. 217). Although useful, this dissertation will not pursue this approach because it has tended to focus on "individual cognitive organization and to blur the distinction between frames and other ideational factors such as values, norms, identity, solidarity and grievances" (Id, p. 218). Instead, this research will address frames at the oppositional and institutional levels because describing individuals at the cognitive level is neither feasible nor useful in the context of this research (Id). Furthermore, this project is very concerned with values and norms and those ideological features of policy and will explore these features through their manifestation within the primary source documents. For the purposes of this research, these documents will provide a more holistic view of these information policies and the oppositions that have coalesced around them. As political scientists Donald Schon and Martin Rein have argued, in order to understand the policy process, and

discrete moments within it, "we must become aware of our frames, which is to say that we must construct them, either from the texts of debates and speeches or from the decisions, laws, regulations, and routines that make up policy practice" (1994, p. 34). The use of documentary evidence is crucial to this research because it is the best, most direct and most concrete artifact of how these policies were justified, negotiated, and opposed.

Frame analysis is particularly useful for policy studies like this because it allows the researcher to identify and "examine political language as used at various stages of the political communication process" (Pan & Kosicki, 1993, p. 70). This is true in the context of both institutional actors such as legislators and social movement organizations that employ frames to mobilize the opposition (see Gitlin, 2003, p. 6). As social movement researchers Robert Benford and David Snow have argued, frame analysis also provides a means for investigating the "collective action frames" (2000, p. 615) used by both oppositional groups and policymakers. Identifying these collective action frames will help explain how "adherents negotiate a shared understanding of some problematic condition or situation they define as in need of change, make attributions regarding who or what is to blame, articulate an alternative set of arrangements, and urge others to act in concert to affect change" (Id). In the context of information policies that manage access to online content, understanding how the opposition frames problems related to policies that employ technological systems is particularly important. Just as important is to understand why lawmakers implemented those solutions in the first place.

In the literature, these "core framing tasks" (Benford & Snow, 2000, p. 615) have generally been applied only to social movement organizations (SMOs) and not to

institutional actors such as policymakers (for seminal examples, see Snow & Benford, 1988, Snow et al. 1986, Klandermans 1984 and Klandermans 1986). This is equally true for online collective action (see Postigo, 2012, Jordan, 2001, and Milan & Hintz, 2013). Scholars position these SMOs external to traditional power structures and conceives of these groups outsiders in any political struggle where policy clashes with values held by the SMO. In contrast, this dissertation will apply these concepts equally to those inside and outside the policy process. Just as SMOs coalesce to contest the presence or absence of certain policies, so too do legislators take concerted action to address their concerns and those of their constituencies. Both policymakers and oppositional groups employ frames to advance an ideological position, rhetorically define a problem, and propose a solution to that problem (Nisbet, 2010, p. 47). Within this dissertation, this will also include the core framing tasks related to the characterization and application of technological systems.

Framing occurs at several levels throughout the policy process. The primary frames at issue here are those that are most fundamental to the cultural, political, and technological narratives formed around these policies. These foundational themes are referred to as the "metacultural frames" (Schon & Rein, 1994, p. xiii) or "master frames" that are the "dominant logic or grammar that provides syntactic (formally ordered) 'codes' that structure the framing process [and] enable movement actors to communicate with a reasonably wide audience by connecting the frame to already recognizable codes" (Williams & Benford, 2000, p. 134). As mentioned previously, at the policy level lawmakers have invoked as master frames the need to protect children from harmful content, the need to protect intellectual property from theft and the need to defend

national security. Despite the fundamental cultural importance of these ideological motivations, these policies have met with intense opposition based on competing foundational principles. The opposition in these instances has focused their arguments on ideals such as free speech, free access, autonomy and the need for transparent mechanisms of enforcement. These are the master frames embedded within these movements and, to a large extent, these oppositional frameworks have been more nuanced about policy and the implications of technology than the legislative master frames invoking the need to protect children, property and national security. Put another way, the master frames articulated by the opposition may have broader "resonance" which is "relevant to the issue of effectiveness or mobilizing potency of proffered framings" (Benford & Snow, 2000, p. 619). Todd Gitlin (2003) and Daniel Hallin (1989) have demonstrated how frames used to mobilize opposition to the Vietnam War have resonated with both the public and with policymakers and, in some cases, forced the direction of policy to adapt or shift to a more widely resonant master frame. Determining if the master frames employed by the movements opposed to the CDA, COPA, CIPA, SOPA, and PIPA have greater resonance than the legislative master frames and finding out if that resonance relates to a critical understanding of technology similar to STS is an important first step in this research.

Master frames reflect core cultural and political values. Although many frames may resonate widely "Only a handful of collective action frames have been identified as being sufficiently broad in interpretive scope, inclusivity, flexibility, and cultural resonance to function as master frames, including rights frames, choice frames, injustice frames…and a 'return to democracy' frame" (Benford & Snow, 2000, p. 619). It is

hypothesized that the master frames employed by oppositional groups in these instances may have garnered judicial support and influenced the direction of policy because they rely on some of the most powerful master frames identified by Benford and Snow and because they better account for the implications of the technology required by policy. Specifically, the opposition in these instances has based its dissent on rights frames, choice frames and democratic frames and these arguments have rested on the supposition that technological mechanisms of implementation and enforcement negatively impact those rights and choices. Within the context of master frames and the ideological principles they represent, these oppositional frames may "rank" more highly than those articulated by policymakers. If the research shows that judicial decisions have endorsed the frames employed by the opposition or woven directly into modified versions of these policies, this would be a strong indication of their resonance. This would support prior research "on values and beliefs [which] indicates that they are typically arrayed in a hierarchy…the more central or salient the espoused beliefs, ideas, and values of a movement to the targets of mobilization, the greater the probability of their mobilization" (Id, p. 621). This would also validate the assertion that a critical analysis of the technological mechanisms these policies require in application is a prerequisite for crafting sound information policy.

Additionally, this dissertation will focus only on policies contemplated by the United States because the frameworks employed by both lawmakers and the opposition are grounded in the political, social, democratic and constitutional context of that government. Master frames that invoke choice, transparency and access "make sense only in a cultural discourse that highlights notions of individual autonomy and equality of

citizenship rights" (Zald, 1996, p. 267). In order for the opposition to be even remotely successful, the political process must make room for dissent and policymakers must be vulnerable to the processes that validate these competing democratic/technological frames. The difficulties these policies have faced may be a direct result of not only the oppositional position, but also a political context that allows for and responds to public pressure. Within this democratic and constitutional context the "framing of injustice and of political goals almost always draw upon the larger societal definitions of relationships, of rights, and of responsibilities to highlight what is wrong with the current social order, and to suggest directions for change" (Id). In particular, the opposition has focused its argument on the need to reconsider the technological mechanisms required by these laws because they may unjustly impact the affordance of rights.

Scholars who conduct frame analysis are often concerned with the narratives of injustice that have appeared as a common thread among social movement organizations. These studies "focus on the development and articulation of…'injustice frames' [and] call attention to the ways in which movements identify the 'victims' of a given injustice and amplify their victimization…injustice frames appear to be fairly ubiquitous across movements advocating for some form of political and/or economic change" (Benford & Snow 2000, pp. 615-616). This dissertation will argue that the opposition has effectively applied these injustice frames to advocate for technological change. To accomplish this, social movements employ frames reminiscent of STS perspectives in order to advance their position and "draw on the cultural stock for images of what is an injustice, what is a violation of what ought to be [in order to] frame a problem and suggests a policy direction" (Zald, 1996, p. 266). Those opposed to federal attempts to regulate the

Internet have drawn from these same narratives of injustice and have argued that "larger state or government structures are not needed in cyberspace" because they harm the ability of the individual to self-govern (Jordan, 2001, p. 9). For example, movements that have opposed online intellectual property regulations have drawn from a similar pool of injustice frames arguing that "user-centered notions of fair use [and] free speech…are often bargained away in click-through agreements" (Postigo 2012, p. 5). Opposition to the policies discussed here have all, in one way or another, focused on the injustices inherent in the technological mechanisms required by these policies. These groups have crafted arguments strikingly similar to STS perspectives and have used them effectively to address the unjust nature of some technologies.

In conjunction with all of these strategies and in addition to master frames, each competing side also employs a "diagnostic" frame (Benford & Snow, 2000, p. 615) that rhetorically defines the "problem" as that side sees it. The process of diagnosis requires an identification of that which is responsible for the problem and, in the examples of the CDA, COPA and CIPA, Congress suggested that the Internet was a potentially harmful medium for children. They argued that it was a compelling government interest to solve this problem. Despite this, the opposition in these examples based its position on the idea that the "solution" proposed by lawmakers was a problem in itself. Since "social movements seek to remedy or alter some problematic situation or issue, it follows that directed action is contingent on identification of the source(s) of causality, blame, and/or culpable agents" (Id, p. 616). By hindering access and choice, the opposition has argued that these technologies unjustly restrict access to protected speech. By identifying the technological mechanisms of implementation and enforcement as the cause of the harm,

oppositional groups in these instances demonstrated this "attributional component [of] diagnostic framing [that] attends to this function by focusing blame or responsibility" (Id). Policymakers performed the same task by identifying indecent online content (i.e. the Internet) as that which was to blame for the problem.

The language used to frame the problem is also important to the process and frame analysis can identify the underlying values and the associated portrayal(s) of technology that rhetoric may advance, obscure, define, or re-define. Regardless of how it is used, rhetoric demonstrates how ideological positions form frames that can advocate for the creation of law, including information policies such as the CDA, COPA, CIPA, SOPA, and PIPA. Frame analysis can shed light on the political nature of problem definition and the value-centric nature of policymaking where "'[P]roblems' are viewed as *interpretations* of conditions that have been subjectively defined as problematic and, as such, demand some type of ameliorative action. It follows, then, that problem definition is fundamentally a political exercise, that is, labeling a phenomenon to be a 'problem' is a political calculus largely based on values" (Ingram et al., 2007, p. 94, emphasis in original). Frame analysis can address the values and ideology that lawmakers employ to advance political positions and those positions that oppose institutional interpretations of the need for and direction of policy (Zald, 1996, p. 262). This includes the tendency of legislators to describe the Internet as a problem that they must solve through policy and technology. Despite this, within all of the policies discussed here, the opposition has invariably offered alternatives that critique the implications of the technologies imposed by these laws in a manner reminiscent of STS.

Frames can manifest at the policy level through the identification and presentation of social problems. Policy is often the result of the perceived need for change in a given circumstance where lawmakers see government intervention as the primary mechanism for achieving that change. Furthermore, due to the political nature of policymaking, lawmakers must persuade people that a problem exists. In such situations, "not every condition is seen as a problem. For a condition to be a problem, people must become convinced that it requires change. People in and around government make that translation by evaluating conditions in light of their values" (Kingdon, 1995, p. 114). In addition, the frames underlying the identification and definition of the problem must be acceptable to others. By making a particular value set explicit, a policymaker "selects some aspects of a perceived reality and makes them more salient…in such a way as to promote a particular problem definition, causal interpretation, moral evaluation, or policy alternative" (Weimer & Vining, 2011, p. 272).

For instance, in the examples of the CDA, COPA, and CIPA, policymakers framed the issues in a way that portrayed technology in general and the Internet in particular as dangerous and children as a group that required protection from it. Legislators intended the CDA to "address an increasing number of published reports of inappropriate uses of telecommunications technologies to transmit pornography [and] engage children in inappropriate adult contact" (Senate Report 104-230, 1995). Lawmakers presented CIPA as a way "to protect America's children from exposure to obscene material, child pornography, or other material deemed inappropriate for minors" (Senate Report 106-141, 1999). Yet others may have framed the issue quite differently and would not have found a problem; at least not a problem that required intervention

through policy or technology. The difference between the two positions is the use of rhetorical framing to push a policy alternative and with it a preferred set of values. This strategy demonstrates "the use of persuasive language to frame issues in favorable ways. At one normative extreme, rhetoric provides correct and relevant information that clarifies the probable impacts of proposed policies. At the other normative extreme, it provides incorrect or irrelevant information that obfuscates the probable impacts of proposed policies" (Weimer & Vining, 2011, p. 283). The simplistic portrayal of technology by policymakers combined with a lack of critical understanding results in exactly the kind of rhetorical framing that can obfuscate the probable impacts of these kinds of information policies and their associated regulatory technologies. Oppositional groups have seized on this and crafted their arguments in a way that isolates these impacts as the problem. This research will explore how both legislators and these oppositional groups employ diagnostic frames during the course of problem definition.

Diagnostic framing then leads directly to "prognostic framing" that articulates potential solutions to the problem and the means for realizing those solutions (Benford & Snow, 2000, p. 615). Continuing with the example of the CDA, legislators suggested a handful of technological solutions to the problem of minors' exposure to indecent online content. In contrast, for the opposition, this has formed the basis of the competing prognostic frame that Congress should reconsider use of these technologies or that the courts should strike down the law (or portions of it) in order to resolve the problem. Based on the argument that policymakers essentially failed to recognize the impact that technological mechanisms of enforcement could have, the Supreme Court accepted the opposition's position that these mechanisms resulted in a situation where "the CDA thus

becomes a total criminalization of constitutionally protected 'indecent' or 'patently offensive' speech" (ACLU Plaintiffs' Post-Trial Brief in Support of Their Motion for a Preliminary Injunction, 1996). This is a common feature of prognostic frames and "it is not surprising that an SMO's prognostic framing activity typically includes refutations of the logic or efficacy of solutions advocated by opponents as well as a rationale for its own remedies" (Benford & Snow, 2000, p. 617). This oppositional rationale has often included the suggestion that lawmakers do not understand how regulatory technologies impact individual rights. The opposition has asserted that, because lawmakers have approached technological mechanisms of enforcement as expedient tools, they are employing these systems without first addressing the potential effect they can have on constitutional guarantees. This kind of assertion often employs arguments similar to those provided by STS scholars and, by using this kind of framework at this point in the process, the opposition may have forced the legal challenges and policy shifts these laws have so often faced.

Building on this supposition, another key area for investigation within this dissertation will be to examine "frame shifts" (Rein & Schon, 1991, p. 283). Both Todd Gitlin (2003) and Daniel Hallin (1989) have described how extenuating factors can shift the dominant frame bringing previously marginalized groups into a position of power within a national conversation or policy debate. In the examples provided by Gitlin and Hallin that factor is the media but as both acknowledge, oppositional groups and SMOs can serve the same function. While the media no doubt influenced the public's perception of these policy frames, this research will focus instead on oppositional groups and their subsequent challenges to policy. Regardless of the focus of analysis, both

authors suggest that all of these forces may act on one another to a greater or lesser degree eliciting action, reaction, framing and re-framing. By inference then, the groups identified within this research can place pressure on institutional actors to reassess or modify the prevailing frame - in this case the portrayal of technology as the only logical policy solution. In recognition of the competing frames offered by the opposition, policymakers may have changed the narrative and/or the scope of these laws in an effort to advance the original master frame. In these examples, lawmakers incorporated portions of the opposition's competing frames into the modified policy either directly or via judicial opinion. Specifically, those frames that offer a more critical view of technology and that align with perspectives from STS.

For example, the CDA underwent just such a shift after the Supreme Court's ruling in 1997. In recognition of some of the oppositional frames that helped strike down portions of the original policy, legislators narrowed the focus of the law to ameliorate concerns about overly broad limitations on adult choice and undue restrictions on constitutionally protected speech. This shift eventually resulted in introduction of the Child Online Protection Act (COPA) and then the Children's Internet Protection Act (CIPA). Like the CDA, lawmakers designed these policies to filter harmful content for minors but the focus of that restriction became successively narrower as the policy evolved. Although the master frame of protecting children from harm did not change, policymakers eventually tailored the law to target children specifically within public institutions such as schools and libraries. Despite this, like the CDA before it, CIPA continues to face strong opposition based on its technological shortcomings. Although the Supreme Court found CIPA to be constitutional, it remains controversial due to

policymakers' potential failure to address the biased and political nature of the technical systems it continues to require. While the modifications to CIPA suggest that policymakers have acquiesced to some oppositional frames and have ameliorated some technological concerns, this possible failure to address the impact of technology fully may result in additional legal challenges (see *Bradburn v. NCRL* and *PFLAG v. Camdenton*).

Across all of these frames, oppositional movements have often articulated the position that the technological solutions proposed by these policies limit choice by restricting access unnecessarily and that those restrictions unduly restrain access to protected speech. This dissertation will describe how the opposition has articulated competing frames and how these groups have been able to modify or defeat the policies in question. This research suggests that the ideological framing of the opposition has been successful because it more appropriately accounts for the political nature of the technologies at issue in a manner similar to STS research. As a result of this more critical view of regulatory systems, the opposition has forced lawmakers to shift these policies to reflect this. By examining the opposition's framing process, this dissertation will isolate precise points where these groups have advanced positions similar to those provided by STS. In turn, this analysis will dissect the policy process to locate instances where lawmakers may have failed to understand the political nature of technology or critically assess the implications it can have for individual rights and autonomy.

Frame Analysis Accommodates the Theoretical Lens of STS

As described above, frame analysis provides the best possible methodology for this project for several reasons but one of the most important is that it can accommodate

the theoretical framework of STS. As noted in Chapter 2, STS provides the most appropriate theoretical lens for approaching these policies and technologies because it provides insight into the subjectivity and potentially biased nature of regulatory systems. Although this research relates directly to the policy process and would seem, for example, to suggest the need for formal policy analysis, the fundamental worldview that underpins that approach is insufficient to address the technological and ideological topics at issue here. Instead, frame analysis allows for an examination of the policy process through the constructivist lens of STS. Therefore, a combination of the frame analysis methodology and STS concepts offers significantly different avenues for research than the more rationalist framework that defines policy analysis.

By way of comparison, the framework represented by the policy analysis approach has several shortcomings that frame analysis does not. First, from its inception, policy analysis and the "policy sciences" have emphasized the role of quantitative data, positivist assumptions, economic metrics, and "the use of scrupulous objectivity" (Laswell, 1951, p. 14) to anticipate the outcomes of specific policy decisions. Instead, as political scientist Giandomenico Majone (1989) has suggested, the construction of policy and its subsequent analysis requires a constant appraisal of socially negotiated values, norms, and priorities. Recognizing this becomes even more important with the introduction of technocratic regulation that relies on technological policy instruments (Id, p. 2). Where these technologies directly impact individual autonomy and democratic freedoms, positivism and economic considerations fail to acknowledge that these regulatory systems are socially constructed artifacts that are distinctly political in nature. Frame analysis goes beyond the rationalist tools used by policy analysts and

accommodates alternative perspectives from STS that recognize "Whenever technologies structurally affect democracy or other important shared values, democratic politics ought to take precedence over economic calculation or unregulated market outcomes. This implies that contesting democratic design criteria can be superior to using today's formal methodologies for public policy analysis" (Sclove, 1995, p. 161). In fact, the metrics provided by traditional policy analysis may serve to echo the instrumental assumptions that already permeate the legislative portrayal of technology as value neutral. By offering a seemingly objective, unbiased examination of technocratic policy, policy analysis may serve to reinforce legislators' uncritical view of the technologies they are imposing. As Richard Sclove suggests, "As applied within the context of pending political decisions, [positivist] methodologies are often portrayed as value-neutral machines operated impartially by expert practitioners to generate social policy analyses or recommendations" (Id, p. 173). Contrasting perspectives provided by STS require a greater depth of analysis for issues related to the portrayal of technology by policymakers and parallel oppositional movements within key frames. This research employs frame analysis in conjunction with STS to approach policy and technology in a way that policy analysis alone cannot.

By filtering this frame analysis through the lens of STS, this research can provide exactly the kind of critical, democratic foundation required for the inquiry described here. Frame analysis allows for the systematic evaluation of policy and it can incorporate the theoretical framework of STS that provides the necessary skepticism about such systems. The economic and other metrics that form the theoretical lens for policy analysis cannot be easily reconciled with these features of STS.

Research Questions

1.) How are the motivations and justifications for these policies articulated within legislative master frames? In contrast, how are the oppositional master frames articulated? In the context of the Internet and the regulatory systems required by the policy, how is technology being (mis)portrayed? Do legislative master frames lack a critical view of technology (per STS) and do oppositional master frames include more of these critical perspectives? Are master frames a point within the policy process where lawmakers would benefit from the framework provided by STS research? Are oppositional groups already employing such a framework within their master frames in a manner that would assist policymakers?

- *Purpose* – To identify how policymakers articulate the key themes and justifications for intervention through policy and, by inference, through technology. Also, to identify how oppositional groups have taken a critical view of policy and its related use of technology. To identify how both sides are portraying technology and if those portrayals include a critical assessment of how these regulatory systems would function in application. To isolate master frames as a potential location within the policy process that would benefit from this kind of critical assessment.

- *Method* – Frame analysis will be used to identify the master frames articulated within the policy and oppositional discourse. This discourse takes the form of documentation including the policy itself, congressional reports, legislative and oppositional press releases, hearing testimony, legal challenges, and other judicial documents.

2.) Within the context of diagnostic framing, how do policymakers define technology as a "problem" that requires government intervention through policy and through technological mechanisms of enforcement? How does the opposition define technological aspects of the policy itself as the "problem" that requires amelioration?

How do both sides frame the argument and rhetorically define the "problem" in the context of technology and policy? Does the process of problem definition include a critical view of technology (per STS)? Are diagnostic frames a point within the policy process where lawmakers would benefit from the framework provided by STS research? Are oppositional groups already employing such a framework within their diagnostic frames in a manner that would assist policymakers?

- *Purpose* – To analyze how policymakers describe access to online content as a "harm" that must be addressed by policy and by technology. Also, to analyze how the opposition describes the "harm" caused by the policy and its technological requirements. To identify if these diagnostic frames include a critical view of technology. To isolate diagnostic frames as a potential location within the policy process that would benefit from this kind of critical assessment.

- *Method* – Frame analysis of the same documentation identified in #1 will also be analyzed here in order to describe the diagnostic frames related to problem definition and the associated portrayal of technology.

3.) How do both sides in these policy debates propose to solve the problem within the context of prognostic frames? By what technological measures do policymakers propose to protect children from harmful content, protect intellectual property from theft, and safeguard national security? In what ways does the opposition propose to address the problems created, as they see it, by the policies themselves and the regulatory technologies they require? Is a critical assessment of technology included in either the legislative or the oppositional process of prognostic framing? Are prognostic frames a point within the policy process where lawmakers would benefit from the framework provided by STS research? Are oppositional groups already employing such a framework within their master frames in a manner that would assist policymakers?

- *Purpose* – To understand the solutions proposed by both sides to ameliorate the "problem" as that side sees it. This includes the role of technology in those solutions and the potential implications of those systems. To isolate prognostic

frames as a potential location within the policy process that would benefit from a more critical assessment of technology.

- *Method* – Frame analysis of the same documentation identified in #1 will also be analyzed here in order to identify the prognostic frames where technological solutions, and their potential implications, are discussed.

4.) Has the judiciary incorporated the opposition's critical view of technology within its opinions? Have these opinions validated oppositional views and has this resulted in policy shifts that have modified the technological requirements and scope of these policies? Do the revised policies include any of the critical perspectives of technology provided by oppositional groups (either directly or via judicial opinion)? Specifically, do the modified policies, in any way, echo the opposition's arguments that the technological mechanisms of implementation and enforcement harm individual rights, autonomy and unduly restrain access to protected speech?

- *Purpose* – To analyze the potential shifts these policies have undergone and to identify whether or not the opposition's more critical view of technology has been incorporated into these new iterations. If policy revisions and judicial decisions echo the arguments provided by the opposition, this will help to establish the validity of oppositional frames (and STS perspectives) that characterize technology as non-neutral and political in nature.

- *Method* – Using frame analysis to identify the frame shifts, the "new" policies will be analyzed and compared to previous iterations. Modifications to the technical requirements of these policies will be examined to understand how they do (or do not) include the opposition's characterization of technology.

Data Selection

The documents that comprise the legislative portion of this analysis were located using several public and private databases. Full text versions of these documents were collected from official government sources including the Government Printing Office and Library of Congress or, when necessary, from third-party databases such as LexisNexis. The results of the initial search were numerous and the selection process was refined by targeting only primary source material including the bills, amendments, and laws that are the focus of this research. Other primary sources collected through this process include Senate and House reports, Congressional Records, governmental hearing transcripts, and other official reports ("official" being defined as any report that was authored by a Congressional committee, Congressional commission, the Congressional Research Service, or some other governmental agency). Secondary sources such as media articles and scholarly publications not authored by those directly involved were eliminated because they do not always represent the direct arguments put forth by legislators. That being said, all available press releases and some editorials were included in the sample but only if the legislative sponsor of the Act was the author.

Oppositional documentation was collected directly from the websites of these organizations (described below). These materials include press releases, informational reports, and any other public statements (such as hearing testimony) that were produced directly by these organizations. Again, this does not include secondary media sources or any other material not authored directly by these organizations.

Next, the legal filings, amicus briefs, and court opinions that make up the judicial documentation for this research were identified. These documents were located primarily

through court websites and, when necessary, through third-party databases such as WestLaw and Cornell University's Legal Information Institute.

Based on the conditions for inclusion outlined above, from an initial sample of several hundred documents, 144 items remained for coding. Table 1 provides information on the total number of and the kinds of documents collected for both the legislative and oppositional sides of the debate.

This investigation also identified the primary oppositional groups that would be the focus of this research. Again, because the majority of these policies were the subject of legal action, those oppositional groups most active in these court challenges were chosen as the primary target of investigation. Specifically, the named plaintiffs in the cases against the CDA, COPA, and CIPA became primary sources. The major organizations represented throughout this dissertation include the American Civil Liberties Union (ACLU), the Center for Democracy and Technology (CDT), the American Library Association (ALA), the Electronic Frontier Foundation (EFF), and the Electronic Privacy Information Center (EPIC).

Finally, although neither SOPA nor PIPA ever became the subject of any court challenge, it was necessary to isolate a core group of organizations opposed to these policies as well. In order to maintain consistency, and because they remained essential to the opposition in this instance, many of the same groups involved with the CDA, COPA, and CIPA became the focus of the investigation on SOPA and PIPA. These groups include the ACLU, CDT, ALA, and EFF. Many of these groups authored press releases opposing these policies, testified before Congress against them or submitted committee reports on these issues. That being said, there were dozens of websites and individuals

that opposed these policies at the (online) grassroots level. This analysis is not intended to privilege traditional activist organizations above these other actors and, for the sake of inclusiveness, some public statements made by interested parties such as Google and the Wikimedia Foundation were included in the coding sample as well. However, these primary activist organizations remain the focus of this research both for the sake of continuity and because these groups produced a great deal of the material opposing SOPA and PIPA. Table 2 provides a breakdown, by policy, of the oppositional groups that comprise the documentary evidence for this part of the research.

Table 1 – Legislative and Oppositional Documents Collected

Document Type	CDA	COPA	CIPA	SOPA/PIPA	Total
Bill/Amendment/Law	1	1	1	4	7
Senate or House Report	2	1	2	0	5
Congressional Record	2	2	3	6	13
Hearing Transcript	1	1	2	3	7
Press Release	12	12	11	9	44
Legal Filing	6	9	6	0	21
Court Opinion	2	6	6	0	14
Editorial/Publication	3	6	0	5	14
Report	2	4	5	1	12
Other	2	1	3	1	7
Total	**33**	**43**	**39**	**29**	**144**

Table 2 – Primary Oppositional Groups Represented

Policy	Groups
CDA	• American Civil Liberties Union (ACLU) • Center for Democracy and Technology (CDT) • Electronic Frontier Foundation (EFF) • American Library Association (ALA)
COPA	• American Civil Liberties Union (ACLU) • Center for Democracy and Technology (CDT) • Electronic Privacy Information Center (EPIC)
CIPA	• American Civil Liberties Union (ACLU) • American Library Association (ALA)
SOPA/PIPA	• American Civil Liberties Union (ACLU) • Center for Democracy and Technology (CDT) • American Library Association (ALA) • Electronic Frontier Foundation (EFF) • NetCoalition

Coding Scheme

The collection of 144 documents obtained through the process described above comprised 3891 pages of material. Those pages provided the documentary evidence for the more substantial coding that took place. This section will explain the coding process that was used to evaluate the central themes and frames that emerged from this source documentation.

Based on a first review as documents were being collected and organized, an initial coding scheme was developed. This scheme represented the general themes that emerged from the documentary evidence and formed the basis for the more thorough coding process that followed. First, the basic master frames for both the legislative supporters of these Acts and the oppositional groups were identified. As noted previously, master frames represent the primary motivations and justifications for these policies as well as the motivations of oppositional groups. From the legislative

documents, three primary master frames appeared and indicated that the state based these policies on its interest in protecting children from harmful online content (LMF1), the government's interest in protecting intellectual property from theft (LMF2), and the desire to safeguard national security (LMF3). The opposition's primary interest was protecting individual autonomy (OMF1), preserving transparency for the user/citizen (OMF2), and safeguarding access to protected speech (OMF3).

The diagnostic frames, or how each side defined the problem, were also isolated through this process. Across all of these policies, legislators consistently argued that the Internet, and unregulated access to it, was the source of the problem. Specifically, unregulated access to online content harmed children (LDF1), led to the theft of intellectual property (LDF2), and endangered national security (LDF3). The opposition, on the other hand, argued that serious problems were created by these policies and the technological mechanisms of enforcement they required. For instance, these policies in general and their technological access controls in particular harmed individual autonomy (ODF1), introduced opacity for the user (ODF2), and had the tendency to reduce access to protected speech (ODF3).

The basic prognostic frames, or the solutions proposed to address these problems, were identified as well. Legislative supporters of these policies repeatedly argued for technological solutions and insisted that access controls would protect children (LPF1), intellectual property (LPF2), and could help ensure national security (LPF3). For the opposition, the solution relied on the minimization of technological systems. These groups argued that regulatory technology should be narrowly enforced or removed from statutory language altogether (OPF1), access controls should be made as transparent as

possible for the citizens forced to operate under them (OPF2), or that these policies should be heavily revised or simply struck down as unconstitutional (OPF3).

Figure 1 provides the coding scheme based on this initial review.

Figure 1 - Coding Scheme

Data Coding and Analysis

With the basic coding scheme established, document analysis began. After the source documentation was organized by policy, the items were reviewed manually. Beginning with the earliest policy (the CDA) and ending with the most recent (SOPA/PIPA), the codes were marked on individual passages of text that were responsive to the themes outlined in Figure 1. Writing in the margins of these documents, these passages were labeled with all codes that applied. Most responsive passages were relevant to more than one theme and were coded accordingly. After this manual review process was done thoroughly for each document, some re-review took place to ensure accuracy in the coding. It is important to note that this coding scheme was not considered exhaustive and documents were reviewed from the perspective that additional themes might emerge. Even with this possibility in mind, no additional codes were warranted and the original coding scheme provided the necessary framework.

As the documents were reviewed, a number of code indicators became apparent. These indicators consisted of specific words and phrases that, taken in context, implied the need for one or more codes. For example, terms such as "protection" or "harmful" often indicated a relationship to the government's master frame regarding the protection of children (LMF1). Similarly, terms such as "empowerment" and "access" became useful indicators of the opposition's master frame related to the protection of individual autonomy (OMF1). A sample of these coding indicators is provided below in Table 3.

Table 3 – Sample Code Indicators

CODE	SAMPLE INDICATORS
LMF1	Protection, Pornography, Children/Minors, Harmful, Indecent
LMF2	Property, Theft, Infringing, Piracy, Illegal, Rogue, Protect
LMF3	Security, Counterfeit, Health, Prescription, Consumers, Rogue
LDF1	Children/Minors, Access, Harmful, Regulate, Restrict, Problem
LDF2	Theft, Piracy, Infringing, Property, Illegal, Rogue, Regulate
LDF3	Security, Protect, Counterfeit, Prescription, Consumers, Health
LPF1	Protect, Children/Minors, Harmful, Access, Pornography
LPF2	Property, Intellectual, Protect, Theft, Illegal, Rogue
LPF3	Security, Protect, Property, Counterfeit, Consumers, Health
OMF1	Autonomy, Empowerment, Control, User, Content, Access
OMF2	Transparency/Opacity, Blocking/Filtering, Categories, Keywords
OMF3	Speech, Access, Constitutional, Protected, Censor
ODF1	Autonomy, Empowerment, Harm, User, Control, Access
ODF2	Transparency/Opacity, Categories, Keywords, Trade Secret
ODF3	Speech, Access, Protected, Constitutional, Censor, Block/Filter
OPF1	Blocking/Filtering, Access, Constitutional, Software, Technology
OPF2	Transparency/Opacity, Blocking/Filtering, Trade Secret, Access
OPF3	Constitutional, Access, Amend, Revise, Strike Down, Illegal

For the sake of clarity and so that the analysis may be replicated if necessary, it is also useful to provide examples of the coding process itself. For instance, a responsive passage appears in Representative Mike Oxley's (R-OH) press release of October 13, 1998 regarding the Child Online Protection Act (see COPA07). On page two of this press release, Oxley states that "The ready availability of hardcore pornography to kids on the Web is a problem that we need to solve." This passage is responsive to two separate codes. First, Oxley addresses the government's compelling interest in protecting children online. This is directly related to the state's first master frame and triggers code LMF1. Second, because Oxley references the legislative definition of the problem, the diagnostic frame is indicated and code LDF1 is applied. Thus, both LMF1 and LDF1 are noted in the margin for future reference.

Another example appears in the transcript from the Judiciary Committee's November 16, 2011 hearing on the Stop Online Piracy Act (see SOPA06). On page 262 of this transcript, Senator Ron Wyden (D-OR), as a critic of SOPA and PIPA, describes competing approaches to online regulation and argues that, "Instead of having government censor the web, we developed an approach that would empower users and technology to address content concerns on their own." Wyden's reference to user empowerment is directly responsive to the opposition's master frame regarding the protection of individual autonomy (code OMF1). Wyden also mentions the potential for state censorship of online content. This suggestion triggers code OMF3 related to the opposition's call for the preservation of protected speech online. Wyden's reference to the voluntary use of technology to control content is also important and makes this passage of particular interest within the context of this oppositional frame.

Once these responsive passages had been identified, these segments of text were copied into a Microsoft Excel spreadsheet, or, where electronic versions were unavailable, manually transcribed. The review process of this legislative and oppositional documentation yielded 4949 total coding entries. The actual number of unique entries, however, was lower owing to the fact that passages were often responsive to more than one code. In such cases, individual entries for each code were made in the Excel coding spreadsheet. A separate spreadsheet for each side of the debate (legislative and oppositional) was created for each policy. Once this process was complete and all documents had been reviewed, coded, and transferred to Excel, these spreadsheets were imported into the NVivo 10 qualitative coding software for organization and further analysis. A breakdown of the total number of coding entries imported into NVivo is included below in Table 4.

Once in NVivo, the entries could be analyzed by code, by policy, or by some combination thereof. NVivo was then used to examine each of the codes as it applied to each policy. For example, all 117 entries responsive to code LMF1 for the CDA were reviewed in order to isolate the thematic narrative that formed around this code. This process was repeated for LMF2, LMF3, etc. In this sense, a form of open coding was performed where the data represented within the coding entries was "broken down into distinct incidents, ideas, events, and acts" in order to "open up the text and expose the thoughts, ideas, and meanings contained therein" (Strauss and Corbin, 1998, p. 102). Again, this was done for each code and within each policy and the end product of that additional review formed the basis for the frame analysis provided within Chapters 4 through 7 of this dissertation.

Table 4 – Coding Totals

Code	CDA	COPA	CIPA	SOPA/PIPA	Total
LMF1	117	73	120	0	**310**
LMF2	0	0	0	138	**138**
LMF3	0	0	0	52	**52**
LDF1	107	96	120	0	**323**
LDF2	0	0	0	130	**130**
LDF3	0	0	0	27	**27**
LPF1	80	124	113	0	**317**
LPF2	0	0	0	123	**123**
LPF3	0	0	0	21	**21**
OMF1	100	88	89	2	**279**
OMF2	0	5	50	0	**55**
OMF3	179	312	402	213	**1106**
ODF1	90	95	88	0	**273**
ODF2	0	10	51	0	**61**
ODF3	220	304	382	197	**1103**
OPF1	86	127	120	56	**389**
OPF2	0	0	29	0	**29**
OPF3	41	71	39	62	**213**
Total	**1020**	**1305**	**1603**	**1021**	**4949**

Additional analysis of these policies, frames, and codes remains for future research. Specifically, although this investigation provides detailed insight into each policy and each code, the convergence of these codes across policies was not examined. Similarly, a longitudinal analysis of these frames from the earliest policy to the most recent could provide a deeper understanding of how these themes evolved incrementally over time. Next, secondary sources such as media reports could be examined to further triangulate information related to the portrayal of these policies and the regulatory technologies they required. In addition, in the event that similar policies are proposed in Congress, those new cases could help refine and verify the conclusions of this research. Finally, examples of these kinds of policies from other national contexts could be analyzed in a similar manner for additional insight.

Delimitations

There are three primary delimitations predicated on the structure of this dissertation. The first relates to the national context of this research. Confining this investigation solely to United States policy obscures the broader international picture. In addition, by narrowing this analysis to the U.S. example, this research does not answer questions related to the larger effects of local regulation in a global medium. This approach also does not account for any other country's efforts to regulate content online or address their specific constitutional, ethical, or political commitments (or lack thereof). Nevertheless, these questions are important and remain of interest for future research.

Second, the methodological approach of this dissertation creates necessary but important limitations. Specifically, by focusing the frame analysis only on governmental/legal sources and other direct documentary evidence, some of the richness of the national dialogue on these issues is lost. For example, this excludes the voices of media outlets, citizen bloggers, and other interested stakeholders. Yet, by narrowing the investigation to a representative yet practical sample of the evidence, it is possible to conduct a thorough study of these issues while maintaining a manageable scope.

Finally, although this dissertation is deeply concerned with the non-neutral nature of regulatory technologies, this research will not delve into the minutia of the technological design process. In order to address the macroscopic issues of policy and democratic rights, this analysis will focus more broadly on the portrayal of these technologies and the immediate implications they have had when mandated by federal regulation. Again, each of these delimitations is ripe for future research.

Summary

This dissertation will describe policies that span a period of fifteen years. During that time, technology has become more prevalent in our society and the Internet has penetrated more deeply into our daily lives. Managing the kinds of content that are available and deciding how to mediate access remains an important regulatory concern. Yet, despite the passage of time, a fundamental lack of technological sophistication at the legislative level and a failure to recognize the political nature of technology seems to remain. Like Senator Exon, subsequent policymakers have sought to control a medium they may not completely understand. Coupled with this misunderstanding is a tendency on the part of lawmakers to compound the problem by using technological solutions to regulate online content. Without exception, these policies have faced serious constitutional challenges directly related to these regulatory technologies.

It is necessary to address these constitutional concerns with a more nuanced, more critical assessment of how these kinds of technological systems will function after implementation and an appraisal of how they will affect individual rights and autonomy. Science and Technology Studies provides the kind of theoretical lens necessary to bring these problems into sharper focus. Although there a number of differing points of view among STS scholars and although STS is not itself a panacea, as a discipline it has consistently offered the kinds of critiques necessary to understand the non-neutral nature of technology, the socially constructed character of its design and the manner in which technology functions politically. Combined with the frame analysis methodology, the theoretical lens of STS can demonstrate the kind of critique necessary to improve future

information policies and points within the policy process where this analysis can be included to the greatest benefit.

At the conclusion of this research, it will be possible to isolate specific points within the policy process (master, diagnostic, or prognostic frames) where lawmakers have failed to consider critically the technological barriers to access that these policies would impose. Parallel to this, it will be possible to locate where in the oppositional process various groups have offered a more critical assessment of technology and technological mechanisms of enforcement. In order to accomplish this, it will be necessary to identify where in the process both groups have or have not discussed how technological systems can impact individual rights and autonomy in a manner consistent with STS.

By describing how legislators have portrayed technology, this research can offer recommendations as to where a more critical assessment can best be included in the policy process. By illustrating how and where oppositional groups have made use of a more critical understanding of technology, this will demonstrate the kind of critical analysis legislators should be including within their debates. Particularly if the judiciary has incorporated these arguments into their opinions and if subsequent laws echo those rulings, this will help to validate both the oppositional arguments and, by inference, arguments provided by Science and Technology Studies. STS provides the substance of the critical analysis that should be included in the legislative process and frame analysis pinpoints where to apply STS concepts. If lawmakers employed such a framework at the necessary points within the policy process, future information policies may be less likely to harm individual rights, autonomy and constitutionally protected speech.

Chapter 4 – The Communications Decency Act

Introduction

This chapter will describe the background and history of the Communications Decency Act of 1996. In keeping with the frame analysis methodology outlined in Chapter 3, what follows is a primarily empirical description of the master, diagnostic and prognostic frames advanced by both the legislative supporters of the Act and those groups who vehemently opposed this policy.

Congressional supporters of the Communications Decency Act based their frames on the premise that it is one of the fundamental duties of the state to protect children. In this case, supporters of the Act believed that they must intervene through policy and through technological mechanisms of enforcement in an effort to protect children from online content they deemed to be indecent. That compelling government interest underpins the entire debate surrounding this policy and extended to the government's assessment that unregulated access to the Internet was the source of that harm. Therefore, from this point of view, the only sensible means for addressing this problem was to impose technological barriers to access around that content.

Despite this, as will be described, the opposition would argue that the fundamental duty of the government in this situation was not only to protect children but also to safeguard adult access to constitutionally protected speech online. In doing so, the state was obligated to ensure the autonomy of the individual – especially when considering the nature and potential of this new medium. The opposition would go on to assert that the scope and technological requirements of this law would have the direct effect of diminishing autonomy and reducing access to protected speech.

Part I – Legislative Master Frames

When drafting the amendment that would eventually become the Communications Decency Act (CDA), Senator Exon and his supporters were overwhelmingly motivated by the perceived need to "protect children from exposure to sexually explicit material that is now widely disseminated on the Internet" (CDA14 p. 20).[2] In service of this master frame, the government sought to advance "methods of compliance [that] are technologically feasible" (CDA16 p. 25) in order to achieve the "compelling interest that government and all of society have in protecting minor children from premature exposure to patently offensive pornography" (CDA16 p. 10). In effect, the CDA was to be nothing less than a means to "establish a uniform national standard of content regulation" (CDA13 p. 49). This new standard would draw a clear and bright line, safeguarding generations of children from online perverts and predators who would seek to do them harm and, in the process, ruin the nascent "educational and informational" (CDA01 p. 100) resource the Internet might become.

From the first, the CDA seemed to be at cross-purposes with its host legislation. Embedded within the Telecommunications Act of 1996, the CDA sought to expand the scope of federal law "to provide for consistent national and State and local content regulation of both commercial and non-commercial providers" (CDA03 p. 203). In contrast, Congress intended the Telecommunications Act itself "promote competition and

[2] The exact statutory language reads as follows: "Whoever--in interstate or foreign communications knowingly--uses an interactive computer service to send to a specific person or persons under 18 years of age, or uses any interactive computer service to display in a manner available to a person under 18 years of age, any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication" (CDA01 pp. 95-96).

reduce regulation in order to secure lower prices and higher quality services for American telecommunications consumers" (CDA01 p. 1). The stated purpose of the CDA seems to directly contradict national policy directives which called on legislators "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation" (CDA01 p. 101). Despite this, the master frame of protecting children allowed Exon and his colleagues to convince most of Congress that a strict national standard for content regulation should be included within a bill meant to limit barriers to competition. By invoking the need to safeguard America's children, Exon had at his disposal a strongly "resonant" rhetorical frame that was difficult for other legislators to oppose (Benford & Snow, 2000, p. 619). What politician wanted to vote against the need to safeguard kids in cyberspace?[3] Initially, the CDA and its technological mandate may have passed not on its merits but because it was "seen as a good press release back home so people voted for it" (CDA24 p. 1). Supporters seem to have thrust aside concerns over the scope of the law or the constitutional implications of its enforcement in the interest of safeguarding kids without delay. Political expedience may also explain the ease with which the amendment passed the Senate in a landslide 86 to 14 vote (CDA24 p. 2). The master frame of protecting children implied an urgency that pressured elected officials to act too quickly. In their haste to do so, lawmakers may have overlooked important considerations regarding the efficacy of the policy and the imposition of regulatory technologies. [4]

---

[3] As Senator Leahy, a vocal opponent of the CDA, would later recall, "Too many Members feared the demagogic syllogism that if they voted against a censorship law purporting to protect children, they must be in favor of exposing children to inappropriate violent or pornographic material. This is a false syllogy" (CDA05 p. 1).

[4] Exon introduced the CDA on February 1, 1995 and Congress had already passed it as an amendment to the Telecommunications Act by June 14th of that same year.

Aside from its political and ideological attraction, the CDA also included a number of affirmative defenses intended to make it more palatable to industry stakeholders as well as to lawmakers who wished to preserve the anti-regulation bent of the Telecommunications Act. The first of these provisions provided a safe harbor for Internet service providers (ISPs) and absolved them from liability if their involvement was "solely for providing access or connection… that does not include the creation of the [indecent] content of the communication" (CDA01 p. 96). Supporters predicated the remaining affirmative defenses on the need to impose technological barriers to access in exchange for immunity from prosecution under the CDA. These technological "enabling tools" would provide ISPs, employers and others with the means to "filter, screen, allow, or disallow content" (CDA01 p. 102). Despite this, in what appears to be a rhetorical inconsistency, the text of the CDA itself marveled at how the Internet had "flourished, to the benefit of all Americans, with a minimum of government regulation" (CDA01 pp. 100-101) while supporters of the Act publicly lamented its necessity. They sadly acknowledged that "Sometimes our technology races beyond our reflection, and we are left with a dangerous gap - a period when society is unprepared to deal with the far-reaching results of rapid change. That is the situation we have on the Internet. This is the situation which [the CDA] will address" (CDA16 p. 28). More regulation, although regrettable, was the only solution to the blight of pornography. This was nothing less than a war for the purity of America's children and the future of the Internet. "Failure to enact strong laws is a concession that the information superhighway should belong to pornographers" and, by extension, the technological mechanisms required by the CDA's affirmative defenses should be the means to cast out pornographers.

From this point of view, the imposition of technological enforcement mechanisms to accomplish this goal was not only a natural but also a necessary solution. If technology (i.e. the Internet) created the problem then technology would have to solve it (CDA26 p. 50). Besides, from the legislative point of view, the CDA was a "technology flexible statute" that did not place onerous burdens on content providers but only required that they take "good faith actions under available technology to limit" access by minors to indecent material (CDA16 p. 24). Supporters of the CDA confidently proceeded from the assumption that there were "sufficient and adequate means already available under present technology" (CDA16 p. 25) that would satisfy this new content standard. Furthermore, as technology advanced, there would "undoubtedly be more ways to comply" with the law and the mere existence of the CDA would spur future innovation in regulatory technologies as "the market is encouraged by the presence of a legal obligation" (CDA16 p. 25). One of the unique aspects of the CDA is policymakers' reliance on the promise of future enforcement mechanisms. Technological "tools" for the protection of children would evolve as the landscape changed and forthcoming regulatory systems promised, "the potential for even greater control in the future as technology develops" (CDA01 pp. 100-101). The CDA's technological flexibility was its strength and the design of future regulatory systems would make this policy even stronger in years to come.

Despite its clarity of purpose and the promise of technological enforcement, the CDA was a policy in search of a metaphor. How to regulate the Internet and the content it carried depended uniquely on how both sides portrayed this new medium. What, exactly, was the Internet comparable to? Was it more like radio and television or was it

more like print? Were website operators individual speakers protected by the First Amendment or were they broadcasters who had "unique access" (CDA16 pp. 9-10) to the children of America? Were Internet Service Providers publishers in control of the content they carried or were they simply the "mailmen" (CDA25 p. 21) who delivered messages? The answers to these questions carried with them a framework for regulation that would permit or disallow certain technological configurations for enforcement of the CDA. That the CDA found a home in the Telecommunications Act is telling in this regard. Proponents of Senator Exon's amendment rallied around the notion that "the Net is still closer to broadcasting than to print" (CDA08f p. 25) and, thus, the CDA was both constitutional and clearly within the federal government's regulatory purview. By portraying the Internet as a broadcast medium, Congress could imply constitutional merit by association. If it "was constitutional for the FCC to channel indecent broadcasts to times of the day when children most likely would not be exposed to them" it was certainly acceptable to legislatively "channel indecent communications to places on the Internet where children are unlikely to obtain them" (CDA14 p. 18). Here the government turned to broadcasting case law that emphasized the persistent nature of the medium and its unique ability to invade the home. Specifically, the government argued that in *FCC v. Pacifica Foundation,* the Court had settled that the state could regulate radio and, by extension, the Internet differently.[5] In fact, the problem was exacerbated by the number of broadcasters on the Internet and "Because millions of people disseminate information on the Internet without the intervention of editors, network censors, or

[5] "Among the reasons for specially treating indecent broadcasting is the uniquely pervasive presence that medium of expression occupies in the lives of our people [and children]. Broadcasts extend into the privacy of the home, and it is impossible completely to avoid" (438 U.S. 726, 1978).

market disincentives, the indecency problem on the Internet is much more pronounced than it is on broadcast stations" (CDA14 p. 25). This new medium must be analogous to radio and television because it was everywhere all the time and kids could not help but be "inundated with pornography and smut on the Internet" (CDA19 p. 2).

Supporters also appealed to the preservation of public decency and invoked analogies to zoning laws as these areas offered some of the most familiar metaphorical ground for legislators. Lawmakers intertwined allusions to FCC broadcast regulations with the concept of zoning precisely because they allowed supporters of the CDA to advance the idea that online content fell under federal jurisdiction and that it was a tangible *thing* that the law could shuffle from place to place as decency dictated. Case law on these points had reliably demonstrated that the state not only had the ability to protect children from pornography[6] but that purveyors of it could be swiftly and constitutionally relegated to areas of town where children would not wander.[7] The government rested heavily on this kind of justification and consistently invoked geographic zoning law despite its potential inapplicability to a discorporate medium. In fact, the legislative master frames for this policy are replete with references to "cyberzoning" and assertions that, just as municipalities could "direct adult theaters away from residential neighborhoods, so Congress could direct purveyors of indecent material

---

[6] *Ginsberg v. New York*, 390 U.S. 629 (1968), "While the supervision of children's reading may best be left to their parents, the knowledge that parental control or guidance cannot always be provided and society's transcendent interest in protecting the welfare of children justify reasonable regulation of the sale of material to them. It is, therefore, altogether fitting and proper for a state to include in a statute designed to regulate the sale of pornography to children special standards, broader than those embodied in legislation aimed at controlling dissemination of such material to adults."

[7] *Renton v. Playtime Theatres, Inc.,* 475 U.S. 41 (1986), "The Renton ordinance…does not ban adult theaters altogether, but merely provides that such theaters may not be located within 1,000 feet of any residential zone, single- or multiple-family dwelling, church, park, or school. The ordinance is therefore properly analyzed as a form of time, place, and manner regulation."

away from areas of cyberspace that are easily accessible to children" (CDA14 p. 18). Therefore, in the context of this argument, websites that provided access to indecent content were indistinguishable from indifferent cashiers who obligingly sold pornographic magazines to curious minors. That the CDA should essentially "move" those storefronts away from schools and neighborhoods was a natural corollary. Again, the technological means for doing so seemed self-apparent and the Internet, as a technological medium, would undoubtedly be uniquely conducive to technological regulation. Since the Internet was "malleable" it would be a simple matter "to construct barriers in cyberspace and use them to screen for identity, making cyberspace more like the physical world and, consequently, more amenable to zoning laws" (CDA18 p. 29). The barriers themselves were nothing more than a technological "gateway" (Id) keeping kids away. By defining the need for and scope of enforcement in this way, these gateways would have no more impact on democratic society than did fencing around school playgrounds.

Therefore, for Senator Exon and other supporters of this legislation, the CDA was based on "law that has been in effect and been approved constitutional with regard to pornography…We're not out in no-man's land…We're trying to expand that as best we can to the Internet" (CDA24 p. 2). Like Easterbrook's law of the horse, the master frames here consistently rely on rhetorical references to traditional forms of regulation and traditional notions of community decency. In addition to broadcast conventions and zoning laws, other metaphors of physicality continually underpinned legislative justifications for the CDA and Senator Exon often appealed to the hypothetical "public outrage" that would result if pornographic images were posted on "lampposts and

telephone poles for all to see" (CDA25 p. 20). Failure to take action against such atrocities was nothing less than "taking a porn shop and putting it in the bedroom of your children" (CDA25 p. 24) or "leaving a loaded gun on a playground" (CDA08d p. 13). This hyperbole served to clarify the legislative master frame that Congress must protect children and that, although the Internet was something new, it was not so new as to be exempt from centralized regulation and control.

Reliance on these metaphors and the concept of cyberzoning was not only constitutionally proper from a historical and precedential perspective; it also served to ameliorate any First Amendment concerns that might manifest. Cyberzoning did not implicate the rights of adults because Congress focused the law and its technological requirements solely on children. The CDA was not inhibiting speech, simply relocating it to clearly demarcated areas cordoned off by regulatory systems. There were no constitutional effects because the law would not harm the ability of consenting adults to communicate directly with one another. As the government put it, the state's "interest in protecting children from patently offensive sexually explicit depictions and descriptions is as legitimate and unrelated to the suppression of constitutionally protected expression as the government's interests in reducing crime, maintaining property values, and preserving the quality of urban life" (CDA14 p. 27). Therefore, "as long as a government zoning scheme is justified by the effects of indecent communications on children rather than adults, and leaves open reasonable opportunities for adult-to-adult communication, it is constitutionally permissible" (Id).

This focus on the protection of children to the exclusion of all else is a defining element of the CDA's legislative master frames. Supporters often swept aside any

concerns about prohibitions on access with rhetorical flourishes that prioritized the needs of children above the constitutional rights of adults. Senator Exon argued that Congress should not play politics while children were encountering online pornography on a daily basis. It was important that other legislators and the public recognize the necessity of regulation when "We are talking about our most important and precious commodity - our children" (CDA19 p. 2). It was equally unthinkable that speech rights could take precedent over the innocence of children. "We cannot simply throw up our hands and say a solution is impossible or the First Amendment is so sacrosanct that we must stand idly by" (CDA19 p. 2). Besides, Exon and his supporters repeatedly affirmed that allowances for the First Amendment were built into the CDA and that the law would "not ban any constitutionally protected material from adults" (CDA06 p. 1). In fact, this new law and the technology it would require would protect "children in ways that are consistent with America's free speech values" (CDA08a p. 4). With "the right technology", regulation could keep kids safely out of the "red light districts of cyberspace" (Id) while permitting adults entry. Even if the CDA might "impose some burdens and costs on adult-to-adult communication of indecent material", it was far better to burden those who peddled "offensive material…than it is to leave children unprotected" (CDA14 pp. 18-19).

In fact, Exon frequently characterized those opposed to the CDA "as a bunch of First Amendment belly-achers" (CDA02 pp. 21-22) who hid behind the Constitution at the expense of America's youth. In their opposition to the Act, these misinformed activists mistakenly believed "that Thomas Jefferson and all of the good people who wrote the Constitution worked overnight and planned and plotted to make sure that the

Constitution protected the most gross pornographers, pedophiles, those who are trying to lure children today" (CDA02 p. 71 actual). This was a common theme used frequently to assuage any constitutional misgivings expressed by those who did not support the CDA. In Exon's view, nothing should supersede the duty of the state to protect children. Only misguided "opponents of the Decency Act [would] rationalize that the framers of the Constitution plotted at great length to make certain that the profiteering pornographer, the pervert and the pedophile would be free to practice their pursuits in the presence of children on a taxpayer-created and subsidized computer network" (CDA04 p. 4). With the stakes so high, it was preposterous that opponents of the CDA would allow the Internet to go unregulated. It was nothing less than anarchy when "critics say that on the Internet, anything should go, no matter how outrageous" (CDA19 p. 1).

This may indicate that the master frame of protecting children qualifies is a core "metacultural frame." The power of this frame derives in part from its appeal to "the broadly shared beliefs, values, and perspectives familiar to the members of a societal culture…on which individuals and institutions draw in order to give meaning, sense, and normative direction to their thinking and action in policy matters" (Schon & Rein, 1994, p. xiii). Therefore, the normative need to establish "rules of the road" for the information superhighway trumped other considerations when "the most vile" content was "only a few click-click-clicks away from any child" (CDA14 p. 13). This may account not only for the ease with which the CDA passed the Senate but also why legislators felt it was unwise to vote against such a policy for fear of the political consequences.

Master frames of this kind may also make it less likely that legislators will devote serious time or effort to conducting a critical analysis of the policy's enforcement

structure. In this case, lawmakers essentially tabled any serious review of the technological mechanisms outlined in the CDA's affirmative defenses. Politicians may have been so concerned with advancing the fundamental value of protecting children that they failed to address the technological specifications of the systems that the policy required. Empirical evidence does exist suggesting that policies surrounding morally charged, ideological issues are less likely to undergo serious analysis[8] and documentary evidence here does support that conclusion. For example, when Senators Leahy, Feingold requested that the Department of Justice examine the amendment and its technological requirements prior to calling for a vote, there was outrage that politicians would delay such an important matter for something so trivial as review and analysis.[9]

All of this would seem to indicate that the articulation of master frames might be one of the key moments in the policy process where a significant critical review of technological mechanisms of enforcement may be lacking. Specifically, when Congress invokes the need to safeguard the innocence of America's children as the primary justification for online regulation, it appears to result in a knee-jerk reaction that leaves little interest in any technological or constitutional scrutiny.

---

[8] Literature describing "morality policy" and its effects explores this phenomenon most thoroughly. "When designing morality policy, members of Congress and their staff use more information about constituents' personal experiences and other emotive information than technical policy analysis, they seek out less information, and they use the information they receive more selectively than when they are designing nonmorality policy" (Goggin & Mooney, 2001, pp. 130-131).

[9] "Although Senator Patrick Leahy and others may urge that the matter be referred to the U.S. Department of Justice for its review and analysis, we [the Christian Coalition] oppose such a course of action. The increasing existence of computer pornography today requires action, not more study" (CDA25 p 28).

Part II – Oppositional Master Frames

Opposition to the CDA coalesced almost instantaneously. In addition to the legislative disapproval of Senators Leahy, Feingold and others, several external groups quickly joined the fray. The American Civil Liberties Union (ACLU) was one of the first and most vocal groups to criticize the law and its technological assumptions. The ACLU, as an organization primarily concerned with First Amendment considerations, would also go on to file the legal challenge to the CDA, eventually taking the case to the Supreme Court. Other groups focusing on rights-based and technology-based frames also contributed significantly to the debate. The desire to preserve a mostly unregulated Internet and to advocate for a more democratic application of technology motivated the Electronic Frontier Foundation (EFF) and the Center for Democracy and Technology (CDT). The stated goals of both the EFF and CDT rhetorically align with the STS framework outlined in Chapter 2. Whether consciously or not, these organizations echo the research of Richard Sclove, Langdon Winner and others in their mission to "support freedom-enhancing technologies" (About EFF, 2014) and "define the boundaries of technology in our daily lives" (CDT Mission and Principles, 2014). The opposition of these organizations and others would offer a striking counterpoint to the legislative justifications for the CDA. Instead of focusing exclusively on the need to protect children, these oppositional groups suggested that a more nuanced approach was required. This included a much different narrative emphasizing the need to safeguard individual autonomy and the absolute requirement that any regulation preserve access to constitutionally protected speech. The opposition's master frames provide an alternative portrayal of the Internet and the technological mechanisms of enforcement required by the CDA.

First, the opposition's conception of the Internet differed drastically from that put forward by Exon and his supporters. Rather than characterizing this new medium as a wild frontier desperately in need of regulation or as a dangerous conduit for minors' access to pornography, these groups emphasized the promise of the Internet as a means of communication (CDA13 p. 24). The Internet had unprecedented potential as a democratic forum (CDA23 p. 5), with vast "social and political significance" (CDA26 p. 176). Its lack of regulation was precisely what made this medium so important. The imposition of technological controls and government standards would "stifle" both the growth of the Internet and the vibrancy of the conversations already underway (CDA26 p. 12). Where Exon and his supporters were, by necessity, bound to metaphors of physicality, zoning, and broadcasting, the opposition articulated a different conception entirely. The Internet, "unlike every other mass medium that has ever existed…has no central authority. There is no person in charge of the 'printing press,' no 'editor-in-chief,' no holder of a broadcast license. Americans have discovered that one can reach a large audience on the Internet without having to assemble a lot of capital or seek the approval of an editor" (CDA26 p. 178).

Opposition to the CDA consistently emphasized how the Internet defied comparisons to existing broadcast media and the associated regulatory frameworks. Unlike radio and television, the Internet was neither ubiquitous nor pervasive. If anything, affirmative action was required to access indecent content and the "user [was] not likely to stumble upon the offensive" (CDA02 pp. 30-31). In fact, autonomy of the user was one of the primary master frames employed throughout the course of the opposition's campaign. Congress and the FCC, as regulatory bodies, had no place online

because the introduction of any central authority was antithetical to the decentralized nature of the medium (CDA13 p. 7). Not only would government regulation fly in the face of the Internet's design principles, as a practical matter, "it would not be technically feasible for a single entity to control all of the information conveyed on the Internet" (Id p. 8). As the Telecommunications Act and the administration's policy initiatives implied, the Internet must be free in order to flourish. From the opposition's point of view (and reminiscent of cyberlibertarian philosophy), regulation and technological mechanisms of enforcement must be "rejected in favor of decentralization and self-determination; censorship [must be] rejected in favor of democratic discourse" (CDA02 p. 44).

User empowerment was at the heart of the opposition's master frames and offered a rhetorical device that may have been as resonant as the legislative frame of protecting children. A report prepared for Senator Leahy by several technology and media companies underlined this point. If the Internet, as a democratic forum, was to retain its unique potential "individuals should be able to speak freely and frankly about issues of their choosing, without fear of reprisal because many people may not agree with or appreciate the nature and content of their messages" (CDA23 p. 16). Numerous scholars cited previously in this dissertation have written extensively on the absolute requirement of individual autonomy when considering policies that employ technology to constrain behavior (e.g. Sclove, Brey, Carroll, Noble, Barker & Downing, etc.). Although the EFF, ACLU, CDT and other opponents of the CDA did not rely on this literature to advance their arguments, both underline the importance of user empowerment.

Although the opposition here emphasized the differences between Internet access and traditional broadcast media, they were just as subject as Exon and his supporters

were to reducing the Internet to a comfortable metaphor. In this case, the opposition emphasized how the medium was very much like print and, consequently, deserved the same rigorous constitutional protection (CDA07 p. 1). Just as print was not subject to centralized editorial control, neither should online content producers be subject to a uniform regulatory standard. This metaphor was bound to the master frame of safeguarding individual autonomy and helped advance the argument that, "every individual is a potential publisher on the Internet" (CDA08f pp. 17-18) who should be free to "exchange information on a vast array of subjects with a worldwide and virtually limitless audience" (CDA15 p. 2). This master frame of individual choice (and individual responsibility for protecting one's children) would go on to form one of the pillars of the opposition's legal argument. As will be discussed later, it also led to oppositional advocacy for screening and blocking technology (such as the voluntary use of commercial filtering software) meant to empower the user. Again, this argument relied on the need to strengthen individual autonomy but, as will be shown, it also demonstrated some oppositional misconceptions about the neutral and instrumental nature of content filters – misconceptions that would haunt these same groups during the negotiation of future policies.

In addition to arguments of autonomy, the motivation for the oppositional master frames included the desire to safeguard access to constitutionally protected speech. Here the opposition focused intensely on the government's fundamental misunderstanding of the medium as well as the nature of regulatory systems. First, Exon's failure to recognize the Internet as a "unique and emerging medium of communication" had, from the opposition's point of view, "led to a constitutionally offensive statute" (CDA02 p. 32).

Furthermore, the "failure of Congress to appreciate this emerging technology" (Id) completely undermined their attempts to regulate it. As the opposition repeatedly argued, "legislators simply do not understand how this medium really works" and, because of this, "We should all be very concerned when anyone tries to stop us from sharing ideas and communicating with each other simply because they do not understand that new technology" (CDA08e p. 14). Appeals to the unique nature of the Internet and its vast differences from traditional broadcast media undercut the CDA's regulatory legitimacy (CDA20 p. 1). For example, the opposition argued that the Internet, as a medium for instantaneous and widely distributed communication, did not distinguish between audience members. Taking the time and technological steps necessary to do so would cripple content producers' ability to communicate effectively. The CDA essentially required that these content producers "assure that their indecent expression is not 'available' to minors" (CDA17 p. 21). Ensuring that access to children was prohibited "has precisely such an unconstitutional effect for most speakers and most modes of communication, because there is no way to satisfy that requirement other than by refraining from speech" (Id). The practical and technological necessities of the CDA, combined with Congress' misunderstanding of the medium had the direct effect of reducing access to constitutionally protected speech. As the opposition would argue through this master frame, "Because it misunderstood the nature of the Internet, Congress thought it could protect indecent speech between adults while regulating speech available to children" (CDA17 p. 22). Yet this was neither technologically feasible (CDA15 p. 1) nor desirable and required online speakers to censor themselves to safer content. Not only did this neuter the potential of the Internet as a democratic forum but, as the

opposition argued, any "statute that reduces adults to reading and seeing only what is fit for children cannot be sustained under the First Amendment" (CDA15 p. 10). As will be discussed below in the context of diagnostic frames, the opposition also had deep concerns about how the specific technological mechanisms required by the law would function as deterrents for free speech and would reduce access to constitutionally protected content. The very nature of these regulatory systems, the opposition would argue, hindered the vibrancy of conversations already underway and, more insidiously, chilled speech preemptively.

In addition to these master frames of safeguarding individual autonomy and safeguarding access to protected speech, the opposition here consistently called for a more in-depth and critical process of review prior to enacting the CDA. Legislative opponents of the policy connected the need for further study with both individual autonomy and free speech guarantees. The need to "empower parents and users" related directly to the need to engage with experts and other stakeholders "before we start imposing liability in ways that could severely damage electronic communications systems, sweep away important constitutional rights, and possibly undercut law enforcement at the same time" (CDA25 p. 32). There had been only one major hearing[10] on these issues prior to passage of the Act and important provisions "were either added in executive committee after the hearings were concluded or as amendments offered during floor debate on the legislation" (CDA18 p. 10). In some cases, "Congresspersons voted

[10] See "Cyberporn and Children: The Scope of the Problem, the State of the Technology, and the Need for Congressional Action." Hearing before the Committee on the Judiciary, United States Senate, One Hundred Fourth Congress 1st Session on S. 892 – A Bill to Amend Section 1464 of Title 18, United States Code, to Punish Transmission by Computer of Indecent Material to Minors. July 24, 1995 (Serial No. J-104-36) (CDA26).

for passage of this regulation without even having time to read, much less consider the impact of, the bill" (CDA09 p. 3). The opposition roundly criticized Exon and his supporters for failing to contemplate the constitutionality and technical requirements of the policy in their rush to push it through Congress. In addition to the Justice Department review advocated by Senators Leahy and Feingold, the Electronic Frontier Foundation had called for a wider conversation on these issues. They lamented that "There have been no public hearings on this legislation. Neither the CDA, nor the larger Telecom Bill have been presented openly to the public" (Id). Due to this, "Congress has neither heard expert testimony about the medium and industry, nor allowed constituents to review and comment on what their 'representatives are doing'" (Id). Intertwined with its master frames was the opposition's repeated insistence that there was a need for critical review of the policy and its associated technology. These groups made a significant connection between the oppressive character of the CDA's mandate and the inability of many stakeholders to comment on it. As Winner has suggested, "Shielded by the conviction that technology is neutral and tool-like, a whole new order is built…without the slightest public awareness or opportunity to dispute the character of the changes underway" (Winner, 1977, p. 324).

Although the legislative master frame of protecting children had the necessary resonance to carry the vote in Congress, the opposition countered with several equally powerful frames. Appealing to the nature of the Internet as a communication medium and vast democratic forum, the ACLU, EFF, CDT, and other groups were able to provide a convincing counterpoint to the analogies of broadcast radio and television that defined the legislative portrayal of technology. The opposition had seized on some of the most

widely resonant "collective action frames" that included frames based on rights, choice and democracy (Benford & Snow, 2000, p. 619). This provided powerful ammunition in the public debate over the CDA.

When considered as a platform for free speech with minimal barriers to entry, the Internet ceased to be a "place" where large swaths of content could be roped off from public view. The concept of cyberzoning and other notions of physicality, the opposition argued, were outdated and did nothing to address the realities of this emerging technology (CDA18 p. 30). Julie Cohen and other scholars have remarked on the limitations of these metaphorical commitments and have cautioned against the invocation of "place- and space-based metaphors" to justify the extension of existing case law (Cohen, 2007, p. 211). The opposition here argued that this appeal to physical zoning laws and the imposition of technological barriers around content "would destroy a principal advantage of the Internet as a medium of communication: the ability of Internet users to research and communicate seamlessly and without interruption across its vast variety of available resources" (CDA12 pp. 7-8). Its competing portrayal of the medium led the opposition to several important arguments about the nature of the policy and the technologies it required. First, lawmakers should carefully evaluate these systems prior to implementation with an eye toward safeguarding individual autonomy. Second, all stakeholders should have the opportunity to comment on the policy prior to its implementation and should have the ability to critique the regulatory systems they would be forced to operate within. Third, this policy and the mechanisms it required had the direct effect of hindering both speakers and listeners in ways contradictory to the First Amendment.

Part III – Legislative Diagnostic Frames

Inextricably bound to the legislative master frame of protecting children from the pervasive presence of indecent material on the Internet was a diagnostic frame that emphasized how the ubiquity of pornography caused immense harm to minors. The invasive nature of the Internet, "if anything, deepens the Government's interest in protecting children from access to or receipt of online pornography" (CDA16 p. 20) and both the harm to children as well as the government's need to act were magnified because pornography was rampant online. The "problem" as defined by Exon and his supporters related directly to the unique access that children had to the Internet and their inability to process adult content that the Web would expose them to. Whether at home or, "more often, outside the home and outside parental control" (CDA16 pp. 9-10), minors could not help but encounter the "spine-tingling" content that the CDA forbade (CDA14 p. 13). It was a duty of the state to constrain access and, accordingly, "Congress sought to ensure that the 'brave new world' of interactive computer services would not be 'hostile to the innocence of our children'" (Id). This is the fundamental pillar of the legislative diagnostic frame: the government had to exert its authority to reduce, as much as possible, the harm that an unregulated Internet could inflict on kids. Adult content would have "deep and harmful effects on children that cannot readily be undone" because "children generally do not possess the same capacity as adults to make informed choices about whether to view indecent material" (CDA14 p. 20). The problem was twofold: first, indecent content harmed children and, second, that harm related directly to the Internet's complete lack of regulation. The problem required state action.

Congressional findings supported this assumption and emphasized that "the pervasiveness and casual treatment of sexual material…erod[es] the ability of parents to develop responsible attitudes and behavior in their children" (CDA01 pp. 103-104). The "simple premise" behind the CDA's diagnostic frame was that "it is wrong to provide pornography to children on computers" and it could scar them irreparably without strict regulation (CDA04 p. 2). Nevertheless, one of the key resources Congress relied upon when drawing this conclusion was itself deeply flawed. In 1995, Martin Rimm, an undergraduate electrical engineering student at Carnegie Mellon, published an inflammatory research paper on the issue of children and online pornography.[11] Among other things, the Rimm study concluded that "83.5% of all images posted" on the Internet were pornographic and many of these images were "pedophilic and paraphilic" in nature (Rimm, 1995). *Time* magazine picked up Rimm's study and repeated his findings in detail in a cover story that year.[12] This widespread coverage, confirming the deepest fears of Exon and others, was strong ammunition that helped bolster the diagnostic frame that unregulated access to the Internet harmed children irrevocably. Congressional supporters of online regulation latched onto both the Rimm study and the *Time* article and "waved a copy in front of the Senate" while "the ink was barely dry" (CDA02 p. 5). The problem with this supporting evidence for the CDA, however, was that Rimm's methodology was fundamentally unsound. Most notably, his conclusion that over 80% of all images online were pornographic was wholly inaccurate. Instead of reviewing anything close to a representative sample, Rimm had based this figure on "a small subset

---

[11] Rimm, M. (1995). Marketing Pornography on the Information Superhighway: A Survey of 917,410 Images, Descriptions, Short Stories, and Animations Downloaded 8.5 Million Times by Consumers in Over 2000 Cities in Forty Countries, Provinces, and Territories. *Georgetown Law Journal,* 83(5), 1849-1915.
[12] Elmer-DeWitt, P. (1995, July 3). Cyberporn – On a Screen Near You. *Time*.

of the Internet" composed entirely of adult bulletin boards (Christensen, 1995). As it turned out, Rimm's work had not been subject to peer review and, in addition to the paper's methodological problems, the author himself had been accused of ethical misconduct including plagiarism (CDA02 p. 6). In a bit of irony, Rimm had also been "working both sides of this issue" and in his spare time had authored "The Pornographer's Handbook: How to Exploit Women, Dupe Men, & Make Lots of Money" (Id). When Rimm's personal and professional shortcomings became public knowledge, Congressional support for the study evaporated even though support for the diagnostic frame did not. Congress abruptly cancelled Rimm's scheduled testimony although, as Senator Leahy would point out, the study had already exerted significant influence. Specifically, Leahy criticized his colleagues who had "voted in large part based on inflammatory stories about pornography on the Internet, like the study by Mr. Rimm" (CDA26 pp. 7-8). Leahy also noted during the hearing that Rimm "was supposed to be here, but got disinvited once a number of people brought out the fact that the study, which was treated as gospel on the Senate floor, was a little bit less than gospel. And I would expect any time now to see Time Magazine, for example, which did a cover story based on it, too, point out that even great media can be conned" (Id).

Despite these setbacks, Exon and his supporters continued to rely on the diagnostic frame that unregulated access to the Internet harmed children. In fact, they expanded the argument that, not only were kids at risk of continuous exposure to indecent content online and incapable of dealing with it once exposed, but they were also at risk because they were uniquely proficient with this new medium. Lawmakers often connected the argument of pervasiveness and accessibility to the idea that children had

become “the computer experts in our Nation’s families” (CDA14 pp. 13-14). Even Senator Leahy, as a leading opponent of the CDA, agreed that the youngest of “children are so adept with computers that they can sit at a keypad in front of a computer screen at home or at school and connect to the outside world through the Internet” (Id). Children as Internet “experts” became a recurring theme as supporters of the CDA defined their diagnostic frames (CDA19 p. 2). Those who opposed the CDA, they argued, had failed to recognize “the ease with which children can maneuver today’s computers, especially in the point-and-click icon format of the World Wide Web” (CDA16 p. 19).

Interestingly, during the major Congressional hearing on this issue legislative supporters juxtaposed their own ignorance of the technology in stark contrast to the technological expertise of kids. As Senator DeWine admitted, “My children, if they were here, would tell you that I am computer-illiterate” (CDA26 p. 48), while he and other legislators simultaneously suggested that they could effectively regulate the Internet through technological mechanisms of enforcement (Id p. 50). Despite their inexperience with the medium and the CDA’s mandated regulatory technologies, Congressional advocates of the policy believed that only their efforts could safeguard these young computer savants (and, presumably, that kids would be unable to find their way around such regulatory systems). Even though Senator Exon agreed that, while others may “know the technicalities of this far better than I” (CDA26 p. 152), the very “seriousness of the problem” was rooted in the fact that “computer literate children can easily find and retrieve” sexually explicit content (CDA14 p. 25). This fact demanded government intervention through policy (CDA16 p. 22).

Furthermore, minors' proficiency with the Internet and their skill at accessing indecent online content could damage not only their fragile psyches but also the "educational and informational" (CDA01 pp. 100-101) resource the Internet might become. Here the legislative diagnostic frame is bound to a strongly instrumental narrative that portrays the Internet as a "vast new world of information that will revolutionize how we all learn and work in the future" (CDA19 p. 1). It is interesting to note that this portrayal of the Internet as a "revolutionary development" (CDA22 p. 1) that was "unprecedented in world history" (CDA19 p. 1) differs significantly from the broadcast and zoning metaphors used previously to place the Internet in familiar regulatory territory. This contradiction appears repeatedly and, on at least one occasion, Senator Exon simultaneously emphasized that "computers" were a "unique medium" while arguing that the Internet was the same as "radio or television broadcasts where youngsters have unique access" (CDA19 p. 2). Despite this inconsistency, it was precisely because of the radical potential of the Internet that lawmakers must safeguard kids while using such a unique and powerful tool. Without some regulation and with the increased risk that kids would find their way to explicit content, the Internet would wither and die for fear of its seamier side. Although Senator Exon did "not claim to be an expert at it," the "Internet system" and its "multitude of good" uses were at risk (CDA22 p. 3).

This is another important part of the problem as defined by those supporting the CDA: parental fear of exposing their children to harm would act as a deterrent from using this vast new informational (and commercial) resource. The Internet "developed in part with taxpayer funds provided by the United States Government" (CDA26 p. 166) would never reach its full potential if that same government did not step in to correct the

situation (CDA14 p. 26). Therefore, it was essential that Congress "give America's parents a new comfort level in public and commercial computer networks if these are to be transformed from the private preserve of a special class of computer hackers into a widely used communications medium. This necessary transformation will never happen if parents abandon the Internet and computer communications technology remains threatening" (CDA14 p. 26). It was crucial that the state domesticate this burgeoning tool of education and commerce if it was to be of use. In harmony with the Telecommunications Act's mandate of increasing competition and reducing barriers to access, this aspect of the CDA's legislative diagnostic frame sought to increase participation online. Problem definition in this instance linked the harm inflicted on children directly to the harm inflicted on use of the medium itself. How was the Internet to achieve its full potential "if people are unwilling to avail themselves of its benefits because they do not want their children harmed by exposure to patently offensive sexually explicit material" (CDA14 p. 17)?

Congress had made its case clear: they must save children from the Internet and they must save the Internet from itself. If they allowed pornographers to run rampant, the innocence of America's children would be lost and the immense potential of this new medium would be squandered. From the legislative point of view, Congress must regulate the Internet to avoid these harms. Lawmakers also used this frame to reiterate the point that they must preserve the Internet for decent and tame uses that would not frighten away parents or other prospective users. In other national contexts, governments had used this diagnostic frame to safeguard economic interests and that was the case here as well. By ensuring that potentially offensive content was off limits, the government

hoped this would both spur investment in online business and make it more likely that average citizens would purchase goods on the Internet. In such instances, the "key regulatory goal" of online content standards "was business and consumer 'confidence and certainty'…'Confidence and certainty' for consumers depended upon notions of a 'safe' Internet, and this conception of safety online became central to a government strategy of promotion of the information economy" (Allen & Long, 2004, p. 232). Allowing bad actors to rule the online landscape would be "a serious deterrent to other people getting on the Internet" (CDA24 p. 2). While this economic impetus may have been part of the subtext of the regulation, both the protection of children and the protection of the Internet as a resource were the primary motivations offered to the public again and again. If Congress was going to make the Internet, "even bigger, and even better" then they must stifle the "raunchy pornography that would turn most people off" (CDA14 p. 14). Only government regulation could solve this problem which is why "Congress determined that a legislative response was necessary to ensure that the Internet would be a 'family friendly resource' that would be 'more frequently used'" (Id).

Interestingly, these diagnostic frames seem to allow more room for commentary and discussion than previous frames. In this context, it is interesting to note that supporters of the CDA were much more open to the use of research within the confines of problem definition. Where the master frame of protecting children had overridden calls for serious and critical review of the policy, here Exon and others often pointed to various studies to reinforce their point of view. This does not necessarily indicate that a critical study of the technological requirements of the CDA was forthcoming but it does at least suggest that Congress felt it needed some data or proof to bolster their argument. In

addition to the Rimm study and studies that warned of pornography's effect on children (CDA01 pp. 103-104), Congress also relied on demographic data illustrating both the volume of online activity and the prevalence of children within those numbers. Specifically, "One study presented to Congress estimated that "[o]f the 6.8 million homes with on-line accounts currently available, 35 percent have children under the age of 18" (CDA14 pp. 13-14). Again, Congress tied this figure to the diagnostic frame that vast numbers of children had access to the Internet as well as large numbers of adults who may turn away from the Internet if their children were unprotected. This data further emphasized the need for government intervention through policy and through technology.

Although these frames did not provoke any deep analysis of the technological requirements of the CDA or any critical discourse on the policy's constitutional effects, it did provide an opportunity for the introduction of research data in the debate. While the master frame of protecting children seems to have been far too ideologically charged to allow for this kind of reflection, the diagnostic frame did engage with research to support its definition of the problem. Despite the deep flaws of the Rimm study, its use did demonstrate that Exon and others were willing to appeal to a broader audience that was concerned with the objective impact the Internet could have on children. Rather than appealing to the more emotional nature of the master frame, legislators here offered more intellectual arguments and withdrew incorrect data from the debate when methodological flaws appeared. This may indicate that an opportunity exists within the context of diagnostic frames. When looking for evidence to bolster problem definition, legislators may be more inclined to reason with opponents and consider alternative points of view.

Part IV – Oppositional Diagnostic Frames

The opposition concentrated their diagnostic frames on the onerous nature of the Act's affirmative defenses, particularly the mandated use of age verification systems, ISP filtering and other technological barriers to access. Not only did these systems diminish individual autonomy by centralizing blocking decisions with service providers and other authorities, they also reduced the ability of users to decide the merit of online content for themselves by creating a national standard for what constituted "decent" material. In addition to the injury done to autonomy, these restrictions and the "good faith" use of technological mechanisms of enforcement would, the opposition argued, curtail free speech from the outset. Furthermore, content providers, especially private individuals and non-profit groups, would bear an enormous cost due to the economic realities of employing age verification and other systems. More importantly, the fear of providing minors with access to "indecent" content, even content that had political, educational, or artistic merit, would result in a reduction of that speech. While the legislative diagnostic frames focused on the harm an unregulated Internet could inflict on children, the opposition focused its problem definition on the individual and constitutional harm that the Act might inflict through the technological barriers it required.

The first diagnostic frame employed by the opposition dealt with issues of individual autonomy. While the related master frame emphasized a normative argument that policy should strive to preserve autonomy, this diagnostic frame detailed how the CDA could and would harm autonomy. Specifically, the CDA's affirmative defenses would limit choice and "weaken the privacy of all Internet users by turning systems operators into snoops and censors" (CDA09 pp. 3-4). In addition, by mandating that ISPs

take preemptive steps to block access to indecent content, this stripped away the ability of individuals to choose whether that content met their personal definition of indecency or not. By imposing a national content standard and enforcing it through regulatory systems, Congress had usurped the power of individual and community standards. As the EFF argued, "the responsibility for controlling our content lies on us - the citizens and the parents – and this is a call for all of us once again to demonstrate how we can be trusted to use this medium responsibly" (CDA08 pp. 1-2). This meant that the "parents, rather than the government" should be "empowered to make the choice about Internet content" (Id). This was a common theme employed throughout the opposition's diagnostic frame. The EFF, ACLU and others argued that the government had essentially taken on a paternalistic role, removing parents' ability to decide what content was acceptable. As will be discussed shortly, the law delegated these decisions to Internet service providers and other gatekeepers that now had a unique ability to decide for parents what was or was not acceptable.

Instead of the centralized technological controls that the Act's affirmative defenses would force on ISPs, oppositional groups argued that user-centered systems were more supportive of individual autonomy and less restrictive of constitutionally protected content. Specifically, commercial filtering software could "be tailored to reflect the parents' values and the age and maturity of the child" (CDA15 p. 8). Users could voluntarily employ these products at the point of access and this would "empower parents to exercise individual choice over what material their children could access… based on the parents' own particular tastes and values" (CDA13 p. 19). The opposition consistently pointed to existing "user-based technologies that already provide a great deal

of protection…such as Cyber Patrol, SurfWatch, CYBERsitter, and Net Nanny" that had "enabled parents and other adults to limit the access of children to material on the Internet" (CDA12 p. 13). They emphasized that products like Cyber Patrol already allowed parents, rather than the government, to "prevent access to particular sites they deem inappropriate" and to "block access to online material" (Id pp. 13-14). It is important to note that while this frame underlined the importance the opposition placed on individual autonomy, it also demonstrated a level of naiveté about commercial filtering software and overconfidence in its instrumental ability to function as a neutral tool. As Chapter 6 will describe, these assumptions about the objectivity and constitutionality of such filtering products would prove to be problematic for the opposition during negotiation of the Children's Internet Protection Act.

In addition to the damage it would do to individual autonomy, the opposition also argued that the CDA's emphasis on discrete content producers would be ineffective – especially as it related to foreign websites. One of the major weaknesses of the CDA was that it was unenforceable outside the United States and, while ISPs could proactively filter content they deemed inappropriate, foreign speakers would have no obligation to censor themselves or employ technological barriers to access such as age verification systems. The opposition argued that the only effect of the CDA would be to harm a large segment of domestic speakers while failing to protect children from sites outside U.S. borders (CDA12 p. 14). Besides, there was no guarantee that centralized ISP-level filtering would protect minors from all indecent content. On the contrary, "The evidence shows that the CDA will not protect minors from the substantial percentage of indecent or patently offensive speech that is posted abroad, whereas the user-based

methods…would block such speech regardless of where it was posted" (Id p. 4). Therefore, as the government acknowledged, ISPs "would have to rely upon" systems similar to commercial filtering technology "for foreign speakers" (Id). As the opposition argued, if filtering software was the answer anyway, why not allow individuals to decide when and if to use it?

The second diagnostic frame emphasized heavily by the opposition dealt with the reduced access to protected speech that would result from the Act. Problem definition here related directly to the limits on speech that regulatory systems required by the CDA would impose. Not only was all "indecent" content, from pornography to medical information, lumped into one category but all providers of such material, whether they were commercial entities or not, were to impose the same technological barriers to access. While for-profit sites could simply pass the cost of these systems on to the customer, private and non-profit websites would have to absorb the economic impact. This was no small matter and the opposition argued that "the administrative burden of creating and maintaining the screening system, and the ongoing costs for verification services, put this method beyond the reach of most speakers" (CDA12 p. 7). For example, one expert witness for the American Library Association estimated that the Carnegie Library would incur a cost of $30,000 just to review existing content for indecent material while the annual cost of maintenance and oversight would be $845,000 (Id). This would force websites that could not bear these costs to shut down rather than risk the criminal sanctions imposed by the CDA for failing to meet its affirmative defenses.

Also, as the opposition pointed out, it was because of these costs and the unique nature of the medium that the CDA would have such an impact on constitutionally protected speech. It was here that the government's allusions to physicality broke down. For example, the serious differences between the disembodied medium of the Internet and physical outlets meant that, not only would website operators incur a direct cost for requesting identification, but they would be unable to gauge the age of prospective viewers accurately. Even if the intent was to provide access only to adults, those running the websites could be held liable for running afoul of the CDA's standard if only one minor made it past the barrier.[13] Fear of noncompliance and the threat of being found "indecent" would prospectively chill the creation of new content. Also, the inability of non-commercial speakers even to purchase age verification software could be equally dissuasive for those who wished to speak.[14] Therefore, the very possibility that Congress would require regulatory technologies was harmful to constitutionally protected speech. Average users would be unable to meet the economic barriers to entry that the CDA created, as would many non-profit organizations that provided access to content meeting broad definitions of indecency. This was problematic for many groups ranging from Planned Parenthood to the ACLU itself. Since the "breadth of the CDA's coverage [was] wholly unprecedented…The general, undefined terms 'indecent' and 'patently offensive'

---

[13] As the Supreme Court would later find, "Given the size of the potential audience for most messages, in the absence of a viable age verification process, the sender must be charged with knowing that one or more minors will likely view it. Knowledge that, for instance, one or more members of a 100-person chat group will be minor-and therefore that it would be a crime to send the group an indecent message-would surely burden communication among adults" (CDA18 pp. 20-21).

[14] In the subsequent legal challenge, the district court's Findings of Fact would demonstrate "that as a practical matter, non-commercial organizations and even many commercial organizations using the Web would find it prohibitively expensive and burdensome to engage in the methods of age verification proposed by the government, and that even if they could attempt to age verify, there is little assurance that they could successfully filter out minors" (CDA13 p. 39).

cover large amounts of nonpornographic material with serious educational or other value" (CDA18 p. 21). Consequently, this speech would be unavailable for even those consenting adults who wished to view it. A multitude of websites would shut down if the costs of compliance exceeded their budgets (CDA13 pp. 28-29).

The technological mechanisms of enforcement required by the CDA were also far too intrusive for the opposition. In particular, the CDA only offered affirmative defenses to those website operators who had "restricted access…by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number" (CDA01 p. 97). This was a dubious proposition for several reasons. First, as a practical matter, the opposition considered this method to be "technologically infeasible" (CDA12 p. 6) even assuming credit card companies would allow non-commercial and non-profit sites to access their client records without charging a fee (CDA17 p. 23). Secondly, there was no guarantee for the government or those attempting to comply with the CDA that a minor had not used a credit card that did not belong to them (CDA13 p. 29) or that the card holder was over 18 (CDA18 p. 9). Furthermore, although the language of the CDA suggested that the policy would not have any effect on existing privacy law (CDA01 p. 102), the law's age verification requirements essentially mandated disclosure of personally identifiable information as a condition of access (CDA11 p. 2). If Congress tied the age of the user directly to credit card verification, for a myriad of reasons individuals might not wish to disclose their online habits to a private entity such as a credit card company. Also, as the opposition pointed out, prior to passage of the CDA existing age verification services were employed almost exclusively by pornographic websites and these systems not only required proof of age through a credit card number

but also a more thorough registration process. Even a government expert on this technology acknowledged that he would not care to be associated with such a service nor could he guarantee that "those systems protected the privacy of registrants" and did not sell those lists to others (CDA17 pp. 23-24).

This provision also assumed that all those consenting adults who wished to view "indecent" material actually possessed a credit card. In the absence of this sort of identification, the CDA "would completely bar adults who do not have a credit card and lack the resources to obtain one from accessing any blocked material" (CDA18 p. 9). The law forced websites that hosted any content considered even mildly distasteful to employ age verification systems (assuming they could afford the technology). These systems forced users to decide whether or not to disclose personal information and credit card data to websites or to anonymous third-party verification services (assuming they had a credit card). As mentioned previously, this could have a deterrent effect on the website operator either indirectly through the economic burden associated with these systems or directly through their decision to create and distribute any such content in the first place. The user was equally constrained and the system either barred access from content at the outset due to lack of a credit card or the user would choose not to proceed past the locked gate of the website for fear of personal indictment (CDA13 pp. 29-30). In this sense, the age verification technologies required by the CDA were clearly not neutral tools and had the potential for negative impact on constitutionally protected speech. The opposition's diagnostic frame here made it quite clear "that requiring such screening for any messages that might be 'indecent' or 'patently offensive' for a minor would have the effect of banning such messages from these types of online communication" (CDA12 p.

6). Ironically, the opposition noted that the websites of online pornographers would be among the few that already had the means to comply with the CDA and the customer base willing to supply age verification and credit card information (CDA13 p. 65). The websites of libraries and other non-commercial entities would bear the brunt of the Act for fear of posting "lawful but arguably 'indecent' words and images for artistic, political, or instructional purposes" (CDA17 p. 25).

Even more threatening to this diagnostic frame was the unprecedented technological control that the CDA would delegate to carriers and Internet service providers. Through the use of filtering, screening, and blocking technologies, the Act granted stunning police powers to commercial entities without the benefit of constitutional oversight or judicial review. In the interest of protecting children at all costs, the CDA essentially encouraged ISPs and other good faith actors to disallow access to any content considered even mildly questionable. The "Good Samaritan" provision of the CDA expanded the affirmative defense for service providers and made them immune from liability "for any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, *whether or not such material is constitutionally protected*" (CDA01 p. 101, emphasis added). Despite Exon's and other legislative protestations that the law would "not ban any constitutionally protected material from adults" (CDA06 p. 1), the opposition argued that the CDA had the direct effect of minimizing the availability of speech whether it was constitutional or not. Not only did the Act allow service providers to throw aside constitutional considerations, they were essentially unable to do anything less for fear of criminal

liability (CDA08a p. 4).[15] The threat of prosecution for industry stakeholders was of concern for several reasons. First, the fear of providing even remotely indecent content to minors would be a public relations disaster and could have serious consequences for future market share (CDA13 p. 41). Second, if ISPs were not overly cautious about what content they allowed through, they could find themselves subject to a government lawsuit. The prospect of preparing a criminal defense and the associated costs were, at the very least, unattractive and, at most, financially debilitating. It was extremely unlikely that any provider would "willingly subject itself to prosecution for a miscalculation of the prevalent community standards or for an error in judgment as to what is indecent" (Id).

All of this encouraged service providers to deploy the most thorough technological mechanisms at their disposal. Since there were no disincentives from blocking a wide range of speech and because Congress so broadly defined the nature of "indecency", the Act might disallow whole swaths of potentially protected speech. As the opposition argued, it was difficult to imagine a technological and "criminal standard that provides less guidance, or to conceive of a speech prohibition that would have a broader chilling effect" (CDA17 p. 18). From this point of view, blocking, filtering and age verification technologies were not simply the neutral "enabling tools" that Exon and others in Congress had suggested (CDA01 p. 102). These technologies had a direct and drastic impact on the most basic constitutional rights of speaking and listening –

[15] It is interesting to note that, in the years since passage of this provision, it has been used as a defense *against* blocking sexually explicit content in the name of protecting minors. For example, in *Doe v. MySpace* (528 F.3d 413 - 5th Cir. 2008), the court upheld MySpace's immunity even though the site did not require age verification or implement other policies to protect children.

especially in the vast communicative medium the opposition considered the Internet to be. Therefore, these enforcement systems ceased to be instrumentally useful objects and became active mechanisms for dictating what speech was allowable within the government's new national content standard. As the opposition emphasized, this broad imposition of a regulatory standard for speech was essentially a hegemonic means for controlling discourse. Any policy or technological system "that stifles speech on account of its message, or that requires the utterance of a particular message favored by the Government, contravenes this essential right [of free speech]. Laws of this sort pose the inherent risk that the Government seeks not to advance a legitimate regulatory goal, but to suppress unpopular ideas or information or manipulate the public debate through coercion rather than persuasion" (CDA13 pp. 67-68). This is strongly reminiscent of Pfaffenberger's warnings about any hegemonic technologies that are "specifically designed to exercise force, that is, to coerce obedience and suppress deviance" (1992, p. 283).

The opposition's diagnostic frames again echo this dissertation's theoretical framework related to user empowerment and the protection of democratic rights. In addition to warnings about hegemonic technologies similar to those made by Pfaffenberger, the opposition also stressed the need for systems that empowered users. Voluntary use of technologies like commercial filtering products would, the opposition argued, be immensely preferable to centralized systems that removed the individual's ability to choose. This mirrors Lewis Mumford's calls for fewer "authoritarian" and "system-centered" technologies and more "democratic" or "man-centered" mechanisms (Mumford, 1964 p. 2). This is also strongly reminiscent of Richard Sclove's normative

assertion that "Democratic societies should seek a balanced mixture of communitarian/cooperative, individualized, and transcommunity technologies, while avoiding technologies that establish authoritarian social relations" (Sclove, 1995, p. 62).

The opposition made a strong connection between these centralized technologies and a diminished ability to exercise constitutional rights. Specifically, use of these centralized, state-mandated technologies would do harm to the democratic rights envisioned by Mumford that included "communal self-government, *free communication as between equals, unimpeded access to the common store of knowledge*, *protection against arbitrary external controls*, and a sense of individual moral responsibility for behavior that affects the whole community" (Mumford, 1964, p. 1, emphasis added). Opponents of the CDA consistently argued that the Internet was unique because there "is no central control" and the "user can determine and control what data the user will be exposed to…The user does not need a paternalistic government determining what is appropriate to view" (CDA02 pp. 30-31). The opposition, within its diagnostic frames, provided a serious critique of the CDA and its technological mechanisms of enforcement. Since the regulatory systems required by the CDA would reduce individual choice, place an economic burden on speakers and listeners, chill the creation of protected speech, and criminalize speech that might have serious literary, political, scientific, or artistic value it was an illegitimate exercise of state control. Furthermore, the opposition stressed that Congress should not use these systems to delegate veto power over content to ISPs without some form of constitutional oversight or judicial review. The ACLU, EFF, CDT, and others argued again and again that there "are constitutional ways to protect children from cyberporn but not restrict the freedom of speech" (CDA08d pp. 12-13).

Part V – Legislative Prognostic Frames

For legislative supporters of the CDA, technology was the only possible solution to the problems they had defined. If children were to remain unharmed by the prevalence of pornography online and the potential of the Internet as a commercial and informational tool was to remain undiminished, the government must act and must employ technologies that precluded both. In fact, the lack of a legislative response would be detrimental because, "if the Government were to do nothing to prevent children's access to online pornography, this abandonment would itself contribute to the harm about which the Government has a compelling interest" (CDA16 p. 22). As Senator Grassley emphasized, within any solution "there is a role for technology and government" and there was "a very definite need for the involvement of government and not putting the total responsibility on parents at this point" (CDA26 p. 50). The legislative prognostic frames consistently referred to the government's compelling interest in solving the problems it had identified and made clear that the technologies mandated by the CDA were the only means to do so.

Within its prognostic frames, Congressional supporters of the Act also emphasized that user-based systems and other commercial blocking technologies were inadequate. In fact, because they were voluntary they would fail to curb kids' access to indecent content. This argument directly contradicts the opposition's theme of user empowerment and individual autonomy. For Exon and others, it was precisely because these commercial systems left the decisions about what, when and if to filter to parents that they were insufficient to address the blight of sexually explicit material online. As supporters of the CDA made quite clear, "Congress has an independent interest in

protecting children from exposure to or receipt of patently offensive sexual or excretory depictions, and is not required and should not be compelled to rely on private, voluntary actions of others, such as parents, but can encourage their assistance" (CDA16 p. 23). Congress simply could not and would not trust parents to exercise good judgment in this regard. The technological means to accomplish the state's interests would be effective because they were "legislative in nature, and therefore mandatory – never voluntary…ad-hoc ways for private individuals to address the problems in which Government has a compelling interest are inapposite to the means by which Government may attempt to promote its compelling interest" (Id p. 22).

Congress specifically aimed this facet of the prognostic frame at the suggestion that commercial filtering products could ever be as effective or as pervasive as the government's preferred technological mechanisms of enforcement. While voluntary filters could be part of the solution, they were not reliable enough for supporters of the CDA to depend upon. These supporters made repeated allegations that these products were insufficient compared to government intervention because they were grossly ineffective. Specifically, they suggested that "filename-based Cybersitter does not block cryptic titles, word-based Net Nanny does not block pornographic images, and Surfwatch does not work on non-Internet sources, such as BBSs" (CDA16 p. 23). While the government did not entirely dismiss either "parental involvement in their children's use of the Internet" or the "installation of filtering software," it was clear that neither was an adequate solution (CDA16 p. 24). Instead, Exon and his supporters argued that these measures "should be regarded as complements to the CDA" but neither one, "individually or in the aggregate, eliminates the need for legal prohibition…or supplants

Congress' constitutional authority to take action in furtherance of its compelling interest" (Id).

Congress was determined to take action and ignored oppositional calls for user empowerment. Individual autonomy was not a mitigating factor when America's children and the Internet itself were at risk. The solution must be a centralized, governmental effort and lawmakers could not leave so important a struggle to parents, communities, or the voluntary use of filtering products. It was inconceivable that the state would trust in the "hope that parents will purchase and install blocking software in the family computer…To the contrary, Congress has a compelling interest to affirmatively protect children so that they may participate in this new and extraordinary medium, especially where private actors fail to use even the blocking and screening methods at their disposal to protect children from the domestic and foreign pornography that is available online" (Id p. 21). While Congress encouraged parents and communities to "make use of whatever software products are available" legislators were sadly confident that "not all parents will purchase such software, and, even if they do, children have access to many computers which will not employ software filtering devices such as in schools, libraries, and neighbors' homes" (Id p. 23). Besides, even if filters were in place, it was important to remember that kids were America's computer experts and "many children are capable of out-maneuvering such technology" (Id). It was clear that, within the legislative prognostic frame, any solution to the dire problems they had recognized could only come through government action and through the use of centralized, state-sanctioned regulatory systems. Only federal law and the mandated use

of such systems would be sufficient in achieving the government's compelling interest in protecting children.

In addition to age-verification technologies and the "Good Samaritan" blocking performed at the ISP level, the Act's supporters suggested several other technological solutions within their prognostic frame. One of the first solutions proposed, and one that made a great deal of sense both from legislative experience and from the example of Motion Picture Association, was the idea of rating system. Although ratings eventually became less promising from a legislative point of view, at the outset of the debate over the CDA ratings seemed quite promising. In fact, policy directives from the Clinton administration had tied rating systems directly to voluntary, user-centered solutions. Specifically, the administration sought to "promote the use of industry ...self-regulation and rating systems, and technical solutions to empower parents and other users to resolve contentious access issues (e.g., children's access, and violence)" (CDA05 p. 3). As mentioned above, supporters of the CDA eventually found these suggestions too weak a response but, for a time, this seemed to be a feasible answer. Also from the beginning, lawmakers directly tied rating systems to technological responses to the problem of online indecency. There was precedent for this type of response and, from a legislative perspective, it was not unreasonable to suggest that the government could "develop a solution for the Internet that is as powerful for the computer as the v-chip will be for television…With the right technology and ratings systems – we can help ensure that our children don't end up in the red light districts of cyberspace" (CDA08a p. 4). Interestingly (and a bit incongruously), supporters of the CDA eventually dismissed a rating system as an inappropriate solution because it was not widespread enough to

guarantee that all material would be labeled suitably and would consequently force parents to be too restrictive of their children's Internet access (CDA14 pp. 31-32).

Briefly, two other potential technological solutions suggested by Congress were to add tags to all adult-themed content on the Internet and to make use of Common Gateway Interface (CGI) scripts to constrain access to such content only to those 18 and older. First, it seemed a "technologically feasible," even "trivial" matter to embed tags denoting adult content either directly in a site's URL or less obviously in the HTML code (CDA13 p. 30). This tagging method would essentially require content providers to label all indecent content by including "a string of characters, such as 'XXX'" that would then be recognized by the user's computer to "screen out any content with that tag" (Id).

CGI script, as explained by CDA advocates, was "technology by which an operator of a World Wide Web server may interrogate a user of a Web site" (CDA13 p. 27). Based on the information obtained from the user, the server could then "grant or deny access to the information sought" (Id). CGI script was, essentially, the means by which a site could "screen visitors by requesting a credit card number or adult password" (Id). Content providers could use these methods in conjunction with the age verification services that websites could employ to qualify for the Act's affirmative defenses. CGI script was particularly useful for content distributed via Usenet feeds "where much of the most graphic and notorious pornography is made available, both hard- and soft-core, normal and perverted, actual and simulated" (CDA16 p. 26). Alternatively, because Usenet feeds must be affirmatively selected in order to be carried by any particular ISP, the service provider could also simply choose not to offer access to any feed that ran afoul of the content standard (CDA16 p. 26). Conveniently, due to the nature of the

"Good Samaritan" blocking provisions of the CDA, no court could find an ISP liable for blocking access to constitutionally protected speech.

All of these prognostic frames for addressing the harms caused by an unregulated Internet emphasized the state's need to act to achieve its compelling interest. Considerations of individual autonomy were insufficient to change the legislative course that Exon and others had set. Although some members of Congress proffered an array of existing and as yet undeveloped technologies as the only appropriate solution (CDA16 p. 25), legislative supporters of the CDA did not demonstrate that they placed much faith in voluntary methods for filtering content. Some legislators actively eschewed the ideal of user empowerment and the government made clear that, while individuals and parents could be part of the solution, they would never be as reliable as government intervention through policy and through technology. This rhetorical strategy deemphasizing parental autonomy and choice was vastly removed from even the Congressional findings that predated the CDA. At the outset of the debate, Congress advocated for "technology that would give [parents] greater control to block" indecent content (CDA01 pp. 103-104). From the beginning, the compelling government interest was not in centralizing control or delegating blocking decisions to service providers but instead there was "a compelling governmental interest in empowering parents to limit the negative influences of [content] that is harmful to children" (Id). Congress intended Section 230 of the Act to "encourage the development of technologies which maximize user control" and "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents" (CDA21 p. 86). Despite these initial suggestions to the contrary, the legislative prognostic frames consistently minimized user empowerment.

Part VI - Oppositional Prognostic Frames

The opposition's prognostic frames suggested that the only sensible solutions to the problems caused by the CDA were to: 1.) minimize or remove the access controls required by the Act; 2.) revise the policy to make accommodations for individual autonomy and protected speech or; 3.) to simply strike the policy down as unconstitutional. Since the diagnostic frames employed by opponents of the CDA emphasized the harms inflicted by the Act's technological mandate, their proposed solutions focused on how Congress should reconsider those technologies or eliminate them altogether. In lieu of such modifications to the policy, the Act remained "a government-imposed content-based restriction on speech" (CDA13 p. 36). Without serious revisions, the opposition argued, the policy's requirements were "either technologically impossible or economically prohibitive for many…to comply with the CDA without seriously impeding their posting of online material which adults have a constitutional right to access" (Id p. 39). As it stood, the CDA was "a hastily drafted statute…that fails to take account of the unique nature of the Internet and obviously sweeps far more broadly than the First Amendment permits" (CDA12 p. 5). Without radical amendment, the only "appropriate response" to the CDA was "to strike down this statute and give Congress the opportunity to make those policy choices itself" (Id). Such a drastic reassessment of the policy was necessary because the CDA's technical provisions were "in serious conflict with our most cherished protection – the right to choose the material to which we would have access" (CDA13 p. 43). If Congress implemented the Act without critical analysis and reassessment, the CDA would,

"without doubt, undermine the substantive, speech-enhancing benefits that have flowed from the Internet" (Id pp. 64-65).

The opposition again tied the need for reconsideration of the Act's technological mechanisms of enforcement to Congress' basic misunderstanding of these systems and their misportrayal of how they would function in application. The use of content tagging, for example, was problematic to the opposition for several reasons. First, from a practical standpoint, there was no "consensus among speakers…to use the same tag to label 'indecent' material" (CDA15 p. 8). Although Congress could have conceivably mandated some uniform tag for indecent content, there was no reason to believe that the contextual standards for indecency would be consistent across individuals or communities. Misunderstandings about what constituted decency in a global medium would make this proposal extremely difficult to implement. Also, the effort required to label all indecent content proactively would be difficult at best. Accurately tagging all content "would be extremely burdensome for organizations that provide large amounts of material" such as libraries or other informational outlets (Id).

Additionally, no precedent or model for content tagging existed and, therefore, provided no guidance whatsoever to those individuals or ISPs who would be required to use tags as a part of their affirmative defense under the law. Without any clear guidelines, "the government's proposal that 'tagging' or self-rating might provide a defense is 'purely hypothetical and offers no currently operative defense to Internet content providers'" (CDA15 p. 11). The legislative suggestion that tagging would prove to be effective and that it would provide a clear, good-faith defense, was contested by the opposition who argued that this provision inaccurately described the state of the

technology. While the government hinted that "some sort of 'speaker tagging' system might constitute a safe-harbor defense at some point in the future… it has pointedly refused to specify" that tagging would qualify as a defense when Congress passed the Act (CDA12 p. 8). Therefore, "the Government's effort to defend the CDA by pointing to the mere possibility that speaker tagging 'might' provide a defense is wholly unpersuasive" (Id p. 11).

Finally, the very act of tagging speech was constitutionally problematic. Particularly where the labeled speech may have been on the borderline of "indecency" as defined by the state, tagging that speech became a political act mandated by the technological requirements of the CDA. This reemphasizes the opposition's argument that the regulatory systems required by the Act amounted to a hegemonic form of control. Within this scheme, the government essentially approved certain content and would tag anything falling outside that zone of acceptability accordingly. From this point of view, "Any de jure or de facto requirement that speakers label their own protected speech 'patently offensive' would amount to a pernicious form of governmentally compelled speech. The Government generally cannot compel citizens to speak, particularly if the speaker is compelled to attach a pejorative label the speaker does not believe is warranted" (CDA12 p. 10). From the opposition's point of view, lawmakers had to revise this provision to account more realistically for the non-neutral and political nature of tagging technology or they should excise it from the CDA entirely.

CGI scripts were equally impractical and required serious reconsideration or, failing that, removal from the Act. This was especially true for those who made use of the large service providers that dominated the market for private Internet access at the

time. Specifically, "Content providers who publish on the World Wide Web via one of the large commercial online services, such as America Online or CompuServe, could not use an online age verification system that requires cgi script because the server software of these online services available to subscribers cannot process cgi scripts. There is no method currently available for Web page publishers who lack access to cgi scripts to screen recipients online for age" (CDA13 p. 28). In the mid-1990s, there were roughly 12 million Internet users who depended on these services (CDA17 p. 23). Without access to CGI scripts, this provision would force any "speakers who wished to screen for age…to establish their own independent Web sites with cgi script capability, which takes time and costs money" (Id). Although inexpensive websites have become the norm since that time and have further democratized the ability to distribute speech, this was not the case some twenty years ago. These economic barriers to the use of CGI scripts would be dissuasive and "non-commercial organizations and even many commercial organizations using the Web would find it prohibitively expensive and burdensome to engage in the methods of age verification proposed by the government" (CDA13 p. 39). Furthermore, the government's representation that ISPs could make use of CGI scripts to manage access to various Usenet groups was also disingenuous. Although it was true that ISPs could use CGI technology to screen access to Usenet groups, they had no incentive to employ this expensive method if the Act's "Good Samaritan" defenses immunized them from blocking access to a multitude of such groups proactively.

Despite these criticisms of tagging, CGI and the age verification technologies described in Part IV, the opposition itself offered as part of their proposed solution a technological fix (CDA02 p. 34). This prognostic frame may have been indicative of an

instrumentalist understanding of technology similar to that demonstrated by Exon and other supporters of the CDA. Specifically, the ACLU, EFF, CDT, and a number of concerned industry stakeholders suggested that a viable alternative to the regulatory systems required by the Act would be the development of the Platform for Internet Content Selection (PICS). Proposed by the World Wide Web consortium (W3C), an international body that sets standards for the Internet, PICS was meant to be a technological means for limiting government regulation of content on the Internet. In direct response to Senator Exon's efforts "a group of companies quickly came to the consortium asking to do something now, because they knew Congress had plans to draw legislation very soon that would be harmful to the Internet" (Berners-Lee, 1999, p. 113). These industry stakeholders, as "members of the W3C realized that without an industry solution, the government would regulate the industry" (governingwithcode.com, 2004).

Oppositional groups embraced this potential solution based on the belief that, similar to the voluntary use of filtering software, PICS "would support parents' ability to filter and screen material that their children see on the Web" (CDA13 pp. 16-17). PICS technology would "provide the ability for third parties, as well as individual content providers, to rate content on the Internet" and when "fully implemented, PICS-compatible World Wide Web browsers, Usenet News Group readers, and other Internet applications, will provide parents the ability to choose from a variety of rating services, or a combination of services" (Id). Despite their enthusiasm for such an apparently user-centered system, these groups were vague about how third party rating services would function more fairly than centralized government solutions or be more accommodating of protected speech. In fact, referring to PICS as "a neutral content-classification scheme"

(CDA08f p. 20), the opposition demonstrated a misunderstanding of the political nature of these systems and the bias that could be embedded within them.

For the most part, the oppositional prognostic frames offered a crippling critique of the regulatory systems proposed by the state. This critique raised serious doubts about the ability of these technologies to function efficiently and constitutionally. Furthermore, although Congress had made its case against autonomy, the opposition argued that any solution to the problems caused by the Act's affirmative defenses must include some form of user empowerment. As the EFF made clear, without some acknowledgment of this and without more rigid safeguards for protected speech, the "CDA was a wholly inappropriate exercise of governmental power under the Constitution" and "would have abridged one of the freedoms…that is central to any democratic society" (CDA08c p. 10). Similar to the theoretical framework outlined in Chapter 2, the opposition made an argument emphasizing that "all government policies involving technology need to be reevaluated from the standpoint of their implications for achieving a more democratic technological order" (Sclove, 1995, p. 224). The opposition's critique of age verification systems, tagging technology, CGI scripts, and ISP blocking all demonstrate this deeper concern for achieving more democratic outcomes. For the opposition, the CDA was so flawed that, at a minimum, the solution required serious reconsideration and, at most, "the Act should be struck down on its face on overbreadth grounds" (CDA12 p. 21). The opposition had invoked frames and raised fundamental concerns that only a different forum could address. The judiciary would make the final determination on the validity, constitutionality, and "resonance" of these competing frames.

Part VII – Judicial Opinion

To say that the opposition wasted no time in filing its legal challenge to the CDA would be an understatement. The ACLU served its complaint just hours after the President signed the Act into law (CDA27 p. 1) and reiterated all of the arguments that this chapter has already described. Filing in the Eastern District of Pennsylvania, the ACLU and nineteen other plaintiffs[16] sought declaratory and injunctive relief to ensure that the government would not enforce the Act before it had its day in court (CDA11 p. 1). From the outset, the panel of three federal judges appointed to this case ordered that a basic but serious review of the technologies at issue be undertaken. In a lengthy Findings of Fact, the court took a great deal of care to describe the nature of this new medium, the circumstances leading to its creation and the development of that medium since its inception (CDA13 p. 6). The court acknowledged that, "in order to apprehend the legal questions at issue in these cases, it is necessary to have a clear understanding of the exponentially growing, worldwide medium that is the Internet, which presents unique issues relating to the application of First Amendment jurisprudence" (Id).

The Findings of Fact did not bode well for the government. The first of the Congressional frames to sustain damage was the metaphorical commitment that Exon and others had made to the similarities between access controls and physical restrictions. The court made it clear that the "Internet is not a physical or tangible entity" but was instead a "giant network" which had no clear precedent (CDA13 p. 6). This would foreshadow the

[16] The plaintiffs in this case represented a variety of different stakeholders with a multitude of interests. These plaintiffs encompassed not only activist organizations such as the ACLU, EFF and Electronic Privacy Information Center but also individual content producers, publishers, journalists, computer professionals and sexual health/education outlets such as the Aids Education Global Information System and Planned Parenthood (CDA11 p. 1).

court's view on the government's position that Internet content could be "zoned" in a form legally analogous to porn shops and theaters. The court also reasoned that the Internet's intangible nature and its existence as "a decentralized, global medium of communications" (CDA13 p. 7) belied the state's ability to control access from a centralized point. In fact, the Internet, "From its inception…was designed to be a decentralized, self-maintaining series" of networks that functioned best "without direct human involvement or control" (Id). Furthermore, because "There is no centralized storage location, control point, or communications channel for the Internet…it would not be technically feasible for a single entity to control all of the information conveyed on the Internet (Id p. 8). Even before the court had debated the merits of either side's argument, it had concluded that it would be neither practical nor desirable for the government to impose technological barriers to access.

The court also provided a lengthy analysis of the comparison the government had drawn between Internet content and broadcast regulations. Although supporters of the CDA had insisted that "the Net is still closer to broadcasting than to print" (CDA08f p. 25), the court remained unconvinced. In their view, broadcasting was vastly different from the realities of the Internet because it was neither invasive nor controlled by a centralized authority (see footnote 5). Instead, the court found that online communication, "while unique, is more akin to telephone communication…than to broadcasting" (CDA13 p. 36). This was important because it directly contradicted the government's assertion that the Internet was a pervasive medium that would expose children to indecent content consistently and involuntarily. Instead, in vindication of the opposition's argument that indecent material must be sought out and the "user [was] not

likely to stumble upon the offensive" (CDA02 pp. 30-31), the court agreed that "an Internet user must act affirmatively and deliberately to retrieve specific information online" (CDA13 p. 36). This struck at the heart of the government's diagnostic frame that unregulated access to the Internet would irreparably harm children. By making this argument, the court had crippled one of the government's key justifications for technological regulation and against user autonomy. Based on the Findings of Fact, the court was confident that the danger to children was nowhere near as dire as Exon and others had suggested and "Even if a broad search will, on occasion, retrieve unwanted materials, the user virtually always receives some warning of its content, significantly reducing the element of surprise or 'assault' involved in broadcasting. Therefore, it is highly unlikely that a very young child will be randomly 'surfing' the Web and come across 'indecent' or 'patently offensive' material" (Id).[17] This emphasized individual agency and personal accountability. Instead of relying on state intervention to determine the acceptability of content, the court suggested that the user had the autonomy to choose whether to take the "affirmative steps" necessary to access adult content (CDA13 p. 26) or not. Even children required a degree of "sophistication and some ability to read to retrieve material and thereby to use the Internet unattended" (Id). Internet content did not "invade" the home or "appear on one's computer screen unbidden" and the user would "seldom encounter content 'by accident'" (Id). As the court pointed out, even the

[17] This line of reasoning also undercut the government's reliance on the precedent set in *FCC v. Pacifica Foundation*, 438 U.S. 726 (1978). Where the *Pacifica* court had found that broadcasting should merit more stringent regulation because of the "uniquely pervasive presence that medium of expression occupies in the lives of our people," the court here deliberately portrayed the Internet as a medium accessed by choice.

government's witness had admitted the "odds are slim" that any user would encounter such material without actively seeking it out (Id).

The court's lack of faith in the government's arguments extended to the use of CGI scripts and tagging. The court concurred with the opposition that customers of America Online, CompuServe and other large providers would not have access to this technology and thus could not employ it as an affirmative defense (CDA13 p. 28). Without CGI scripts, these millions of users would have no confidence that potentially indecent content had been completely screened from minors. Therefore, the Act would dissuade providers of even mildly offensive content from speaking in the first place. Tagging would be equally prohibitive and the government had failed to establish that such technology would be either feasible or effective in keeping children away from "indecent" content (CDA13 p. 30). In fact, such a provision would "require all content providers that post arguably 'indecent' material to review all of their online content, a task that would be extremely burdensome for organizations that provide large amounts of material online which cannot afford to pay a large staff to review all of that material" (CDA13 p. 30). Not only would the prospect of such a massive effort dissuade a number of content providers from speaking but, if put into effect, tagging could force kids away from perfectly acceptable speech. Specifically, in "lieu of reviewing each file individually, a content provider could tag its entire site but this would prevent minors from accessing much material that is not 'indecent' under the CDA" (Id).

Next, the court tackled the primary technological mechanism of enforcement outlined in the CDA's affirmative defenses, namely age verification systems. After confirming the opposition's assessment that any "credit card requirement would

completely bar adults who do not have a credit card…from accessing any blocked material" (CDA13 p. 29), the judges then provided an analysis of the effectiveness such technology would have in accomplishing the state's compelling interest in protecting children. Like the opposition, the court found that the age verification systems mandated by the law would not function as the government had suggested and, thus, there was no way for individual content providers to ensure that they qualified for this good faith defense under the Act. In fact, the court found that "no current technology could give a speaker assurance that only adults were" accessing certain content (CDA13 pp. 26-27). Furthermore, the court noted that, even if such systems were put in place, the government had "presented no testimony as to how such systems could ensure that the user of the password or credit card is in fact over 18" (CDA13 p. 30).

Furthermore, because many of the age verification systems advocated by the government relied on credit card numbers as a proxy for age, the court addressed the practicality of such systems. They found without exception that "verification of a credit card number over the Internet is not now technically possible" (CDA13 p. 28). In fact, large credit card companies such as Visa and MasterCard did not consider "the Internet to be sufficiently secure under the current technology to process transactions in that manner" (Id). The court acknowledged that commercial transactions were taking place online at the time but only because "the seller must then process the transaction with Visa or Mastercard off-line using phone lines in the traditional way" (Id). Although both companies were conducting feasibility testing for a technology that would eventually become routine, at the time of the decision, "credit card verification is effectively

unavailable to a substantial number of Internet content providers as a potential defense to the CDA" (CDA13 p. 29).

Even assuming that such credit check systems would be widely available in the very near future, the court agreed that they "will remain economically and practically unavailable for many of the non-commercial plaintiffs in these actions" (CDA13 p. 28). Credit card companies and age verification firms did not provide their services for free and the government's own expert witness on this issue had testified it was likely that existing "verification agencies would decline to process a card unless it accompanied a commercial transaction" (Id). Although commercial websites could potentially absorb the cost of verification, the court found that "Using credit card possession as a surrogate for age, and requiring the use of a credit card to enter a site, would impose a significant economic cost on non-commercial entities" (Id). This would force the educational, activist and informational groups who comprised the plaintiffs to "incur a monthly cost far beyond [their] modest resources" and such organizations would "regard charging listeners to access their speech as contrary to their goals of making their materials available to a wide audience free of charge" (Id pp. 28-29). Therefore, the court argued that the CDA would have the unintended effect of making it financially impossible for some who wished to speak to do so. This was in direct contradiction to the court's portrayal of the nature and purpose of the Internet.

Imposing an artificial barrier to access would also negate the advantages inherent in the medium in the court's view. What good was the Internet if a series of gatekeepers made the act of information seeking a lengthy and hostile inconvenience? By mandating such a technological verification system, the Act would "significantly delay the retrieval

of information on the Internet" (CDA13 p. 29) and frustrate access to protected content in the process. The court relied on testimony from both sides on this point. The government's witness admitted that even "a minute is absolutely unreasonable" and users "will not put up with a minute" waiting for credit card verification (Id). Plaintiffs' expert agreed that individuals would not tolerate such interruptions and that "excessive delay disrupts the 'flow' on the Internet and stifles both 'hedonistic' and 'goal-directed' browsing" (Id). From the outset, the court had noted the speed of the Internet as one of its unique attributes commenting that online "communications can occur almost instantaneously" (CDA13 p. 7). The court did not wish to see this distinct advantage of the medium sacrificed and did not agree that the technologies mandated by the Act were the only means available for accomplishing the state's compelling interest.

The court was also critical of the government for its apparent lack of analysis of age verification technology. This relates directly to the oppositional calls for more substantive study. Perhaps because the court had gone to such lengths to establish its Findings of Fact about the nature of the medium, all three judges were displeased at the government's failure to undertake a similar effort. The court chided the government for offering "very limited evidence regarding the operation of existing age verification systems" and, when lawmakers did offer such evidence, it "was not based on personal knowledge [of the witness]" (CDA13 p. 29). They scolded this government witness for admitting "that his knowledge of these services was derived primarily from reading the advertisements on their Web pages" and because he "had not interviewed any employees of these entities, had not personally used these systems, had no idea how many people are registered with them, and could not testify to the reliability of their attempt at age

verification" (CDA13 p. 29). Such a glaring lack of critical review was, in the court's opinion, a blemish on the government's entire argument.

Finally, the court addressed the opposition's arguments regarding the effect the Act and its technological mechanisms of enforcement would have on constitutionally protected speech. The judges overwhelming adopted the position that the CDA would harm the ability of both the speaker and the listener to communicate effectively in this new medium (CDA13 p. 39). These regulatory systems would function not only as disincentives to speech but also as active criminal deterrents. As the court made clear, "this is not a case in which we are dealing with a mere incidental inhibition on speech…but with a regulation that directly penalizes speech" (CDA13 p. 35). In a direct reference to the opposition's diagnostic frame that the CDA and its technological mandate would wreak havoc on the ability to speak without fear of reprisal, the court noted that "Subjecting speakers to criminal penalties for speech that is constitutionally protected in itself raises the spectre of irreparable harm" (Id). Furthermore, because the technological systems necessary to qualify for the Act's affirmative defenses were "effectively unavailable for non-commercial, not-for-profit entities" those "speakers who display arguably indecent content on the Internet must choose between silence and the risk of prosecution" (CDA13 p. 32). These technological requirements, "if not enjoined, will have a chilling effect on [plaintiffs'] free expression" (CDA13 p. 35). The court also directly rejected the CDA's diagnostic frame stating that "the Government's asserted 'failure' of the Internet rests on the implicit premise that too much speech occurs in that medium, and that speech there is too available to the participants. This is exactly the benefit of Internet communication, however. The Government, therefore, implicitly asks

this court to limit both the amount of speech on the Internet and the availability of that speech. This argument is profoundly repugnant to First Amendment principles" (CDA13 p. 68).

In a ringing endorsement of the opposition's case, the District Court found that "the Internet may fairly be regarded as a never-ending worldwide conversation. The Government may not, through the CDA, interrupt that conversation. As the most participatory form of mass speech yet developed, the Internet deserves the highest protection from governmental intrusion" (CDA13 p. 70). During the inevitable appeal, the Supreme Court would go on to validate this decision and emphasized several important points made by both the District Court and the opposition. The Supreme Court would provide constitutional validation for these arguments and, by inference, for the theoretical framework described throughout this dissertation.

First, the Supreme Court upheld the idea that user empowerment should not be sacrificed through passage of the CDA. The Court here emphasized the right of parents to make choices for themselves and for their children without the heavy hand of government regulation. The provisions of the Act and its technological requirements were, in the Court's opinion, an illegitimate means for removing deeply personal decisions from individual families and delegating that power to the state. Specifically, the CDA did "not allow parents to consent to their children's use of restricted materials" even if the parent believed their child could and should have access (CDA18 p. 2). While the Court acknowledged the "State's independent interest in the well-being of its youth," that interest could not be used to usurp "the parents' claim to authority in their own household to direct the rearing of their children" (Id pp. 13-14). This parental authority,

and the individual autonomy it represented, was not only necessary but "basic in the structure of our society" (Id). In the Court's view, no government interest was so compelling that it could supplant the ideal of parental empowerment.

The Court would also remain unconvinced of the government's argument that its interest in protecting the nascent "educational and informational" (CDA01 p. 100) resource the Internet might become was so compelling that it trumped any other considerations (CDA18 p. 4). In fact, the evidence did not support the government's fear that the plague of indecent material on the Internet would drive away prospective users. This struck directly at the legislative diagnostic frame arguing that unregulated access would harm the Internet's potential. The Court found it wholly "unpersuasive" that "the unregulated availability of 'indecent' and 'patently offensive' material is driving people away from the Internet" (Id). On the contrary, the Court believed that the "dramatic expansion of this new forum contradict[ed] the factual basis underlying this contention" (Id) and the "record demonstrates that the growth of the Internet has been and continues to be phenomenal" (CDA18 p. 26).[18]

Next, the Supreme Court expanded on the idea that "cyberzoning" was an incorrect metaphorical extension of legal and regulatory precedent. The Court made important distinctions between the physicality of traditional zoning laws and the global nature of this new medium. Although laws could target the effects of zoning at distinct pornographic bookstores or theaters and would not inhibit the exercise of free speech

[18] "By mid-1995, there were more than 50 to 70,000 computer bulletin board ("BBS") systems operating in the United States…This growth was accompanied by the emergence of online services such as America Online, Prodigy, CompuServe, Delphi, GEnie and Apple Computer's e-World. These services, now [host] approximately 7 million subscribers" (CDA26 p. 23).

outside of those zones, the effect of the CDA would be anything but local. On the contrary, because "the CDA applies broadly to the entire universe of cyberspace" (CDA18 p. 15) it would preclude a great deal of adult speech in the name of protecting minors. In the Court's opinion, the CDA was more "akin to a law that makes it a crime for a bookstore owner to sell pornographic magazines to anyone once a minor enters the store" (CDA18 p. 31). The Court had made a clear distinction between the government's metaphors of physicality and the intangible nature of the Internet. While such zoning laws "might be constitutional in the physical world as a reasonable alternative to excluding minors completely from the store", these laws were entirely inappropriate online (Id).

For the Court, the Act's affirmative defenses and technical provisions lacked "the precision that the First Amendment requires when a statute regulates the content of speech" (CDA18 p. 19). First, the criminal sanctions imposed by the CDA would "cause speakers to remain silent rather than communicate even arguably unlawful words, ideas, and images" (CDA18 p. 18). More insidiously, the CDA had the potential to become a means for endorsing certain kinds of speech over others. Whether it be through the use of content tagging, ratings systems, or the blocking of content at the ISP level with little or no oversight, the Act was a hegemonic means for privileging speech that was "decent" above that which the state defined as "indecent" whether that speech merited constitutional protection or not. Due to the "risk of discriminatory enforcement" (Id) and "Given the vague contours of the coverage of the statute, it unquestionably silences some speakers whose messages would be entitled to constitutional protection" (Id p. 19). The

law would create a "heckler's veto" and "confer broad powers of censorship" not only on the state but also "upon any opponent of indecent speech" (CDA18 p. 3).

The Court also rebuked the government for its lack of critical analysis. The mechanisms required by the Act were so broad and so intrusive that they could not qualify for the standards of strict scrutiny that any law regulating speech must meet.[19] In the Court's view, if Congress had conducted a proper review of the Act's technical provisions, it would never have passed such a policy. This was particularly true "in light of the absence of any detailed congressional findings, or even hearings addressing the CDA's special problems" (CDA18 p. 3). Furthermore, not only were content decisions delegated to ISPs and the blocking technologies they employed, but at no point did the CDA's broad prohibitions on speech engage "an agency familiar with the medium's unique characteristics" (Id p. 2) or any institution that could provide oversight and protection for constitutional speech. This was an unacceptable abuse of state power and an inappropriate technological means for regulating the Internet. As the opposition, the District Court and now the Supreme Court had made clear, "As a matter of constitutional tradition…we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The Interest in encouraging freedom of expression in democratic society outweighs any theoretical but unproven benefit of censorship" (CDA18 p. 26). The Court had struck down the CDA.

---

[19] Specifically, any such law must pass the "Least Restrictive Means Test." This Test "is a standard imposed by the courts when considering the validity of legislation that touches upon constitutional interests. If the government enacts a law that restricts a fundamental personal liberty, it must employ the least restrictive measures possible to achieve its goal. This test applies even when the government has a legitimate purpose in adopting the particular law. The Least Restrictive Means Test has been applied primarily to the regulation of speech" (Farlex, 2014).

Table 5 – Communications Decency Act Frame Analysis Summary

Frames	Legislative Themes
Master (Motivation)	• Motivated by a desire to protect children from sexually explicit content online. • It is a compelling interest of the state to protect children. It is also within the state's authority to regulate the Internet similar to broadcast radio and television and "zone" pornography on the Web. • Due to the core cultural values and ideology embedded in the state's desire to protect children, this master frame does not appear to be particularly amenable to a sustained and critical debate.
Diagnostic (Problem)	• Unregulated access to the Internet harms children. • The "invasive" nature of the Internet not only makes the danger to children more immediate, but it also speaks to the ability of the state to regulate the Internet similar to other broadcast media. • The Internet is a lawless frontier that requires intervention through policy and technology in order to make it safe for minors. Speech rights and autonomy are secondary to the protection of children.
Prognostic (Solution)	• Access controls and regulatory technologies such as age verification systems protect children. • It is the duty of the state to provide a solution to this harm in the form of technological mechanisms of enforcement including age verification systems. • The Internet is uniquely responsive to technological regulation. Those mechanisms allow the state to regulate content without bias and with viewpoint neutrality.

Frames	Oppositional Themes
Master (Motivation)	• Motivated by the need to protect individual autonomy and adult access to protected speech. • Although children require protection from some online content, the state is equally compelled to ensure the right of adult access. • The use of regulatory systems should not constrain autonomy, freedom, and constitutional guarantees systems and Congress must consider that potential prior to implementation.
Diagnostic (Problem)	• Technological barriers to access harm adult rights and autonomy. • The opposition rhetorically defined the Internet as a vast democratic forum that had the potential to revolutionize and democratize the ability of individuals to communicate with one another. • The Internet does not conform to traditional metaphors of zoning or broadcast media and legislators should not unjustly restrict it through poorly understood regulatory systems.
Prognostic (Solution)	• Congress would apply the technological mechanisms required by the policy too broadly and would damage constitutional freedom and individual autonomy. • The solution is to re-draft the legislation, severely limiting the use of these regulatory systems in the process, or have the CDA struck down as unconstitutional by the courts. • If legislators must impose regulatory systems, they should implement them voluntarily and should empower the user to make their own decisions about content.

Communications Decency Act Documentation Index

CDA01	Communications Decency Act of 1996, (CDA), Pub. L. No. 104-104 (Tit. V), 110 Stat. 133 (Feb. 8, 1996), codified at 47 U.S.C. § 231.
CDA02	Cannon, R. (1996). The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway. *Federal Communications Law Journal*, *49(1).*
CDA03	Senate Report No. 104-230 (Feb. 1, 1996).
CDA04	Exon, J. (1996). The Communications Decency Act. *Federal Communications Law Journal, 49(1).*
CDA05	Senator Pat Leahy. (1997). Statement on Supreme Court's Decision Declaring Unconstitutional the Communications Decency Act [Press Release].
CDA06	Center for Democracy and Technology. (1996). Exon Issues Statement on Court Ruling on Decency Act [Press Release].
CDA07	American Civil Liberties Union. (1997). ACLU Hails Supreme Court Victory in Internet Censorship Challenge [Press Release].
CDA08	Electronic Frontier Foundation. (1997). Supreme Court Victory for Free Speech: CDA Ruled Unconstitutional [Press Release].
CDA08a	The White House, Office of the Press Secretary. (1997). Statement by the President [Press Release].
CDA08b	Citizens Internet Empowerment Coalition. (1996). Supreme Court Agrees to Hear Landmark Case to Determine Future of Free Speech in Cyberspace [Press Release].
CDA08c	Electronic Frontier Foundation. (1996). Federal Court Rules Communications Decency Act Unconstitutional [Press Release].
CDA08d	The Family Research Council. (1996). Arrogant Decision Contradicts Prior Cases on Pornography Distribution to Minors, FRC Says [Press Release].
CDA08e	Electronic Frontiers Georgia. (1996). CDA Reaction from EFG [Press Release].
CDA08f	Electronic Frontier Foundation. (1996). What the Final Arguments Tell Us About The Fate of the CDA [Press Release].
CDA09	Electronic Frontier Foundation. (1996). Your Constitutional Rights Have Been Sacrificed for Political Expediency [Press Release].
CDA10	Electronic Frontier Foundation. (1997). CDA 230: The Most Important Law Protecting Internet Speech. Retrieved from https://www.eff.org/issues/cda230/legislative-history
CDA11	American Civil Liberties Union, et al. v. Janet Reno, 138 L. Ed. 2d 874 (1996). Complaint.
CDA12	American Civil Liberties Union, et al. v. Janet Reno, 138 L. Ed. 2d 874 (1996). ALA Plaintiffs' Post-Hearing Brief in Support of Motion for Preliminary Injunction.
CDA13	American Civil Liberties Union, et al. v. Janet Reno, 138 L. Ed. 2d 874 (1996). Adjudication on Motions for Preliminary Injunction.

CDA14	Janet Reno v. American Civil Liberties Union, et al., 521 U.S. 844 (1997). Brief for the Appellants.
CDA15	Janet Reno v. American Civil Liberties Union, et al., 521 U.S. 844 (1997). ACLU's Motion to Affirm the Decision of ACLU v. Reno.
CDA16	Janet Reno v. American Civil Liberties Union, et al., 521 U.S. 844 (1997). Brief of Members of Congress.
CDA17	Janet Reno v. American Civil Liberties Union, et al., 521 U.S. 844 (1997). Brief of Appellees American Library Association, et al.
CDA18	Janet Reno v. American Civil Liberties Union, et al., 521 U.S. 844 (1997). Opinion of the Supreme Court of the United States.
CDA19	Exon, J. (1995, April 9). Keep Internet Safe for Families. *Dallas Morning News*.
CDA20	Harrington, J. (1995, April 9). Beware of Chilling Freedom of Expression. *Dallas Morning News*.
CDA21	House Report No. 104-458 (Jan. 31, 1996).
CDA22	104 Congressional Record (1995) S8053, 8087-8091 (statement of Senator Exon).
CDA23	Interactive Working Group Report to Senator Leahy. *Parental Empowerment, Child Protection, & Free Speech in Interactive Media,* July 24, 1995.
CDA24	Exon, J. (1995, June 22). Interview by E. Farnsworth, *The MacNeil/Lehrer NewsHour* [Television Broadcast]. Washington, D.C.: Public Broadcasting Service.
CDA25	104 Congressional Record (1995) S8310, 8329-8350 (statements of Senators Exon and Leahy).
CDA26	U.S. Senate, Committee on the Judiciary. *Cyberporn and Children: The Scope of the Problem, the State of the Technology, and the Need for Congressional Action*, Hearing, July 24, 1995 (Serial No. J-104-36). Washington: Government Printing Office, 1995.
CDA27	American Civil Liberties Union. (1996). ACLU Background Briefing – Reno v. ACLU: The Road to the Supreme Court [Press Release].

Chapter 5 – The Child Online Protection Act

Introduction

Chapter 5 will provide an analysis of the frames underlying the CDA's successor, the Child Online Protection Act. Passed in the wake of the Supreme Court's landmark decision in *Reno v. ACLU* striking down the CDA, this policy would attempt to advance many of the same master, diagnostic and prognostic frames described previously. Specifically, this chapter will address the government's continuing interest in protecting children from material deemed harmful to them and their reliance on a technological solution for ameliorating any harm caused by unregulated access to online content.

Similarly, faced with the specific requirements of this new policy, activist organizations and online content providers would argue that no significant changes had been made to differentiate it from the CDA. These groups would advance a number of the same frames and again suggested that the government had failed to account for access to protected speech in this new online forum as well as the autonomous ability of the individual to both speak and listen. Lacking any significant modifications, the opposition continued to argue that Congress should carefully analyze technological access controls prior to implementation or that the courts must strike COPA down.

Despite the opposition's insistence that this new policy did not represent any significant difference, Congress did demonstrate a willingness to address some of the concerns that had plagued the CDA. Supporters of this new policy had carefully studied the CDA's progress through the courts and made several frame shifts in the face of the opposition's arguments and the Supreme Court's constitutional criticisms. These concessions would narrow enforcement and reassess the use of regulatory technologies.

Part I – Legislative Master Frames

The Communications Decency Act failed but the master frame of protecting children from indecent online content carried on. Even before the Supreme Court had handed down its decision, there were indications that there would be further legislative attempts to police the Internet. Although the constitutionality of the CDA was in serious doubt at the time, "Proponents of Internet content regulation have already indicated their desire to take a 'second bite of the apple' if the Communications Decency Act is struck down" (CDA07 p. 9). This time Representative Michael Oxley (R-OH) led the charge and proposed H.R. 3783, commonly referred to as the Child Online Protection Act (COPA). Oxley and other legislative supporters of COPA had paid close attention to the debate surrounding the CDA and had "carefully drafted" COPA "to respond to the Supreme Court's decision" (COPA21 p. 5). As opposed to the CDA, this bill had the stated goal of striking "the appropriate balance between preserving the First Amendment rights of adults and protecting children from harmful material on the World Wide Web" (Id).

COPA differed from the CDA in a number of important ways. First, it purposely narrowed the scope of regulation. Where the CDA was overly broad and harmful to a multitude of private and non-profit speakers, COPA specifically targeted commercial content providers. The hope was that COPA would be "narrower than the CDA" because it focused only on "entities engaged in the business of transferring or selling over the World Wide Web information deemed 'harmful to minors'" and required them to place that content "behind a barrier surmountable only by those over 17" (COPA11b p. 11). By avoiding individual speakers and non-commercial outlets, Oxley hoped that COPA

would circumvent many of the constitutional concerns raised by the CDA's broad mandate. The lesson that Oxley and other supporters of COPA had taken from the Supreme Court's decision was that private and non-profit speech was off limits. By contracting the effect of the law, Oxley believed that COPA's focus on commercial pornographers would guarantee its constitutionality. From the Congressional point of view, COPA's provisions would "not inhibit the ability of adults to access such speech or the ability of commercial purveyors of materials that are harmful to minors to make such speech available to adults" (COPA14 p. 5).

Furthermore, the bill dropped the much more legally ambiguous "indecency" standard used within the CDA and dealt only with that content more specifically defined as "harmful to minors." The CDA's "indecency" standard had been problematic because it was both vague and covered a wide range of speech including "any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs" (CDA01 pp. 95-96). By contrast, COPA's use of the "harmful to minors" standard was both more specific and better understood by courts and content providers. The government argued that this standard would prove to be constitutional in an online context because it "does not cover material unless it is designed to appeal to the prurient interest of minors; it specifies the particular sexual acts and parts of the anatomy the depiction of which can be found to be patently offensive; it makes clear that the prurient interest and patently offensive determinations should be made 'with respect to minors'" (COPA17 p. 52). For these reasons, Oxley and

his supporters believed that the "harmful-to-minors standard [did] not impose an undue burden on protected speech" (COPA17 p. 34).

This was a clear and direct frame shift – a reduction in the scope of enforcement predicated on the opposition's arguments against the CDA and the subsequent legal challenge. In a move motivated entirely by oppositional First Amendment concerns, Oxley had tailored COPA to ameliorate some of those anxieties. It was precisely because the CDA had been struck down that Congress responded with COPA and found that "H.R. 3783 is currently the most effective, yet least restrictive approach that should be taken given the current state of the technology" (COPA24 pp. 2-3). By excluding private and non-profit content providers and by eliminating vague references to "indecent" content, "Congress responded directly to the Court's concern about the unprecedented breadth and undefined parameters of the CDA" (COPA17 p. 52). Other frame shifts were also manifest in COPA and would relate much more specifically to the opposition's calls for a critical review of the policy's technological mechanisms of enforcement.

Despite this, many of COPA's specific provisions would remain remarkably similar to those found in the CDA. For example, while the scope and target of content regulation had changed, the motivations for COPA were indistinguishable from those behind the CDA. The prevalence of adult material and the ease with which it kids could access it was harmful and the state had an obligation to minimize the damage this caused to children. Supporters of COPA had no compunctions about invoking this same master frame and, on the contrary, believed that this issue continued to demand legislative action. They recognized the ideological justifications they shared with proponents of the CDA and acknowledged that "The protection of America's children online has been a

powerful motivating issue for policymakers since the Internet became widely available" (COPA04 p. 11). Like those that came before them, Congressional supporters of COPA recognized that the "Internet promises to revolutionize access to information, create new forms of social interaction, promote economic opportunity, and reinvigorate civic discourse" while insisting that "this same technology risks exposing children to material, particularly material of sexually-explicit nature, that many believe is inappropriate or harmful to their development" (Id). COPA's advocates believed that Congress must "take steps to stop our children from being hurt" and failure to act would mean that "our children will be right to blame us for what we have allowed" (COPA04 p. 70). In language nearly identical to that used to justify the CDA, Congress found that "the protection of the physical and psychological well-being of minors by shielding them from materials that are harmful to them is a compelling governmental interest" (COPA17 pp. 13-14). As will be discussed shortly, the technological means for accomplishing that compelling interest would also be similar to those mandated by the CDA.

Embedded within this master frame, COPA's supporters employed some of the same metaphorical rationales they had used for the CDA. Although the Supreme Court had deconstructed some of these analogies, this did not prevent Oxley and others from trying again. Specifically, these frames continued to emphasize the invasive nature of the medium and appealed to physical analogs for legal and constitutional support. Lawmakers insisted that protections "from commercial pornography in the real world of homes, schools, libraries, and neighborhoods…convenience stores and other areas that children frequent" should extend to "an analogous level of protection online" (COPA4 p. 53). Like laws regulating real world pornographers, the intent of Congress here was to

require online pornographers to do the same by placing their wares away from minors. This was not constitutionally problematic because it was simply an extension of "existing requirements…that such material be held behind the counter or sold in a paper wrapper in a physical store" (COPA14 pp. 22-23). There were no implications for adult speech within the structure of this frame. COPA would be no more than a natural extension of state laws requiring those who sold adult magazines and videos "to sell them on display racks that are out of reach or sight of minors, while still available for purchase by adults" (COPA24 pp. 20-21). Congress believed this was solid regulatory terrain and just "Such an adult sales method is what this Act intends to and would extend to the commercial Web, as it fairly should" (Id).

In the absence of such safeguards, harmful material would assault kids' computers and even "Innocent search requests [would] turn up lurid descriptions of pornographic sites that can be accessed via a mouse-click" (Id). Perhaps in reference to Senator Exon's assertion that pornography was "only a few click-click-clicks away from any child" (CDA14 p. 13), COPA's supporters reemphasized that "In only a few mouse clicks, children can be exposed to material that can never be erased from their minds" (COPA04 p. 77). The pervasive presence of harmful material and the ease with which children could reach it demanded government intervention. Supporters of COPA consistently referred to the invasive nature of this medium as justification for federal regulation. This new technology created a unique circumstance and "Never in the history of telecommunications has an entire generation of children been invaded by sexually-explicit material with so few restrictions" (Id). Therefore, from the perspective of this

master frame, it was "incumbent on parents, industry and government to work together to provide children the protected space of innocence they deserve" (Id).

Despite its apparent novelty, COPA's supporters did not entirely abandon the idea that the Internet's pervasive presence in America's homes made it comparable to broadcast radio and television. Keeping in mind the Supreme Court's ruling that *FCC v. Pacifica Foundation* did not justify heavy-handed Internet content regulation (see page 134), Oxley and others did not overtly rely on comparisons to broadcasting. In fact, they admitted that "While clearly the Internet is not yet as 'invasive' as broadcasting, its popularity and growth because of electronic commerce and expansive Federal subsidy programs make it widely accessible for minors" (COPA21 pp. 9-10). Allusions to broadcasting continued to appear throughout the rhetoric supporting COPA. The Internet, like television, was intrusive, unavoidable, and easy for kids to use. Minors could find harmful material online "as easily as they can change television channels" (COPA17 p. 33) and kids, "who can read and type are capable of conducting Web searches as easily as operating a television remote" (Id p. 10). The veiled assertion seemed to be that because "television rules limit programming containing indecent adult material to late evening hours" the Internet should be subject to "an analogous" regulatory scheme (COPA04 p. 53). Comparisons to broadcast content regulations had moved to the background but they persisted throughout the debate over COPA.

Congressional support for COPA also relied on the same regulatory systems that had underpinned the CDA. Specifically, COPA again mandated the use of age verification systems as the primary "technological tools" (COPA01 p. 6) which would accomplish the state's compelling interest in protecting children (COPA03 p. 3).

Specifically, the Act's affirmative defenses provided immunity for those commercial content providers who restricted access "by requiring use of a credit card, debit account, adult access code, or adult personal identification number…by accepting a digital certificate that verifies age; or…by any other reasonable measures that are feasible under available technology" (COPA02 p. 2). Oxley and others believed that there was nothing inherently wrong with enforcement through age verification technologies only that Congress had applied these systems overzealously through the CDA. Besides, by more narrowly tailoring the breadth of COPA and limiting enforcement only to commercial content providers, the policy was simply formalizing an arrangement that was already "standard practice" (COPA21 pp. 14-15). It was accepted wisdom that the proprietors of most adult websites "already put most of their material behind age verification screens" (COPA17 p. 47). COPA would simply serve to extend that technological arrangement to any bad actors who allowed access without proof of age.

While the vast array of sexually explicit content on adult websites was of primary concern to legislators, they were also troubled by the tantalizing images that lured customers (and children) to these sites in the first place. Due to the enticing pictures of scantily clad models placed on or before age verification screens, Congress was concerned that these photographs and animated graphics would be just as damaging to children, if not more so, because of their readily available nature (COPA14 pp. 1-2). The master frame of protecting children was, in this instance, directed at these "teaser" images that offered such unseemly temptation. Without direct government intervention, "unsupervised minors [would], with the click of a mouse, visit one pornographic site after another, and view and then print one set of pornographic teasers after another" (COPA17

p. 33). For Oxley and his supporters, these "Teaser pages should be located only beyond the front, public page" (COPA04 pp. 45-46) and it was crucial that COPA "require those commercial pornographers to put their teasers behind age verification screens as well" (COPA17 p. 26). This would help fulfill COPA's master frame and would "protect the great majority of minor children in America from the instant and unrestricted access to the free pornographic 'teaser' pictures now openly available at commercial porn sites on the World Wide Web" (COPA24 pp. 2-3). Within the context of COPA's mandate, this focus on teasers and the enticement they represented was completely appropriate. From the legislative point of view, this requirement was simply a sterner means for regulating commercial pornography and keeping all such images "behind the counter" (COPA14 pp. 22-23) of age verification screens.

From the standpoint of the opposition's previous criticisms, the most important distinction between the CDA and COPA was its mandated call for critical review. Built into the language of the policy was a requirement establishing a Commission on Online Child Protection "to study technological and other methods to help reduce access by minors to material that is harmful to minors on the Internet" (COPA21 p. 6). This Commission would represent a broad range of stakeholders and interests although the collective expertise of those appointed to the Commission overwhelmingly related to the technology industry and technological barriers to access. By specific statutory provision, individuals comprising the Commission were to include: members "engaged in the business of providing Internet filtering or blocking services or software;" members "engaged in the business of providing Internet access services;" members "engaged in the business of providing labeling or ratings services;" members "engaged in the business of

providing Internet portal or search services;" members "engaged in the business of providing domain name registration services;" members "who are academic experts in the field of technology;" and members "engaged in the business of making content available over the Internet" (COPA01 pp. 5-6). It is interesting to note that one of the Commission's eventual members would be a representative of the Center for Democracy and Technology (CDT), one of the key groups responsible for targeting the CDA and one of the named plaintiffs in the court action that led to its demise. It could be inferred that legislative supporters of Internet content regulation had learned a valuable lesson from both the opposition's arguments against the CDA and from the Court's ruling. In requiring this Commission, Oxley and others appear to have heard some of the criticism that doomed COPA's predecessor and, accordingly, conducted this critical review in order to include oppositional perspectives. This particular frame shift appears to have been a self-conscious move on the part of COPA's supporters to assuage any ethical, constitutional, or technological concerns from the outset. This awareness was explicit in debates surrounding COPA and the law's supporters were mindful that the Supreme Court had been critical of the CDA in part because "Congress did not hold legislative hearings on the CDA, nor did Congress reach any detailed findings addressing the problem of distributing indecent materials to minors over the Internet" (COPA21 p. 16). Through this Commission and subsequent hearings, COPA's supporters meant to avoid any such oversight if this policy came under constitutional scrutiny. Despite this, the Commission's membership and its overpowering focus on technological mechanisms of enforcement were indicative of Congress' technological commitments.

Part II – Oppositional Master Frames

Despite the important policy shifts that had occurred during the interim between the CDA and COPA, the opposition was unconvinced that this new law would adequately address their core concerns. Due to this, the oppositional master frames related to COPA remain nearly identical to those employed during the debate over the CDA. For the opposition, COPA was strongly reminiscent of the CDA and any differences between the two were merely window dressing. For all intents and purposes, "COPA traces the same path as the CDA and suffers from many of the same crippling constitutional flaws" (COPA23 pp. 4-5). Like the CDA, COPA's flaws disallowed or actively criminalized a "broad category of speech that is lawful as to adults" (Id) despite its more narrow focus on commercial websites. Opponents also remained skeptical that the age verification systems required by COPA would prove to be less restrictive in this new context than they had been in the old. In fact, the opposition was relatively certain that these regulatory systems would impose a direct burden on speech and would "discourage readers of controversial or potentially controversial material" (Id). Oppositional groups would also maintain their argument that centralized content regulation disempowered parents and reduced individual autonomy. Like the CDA, COPA's mandate implied that parents were unable or unprepared to take the steps necessary to protect their children. From this point of view, COPA's affirmative defenses and age verification requirements seemed to presume "that parents lack the ability, not the will, to monitor what their children see" (COPA25 pp. 15-16). The opposition would challenge this presumption and would offer a variety of technological and non-technological alternatives to what they saw as an overbroad and unconstitutional policy.

One of the key differences here was that, for the first time, the opposition focused one of its key master frames on non-technological methods for both protecting minors and preserving access to constitutional speech. This master frame intertwined with the frames of user empowerment and parental oversight while minimizing the need for a centralized, governmental solution. While "low-tech" options including parental supervision had been a tangential recommendation offered during the fight over the CDA (CDA17 p. 31), here they became a core foundation of the opposition's argument. One of the primary means for accomplishing this, and for maintaining parental autonomy in the process, was a wide call for education. The opposition saw this alternative as vastly preferable to the more restrictive measures required by COPA. Education would also have the direct benefit of raising awareness in the home and across communities while keeping the government out of the business of criminalizing content. As one ACLU spokesman noted, "Lawmakers should stop passing criminal laws for the Internet and focus instead on educating users to make their own choices about what content to view or avoid" (COPA09a p. 5). The Center for Democracy and Technology (CDT) echoed this call and decried the "expensive cycle of legislation and litigation [that] does little to serve children and families online" (COPA10b pp. 18-19). Instead, the CDT believed that "giving users control over what they see and do online – through education…will more effectively protect kids in ways consistent with their own family values, and with the Constitution" (Id). Rather than mandating the imposition of inappropriate technical solutions, the opposition felt that "educating…children to make their own informed choices" (COPA18 pp. 21-22) better served parents and democratic society.

According to the opposition, options like education and parental supervision would have vastly superior outcomes because "non-technological parental controls are less restrictive than COPA and target inappropriate content more effectively" (COPA18 p. 24). Where COPA lacked "flexibility and specificity" (Id), "Non-technological user empowerment techniques…are a more effective and less restrictive alternative to COPA as a way of protecting children from inappropriate online content" (Id p. 25). Clearly, from the opposition's point of view, low-tech or no-tech options, particularly education, were preferable to COPA's technological requirements that inhibited speech, reduced autonomy and failed to protect children (COPA10a p. 10).

Of course, these non-technological methods were not the only alternatives offered by the opposition. If anything, the opposition increased its calls for the use of blocking and filtering software as Congress considered COPA. Nevertheless, just as they did during the debate over the CDA, the opposition here cited these systems as voluntary methods that could be tailored to reflect individual values and customized to account for the varying maturity levels of children (COPA20 p. 72). Although the emphasis was on technological filtering software, the opposition based its recommendation of such systems on the presumption that they would afford parents the opportunity to exercise some measure of autonomy. The opposition made it quite clear that "a voluntary decision by concerned parents to use these products for their children constitutes a far less restrictive alternative than COPA's imposition of criminal penalties for protected speech among adults" (COPA16 p. 46). In fact, the opposition seems to have made a rhetorical choice to differentiate filtering software as "technological user empowerment tools," contrasting such systems with those required by COPA which would be both

"more restrictive of protected speech" and "less effective at achieving the governmental interest" of protecting children (COPA18 pp. 20-21).

It is interesting to note that in this instance the opposition underwent a frame shift of its own. Although their advocacy of voluntary filtering software had carried over from the debate on the CDA, opponents of COPA began to express certain doubts about such commercial systems. While these "user empowerment tools" offered a degree of autonomy to individuals and helped safeguard constitutionally protected speech by not regulating that speech *a priori*, the subtext of the opposition's argument differs significantly from its previous incarnation. Specifically, although these "user-control tools" offered significant advantages "without need for government regulation" (COPA23 pp. 3-4), the opposition repeatedly pointed out that "filters may be considered over- or under- inclusive by various individuals and communities" (COPA11b p. 17).

While the opposition unconditionally supported filtering software in their arguments against the CDA, here they tempered that support with a growing awareness of the technology's shortcomings. Despite the numerous advantages the opposition saw in filtering products, they increasingly acknowledged that "user-based blocking programs are not perfect" (COPA16 p. 46). Oppositional groups pointed to the District and Supreme Court's rulings on the CDA as evidence of the efficacy of filtering software (COPA11c p. 23) but their previous enthusiasm was gone. In its place, a more technically critical and measured approach to such systems dominated the opposition's arguments.

Part of the solution offered by the opposition to alleviate this unease was to mandate that Congress and industry undertake sustained and critical analysis of these

systems. While industry should work to "improve filtering and blocking technologies" (COPA04 p. 42), it was incumbent upon government to determine how those technologies could impact autonomy and speech whether they be used at the individual, community or federal level. As the opposition noted, to that point there had "been no study, no discussion, and no comparison of the effectiveness of various approaches, their likely impact on speech, and their appropriateness for the Internet" (COPA11c pp. 26-27). This was especially troubling considering the courts' stated views on filtering technology from the CDA opinions. Both courts had noted that "these tools, unlike a criminal statute, can protect children from domestic and foreign material" (COPA11c p. 23). Despite suggestions from the Supreme Court that these systems could offer at least a partial solution to the problem of sexually explicit online content, Congress had not conducted any study of this technology in the interim and had instead proposed another sweeping statute targeting content providers and criminalizing speech at the source (Id). This insistence on federal regulation concerned the opposition and they noted Congress' lack of meaningful review of this promising technology. If the harm done by sexually explicit websites so concerned Exon, Oxley and their supporters, why were they not pursuing all alternatives? It was puzzling that Congress had "developed no record to explain why it was rejecting further efforts that can be undertaken to educate parents and other care-takers about the availability of blocking and filtering tools" (Id). Although the opposition had noted that these systems would sometimes "fail to screen all inappropriate material and…block valuable websites" (COPA13 p. 13), it was still necessary for Congress to find out what, exactly, the benefits and shortcomings of such technologies might be. Without such a critical review, the opposition argued, and without "a factual

record to support this bill, the Court will find it, like the CDA, unconstitutional" (COPA11c pp. 26-27). If Congress was truly interested in pursuing "the most effective, yet least restrictive approach that should be taken given the current state of the technology" (COPA24 pp. 2-3), then they must undertake a critical review of voluntary filtering software. Without such an effort, the opposition argued, legislators had made it clear that they were unwilling to pursue any options other than those that centralized content decisions and criminalized a great deal of protected speech (COPA12a p. 13). It remained to be seen if the statutory requirements establishing the COPA Commission would prove to be satisfactory in this regard.

Part of the motivation for this shift in the opposition's master frame regarding the utility of commercial filtering software related directly to bills proposed in parallel to COPA. The opposition's growing wariness of filtering and blocking products had arisen in response to the Safe Schools Internet Act, the Child Protection Act and the E-Rate Policy and Child Protection Act (COPA11b pp. 13-14). Although tangential to COPA and never enacted, these proposals represented a further frame shift in policy debates. As opposed to Oxley and other supporters of centralized solutions like COPA, supporters of these proposed Acts focused content enforcement at the local level, namely schools and libraries. The technological mechanism for accomplishing the goals of these proposed policies was primarily the mandatory installation of commercial filtering software within these local institutions (COPA11b p. 13). The CDT, perhaps out of concern that such requirements might migrate into COPA's mandate, prepared a critique of these systems that would color what had previously been relatively unanimous support for filtering software on the part of the opposition. In a blistering appraisal of the compulsory

implementation of filtering software, the CDT essentially set the stage for the debate that would coalesce around the Children's Internet Protection Act (CIPA). Although CIPA will be the focus of Chapter 6, it is important to trace the evolution of this argument within the context of COPA. In language remarkably similar to that used in future frames, the CDT argued that such obligatory use of filtering software would remove any benefits it had as a voluntary mechanism, reduce parental autonomy and "usurp local communities' ability to set standards that reflect their values" (COPA11b p. 13).

The ability of communities to set these standards is not simply a rhetorical nod to some hypothetical, preferred arrangement between federal regulators and localities. Although certainly not a universal feature of governmental hierarchy in an international context, municipal autonomy and the local determination of community standards are a well-established feature of the U.S. political landscape. The Tenth Amendment to the Constitution guarantees that "The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people." Implementation of Home Rule or the state's grant of self-determination to municipalities can formalize this relationship as long as state laws remain in force (see Munro, 1930). Based on this precedent, states, municipalities and local library boards (comprised of community representatives) are not beholden to the federal government when making determinations as to, for example, the suitability of content in public libraries. The Supreme Court has historically supported state and local authority and community standards were the basis for the Court's obscenity test in *Miller v. California* (413 U.S. 15, 1973). Specifically, the Court found that the state should strictly observe the Tenth Amendment and that the federal government must not interfere with local

determinations as to the obscenity, indecency, or suitability of material within that community. Instead, content is classified based on whether or not the "average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest" (Id). In the context of COPA and, eventually, CIPA, Congress encroached on rights that local communities took for granted. The opposition premised its arguments against centralized and/or technological regulation on that understanding.

The opposition also extended its argument to employ a novel master frame. Specifically, the opposition argued that mandatory use of filtering software would minimize technological transparency. First, due to financial constraints, public schools and libraries would be unable to design and implement their own filters that could meet both local standards and statutory requirements (COPA11b p. 13). Furthermore, this lack of options would require the purchase of commercial software, the producers of which "do not disclose the standards under which they filter or the list of filtered sites" (Id). This was particularly concerning for the opposition when some filters had demonstrated a decidedly hegemonic view of "acceptable" content. The CDT pointed to a number of studies "of commercial [sic] available filters [which] suggest that they curtail access to information on topics ranging from gay and lesbian issues, women's health, conservative politics, and many others" (Id p. 14). As the opposition made clear, "[t]he prospect of schools and libraries…delegating their traditional power to unchecked private entities raises troubling First Amendment issues" (Id pp. 13-14). The master frame of technological transparency would remain a peripheral issue during the debate

surrounding COPA but it would presage the opposition's evolving position on commercial filtering software.

The final master frame employed by opponents of COPA deals with the need for any policy or technological mechanism of enforcement to preserve access to constitutionally protected speech. Just as the opposition argued during the debate over the CDA, it was crucial for government to explicitly consider the impact laws like COPA could have on both speakers and listeners. Wary of Oxley's commitment to this constitutional necessity the opposition remained unconvinced that COPA represented any significant improvement over the CDA in this area. In addition to concerns directly related to the age verification technologies required by COPA (concerns that will be addressed in detail in Part IV), the opposition derided this new policy and Congress for the continued failure to understand the nature of the Internet.

While Oxley and his supporters had learned a great deal from the controversy over the CDA and had shifted the scope of enforcement, the opposition continued to argue that COPA's "constitutional flaws…were identical to the flaws that led the Supreme Court to strike down the Communications Decency Act" (COPA09 p. 1). Despite its narrower focus on commercial speakers, COPA "suppresses a wide range of socially valuable speech that adults have a right to communicate" (Id p. 3). Rather than recognizing the policy shifts represented by COPA as constitutionally significant, the ACLU and others pointed to its overwhelmingly similarity to the CDA. From this point of view, COPA was simply "Congress' second attempt to censor free speech on the Internet" (Id p. 4) and "the successor to the Communications Decency Act" (COPA10c p. 21). By targeting speech at the source and by employing the same technological

mechanisms of enforcement, Congress had essentially, "created a nearly identical scheme of government censorship that suffers from the same constitutional deficiencies that the courts found in the CDA" (Id). Until supporters of centralized content management realized that these kinds of efforts were entirely inappropriate from the standpoint of free speech, opponents would maintain their position and continue their legal challenges. While the opposition did not disagree that the Internet provided access to a great deal of content that was inappropriate for minors, these groups argued that the CDA's centralized technological "approach to protect children online has been an utter failure" (COPA11 p. 2) and that COPA would reproduce that failure.

One of the primary causes of this constitutional failure and why Congress was doomed to "repeat the mistakes of the CDA" was because, as the CDT put it, lawmakers had failed "to take into account the special aspects of this potentially powerful medium" (COPA11a p. 6). From the opposition's perspective, the Internet functioned as a "democratizing medium that expands the power of citizens to engage in speech in unprecedented ways" (COPA04 p. 64). As the ACLU would argue, Congress had "once again fundamentally misunderstood the nature of the Internet" (COPA09b p. 6) by failing to recognize that COPA would greatly reduce access to a wide range of constitutionally protected speech. Specifically, Congress drew false distinction between commercial and non-commercial speech, walling off a number of educational, informational and artistic websites simply because they were "engaged in the business of transferring or selling" information online (COPA11b p. 11). This extended to protected speech including "the poet Lawrence Ferlinghetti, writers of sexual advice columns, and websites for a

bookstore, an art gallery, and the Philadelphia Gay News, to name a few" (COPA09b p. 6).

For the opposition, Congress had neither taken the nature of the medium into account nor recognized the impact regulations like COPA could have on protected speech. This grave misunderstanding related directly to legislators' insistence that the Internet could be regulated based on local standards. In particular, the opposition argued that COPA's "harmful to minors" standard would prove to be unconstitutional because it confined content producers to community standards of what constituted "harmful" material. This was a facet unique to COPA and differed from the CDA's attempt to "establish a uniform national standard of content regulation" (CDA13 p. 49). In contrast, COPA left determinations of acceptability to local mores, forcing speakers to wall off any speech that could conceivably be considered harmful and "abide by the most restrictive community's standards" (COPA09c p. 9) when doing so. By confining speakers to the most conservative local standards, this provision of COPA failed to account for the "geography-free nature of cyberspace" (Id). This would leave Website operators to make their best guess as to "what contemporary community standards should or could mean in a medium without geographic boundaries" (COPA15 p. 19). Precisely because COPA relied on local notions of suitability when regulating content, it would preemptively chill a great deal of speech from those who did not wish to run afoul of the law's criminal provisions. In relation to the opposition's master frame of protecting access, such a requirement "must lead inexorably to a holding of…unconstitutionality of the entire COPA statute" (COPA09c p. 9). If a judgment of content could "only be made in the context of local community standards" then the law's foundation and technological

requirements raised a serious "constitutional question whether it is possible to reconcile First Amendment obscenity jurisprudence with the technological fact that the 'community' of speakers and listeners on the Internet is inherently global" (COPA04 p. 85).

From the perspective of the ACLU, CDT and other oppositional groups, the differences between the CDA and COPA were insignificant and constitutionally irrelevant. The best that could be said of COPA was that it was "not quite as censorious" as the CDA (COPA09a p. 4). A law regulating Internet content, like "a law banning books does not become constitutional because it is re-written to remove only every other book on the shelves" (Id). This was the crux of the opposition's constitutional argument: the narrow focus on commercial websites and the reliance on local "harmful to minors" standards made COPA no less egregious than the CDA. Congress' insistence on managing Internet content through federal regulation and through technological mechanisms of enforcement was unlikely to pass constitutional muster no matter where or how narrowly it was targeted. For the opposition, any attempt at "[c]entralizing content decisions in the federal government" would inevitably lead to a reduction in access to speech otherwise available to adults (COPA11b p. 11). The opposition also remained adamant that Congress must examine the constitutional implications of policies like COPA and technologies such as age verification systems prior to implementation. Although COPA mandated a commission to research some of these issues, that study would not occur until after Congress had enacted the law. Until such critical analysis was complete, "Congress should refrain from imposing new access restrictions" (COPA10 p. 7) that had the potential to cause constitutional harm.

Part III – Legislative Diagnostic Frames

The legislative diagnostic frames employed by Congress to promote COPA are again remarkably similar to those invoked during the debate over the CDA. The Internet, and unregulated access to it, were continuing problems due to the pornography readily available to children. The harm caused to children by such unregulated access was both irrevocable and irreparable. In the absence of government intervention through policy and through technology "There is no way to restore innocence lost and a diet of pornographic fare will lead to disasters in fighting sexual harassment, STDs, and sexual or domestic violence" (COPA04 p. 70). This time Oxley and other supporters of COPA had additional evidence to back up their assertions that "A child with minimal knowledge of a computer, the ability to operate a browser, and the skill to type a few simple words may be able to access sexual images and content over the World Wide Web" (COPA14 pp. 1-2).

First, Congress relied on a series of Legislative Findings to support their primary diagnostic frame and to emphasize the need for government regulation of the Internet. Within these Findings, Congress recognized that there were many "opportunities for minors to access materials through the World Wide Web in a manner that can frustrate parental supervision and control" and that the "protection of the physical and psychological well-being of minors by shielding them from materials that are harmful to them is a compelling government interest" (COPA17 pp. 13-14). The first point may be a direct response to the opposition's argument that parents should be the first line of defense and should have the ability to decide for themselves what content was or was not appropriate for their children. While Congress agreed that "custody, care, and nurture of

the child resides first with the parent" (COPA01 p. 1), parental involvement was insufficient to stem the tide of "an increasing number of thousands of sites that openly allow children…to see hard-core and soft-core porn pictures" (COPA24 p. 3). Oxley and his supporters believed strongly that Congress must take measures to mitigate this harm at the federal level and show that legislators were "united in protecting our children from pornography over the World Wide Web" (COPA06 p. 1). Representative Oxley himself made what may be the clearest articulation of this legislative diagnostic frame when he asserted that "The ready availability of hardcore pornography to kids on the Web is a problem we need to solve" (COPA07 p. 2). Direct federal intervention through COPA was the means by which "Congress sought to address that serious problem" (COPA17 pp. 33). Only a "national solution" could adequately deal with "the problem of minors accessing harmful material on the World Wide Web" (Id pp. 13-14).

Oxley and his supporters also depended on a Report prepared by Representative Bliley of the Commerce Committee as evidence that unregulated access to the Internet caused grave harm to children.[20] This Report estimated that, as of 1998, "almost 70 percent of the traffic on the Web is adult-oriented material" (COPA21 p. 10). In the absence of federal legislation, and despite parents' best efforts, "minors can move from Web page to Web page, viewing and downloading this material without restriction" (Id). Without some sort of age verification technology to mediate this unrestricted access "children exposed to pornography can become victims or victimizers, encouraged by the strong sexual images contained in pornography found on the World Wide Web" (Id p. 11 Actual). This Report also strengthened the legislative diagnostic frame by providing

[20] Report to Accompany H.R. 3783, Submitted October 5, 1998 to the House of Representatives, 105th Congress (COPA21).

demographic data about both the number of computers connected to the Internet and the number of children who had access to those computers. The problem was even more urgent because these numbers had increased exponentially since the Supreme Court had struck down the CDA. The implication seemed to be that the CDA, had it been enforced, could have addressed minors' access to pornography but, failing that, COPA surely must be enacted now to mitigate any further harm. Unregulated access to the global network was cause for concern and for legislative intervention because, "Since January 1996 (one month before the CDA was enacted), the number of host computers has more than tripled from approximately 9.4 million hosts to more than 29.6 million hosts" (COPA21 p. 9). During that same period, and while the CDA could have been enforced, Congress estimated that the number of children online had increased to about 16 million (Id). Congress' mandate was clear; it must act to mitigate any further harm.

In addition to its Legislative Findings and Report to the House of Representatives, Congress also relied on two major hearings to identify the scope of the problem of unregulated Internet access and to clarify the form that government intervention should take.[21] These hearings were a direct result of the Supreme Court's decision to strike down the CDA and lawmakers sought to create a clear record of Congressional intent and the need for legislative action (Id). Congress held these hearings to stave off any potential criticism that they had not bothered to establish "any detailed findings addressing the problem of distributing indecent materials to minors over the Internet" (COPA21 p. 16). Not surprisingly, for legislative supporters of COPA, both hearings

[21] Cited as "Hearings on H. R. 3783, H.R. 774, H.R. 1180, H.R. 1964, H.R. 3177, and H.R. 3442 Before the Subcomm. on Telecomms., Trade, and Consumer Protection of the House Comm. on Commerce, 105th Cong., 2d Sess. (1998); Internet Indecency: Hearing before the Senate Comm. On Commerce, Sci. and Transp., 105th Cong., 2d Sess. (1998)" (COPA17 p. 13).

seemed to buttress lawmakers' diagnostic frame. From this point of view, testimony from a number of witnesses "highlighted the problem of children getting easy access to pornography and the need for Congressional action to stop the widespread distribution of material harmful to minors" (Id). Nonetheless, the outcome of these hearings was not universally agreed upon and, as the opposition pointed out, neither occurred before Congress finalized COPA's statutory language (COPA23 p. 15). Furthermore, opponents of COPA protested loudly that Congress had not done nearly enough to address the constitutionality of this new policy, its intended scope or its reliance on age verification systems.[22] Although Congress had taken steps toward critical analysis and public review of policy regulating online content, for the opposition, it was by no means certain that they had come to the correct conclusions.

It is interesting to note here that, despite its increased propensity for public hearings, comment, research and review, Congress had still done little to address the efficacy of commercial filtering software. While legislative supporters of COPA did not view voluntary filtering mechanisms as part of the problem, they certainly did not view these systems as part of the solution. The opposition complained loudly about the lack of serious discussion about these products and noted that "The House Commerce Committee's lone panel of non-Congressional witnesses did not include a single technology expert or provide any basis for a detailed examination of the variety of user-control technologies currently available" (COPA23 p. 15). The record established by Congress to support COPA and its diagnostic frame made clear that Oxley and others

[22] "Congress did not create the detailed factual record constitutionally required to support its claim that COPA is the most narrowly tailored means to achieve its intended ends. The Senate held no hearings on COPA, and the House Commerce Committee conducted only a single hearing, mere weeks before the passage of COPA, as part of an Omnibus appropriations bill" (COPA23 p. 15).

took a jaundiced view of filters. In fact, the Report to the House of Representatives stated explicitly that "While blocking and filtering techniques may be effective for many parents, schools, and libraries, the Committee does not believe, however, that they are as effective as the approach taken in H.R. 3783" (COPA21 p. 19). Tangentially, it is important to point out that Congress' position of filtering products would evolve significantly prior to passage of the Children's Internet Protection Act (CIPA). In the context of COPA, Bliley's Report to the House explicitly expressed concern "that a national mandate requiring the use of blocking or filtering could lead to private censorship or inadvertent blocking" (COPA21 p. 19). The Report went on to extol the virtues of age verification systems while, in contrast, minimizing filters as "not the preferred solution" (Id). Bliley lamented the inability of private actors to create software which would mitigate the harms outlined in Congress' diagnostic frame and suggested that reliance on such systems would create a patchwork solution at best. Commercial products would never replace the centralized solutions mandated by federal policy and "industry-led efforts" would never provide "a national or uniform solution to the problem of children accessing harmful material" (Id p. 17). The Report blasted filtering software because it employed a "discretionary means to screen information" which increased the "chance that protected, harmless, or innocent speech would be accidentally or inappropriately blocked" (Id). This criticism is astonishingly similar to the language that the opposition would employ in its campaign against CIPA. As will be discussed at length in Chapter 6, in the interim between COPA and CIPA the two sides would essentially swap positions on the appropriate use and impact of this technological mechanism.

Legislative supporters of this new policy would also, of course, rely heavily on the COPA Commission's report to bolster their definition of the problem. Since Congress did not convene the Commission prior to passage of COPA and the Commission did not release its findings until two years later, it is fair to say that that report did not significantly impact the entrenched diagnostic frame. Furthermore, like the Congressional hearings on COPA, both sides would be able to make inferences from the Commission's final report that supported their point of view. For example, in the case of the legislative diagnostic frame, supporters of COPA would point to the Commission's report as further evidence that unregulated access to the Internet "risks exposing children to sexually explicit material that many believe is inappropriate or harmful" (COPA04 p. 7). In its effort to create a factual record that would demonstrate its careful review of the problem to both the opposition and the courts, Congress was able to point to the various reports, hearings, and Commission findings to reinforce the need for government intervention through policy and through technology. This is, perhaps, one of the key moments in the policy process where criticism and critical review of regulatory systems may be successfully advanced. Following the CDA, Congress made great strides in its commitment to review content regulation policy. While there remained a strong commitment to the legislative master and diagnostic frames, there is also an increased need for evidentiary data and objective testimony. Criticism of both the opposition and the courts forced Congress to create such a record in the interest of completeness and constitutionality. If such a shift can occur within this diagnostic frame, it is not unreasonable to assume that this part of the process can shift even further to include a truly critical review of regulatory systems.

Part IV – Oppositional Diagnostic Frames

While the COPA Commission's final report would provide ammunition to both sides of the debate, based on the evidence it provided the opposition was able to make a powerful argument that this policy, and the technological mechanisms it required, could cause serious harm. The opposition primarily based its diagnostic frames on the argument that centralized, government-mandated technological barriers to access would do damage to both individual autonomy and constitutionally protected speech. What is most striking about this is that, for the first time, the opposition was able to point directly to a congressionally mandated analysis to support its claims.

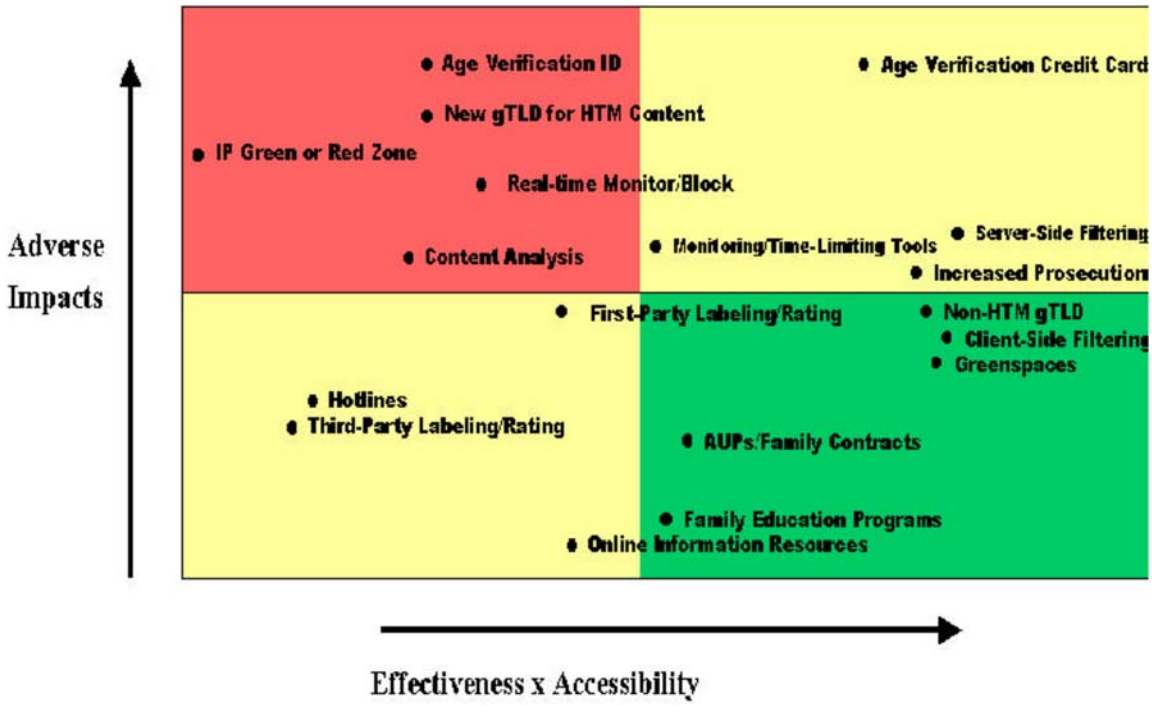
This report was released on October 20, 2000 – nearly two years after COPA was signed into law – and the Commission's purpose was to study "various technological tools and methods for protecting minors from material that is harmful to minors" (COPA03 p. 3). Although explicitly mandated by COPA, the Commission received no federal funding and consisted entirely of volunteers with a wide range of expertise (COPA04 p. 2). Members of the Commission included individuals representing industry, academics, activist groups, and government.[23] Although the Commission did examine some "low-tech" solutions to the problem of minors' access to sexually explicit material such as parental education, the Commission's report primarily dealt with technological mechanisms of enforcement (COPA04 p. 5). These mechanisms included filtering and

[23] The Commission was chaired by Donald Telage of Network Solutions, Inc. and its members included: Stephen Balkam, Internet Content Rating Association; John Bastian, Security Software Systems; Jerry Berman, Center for Democracy & Technology; Arthur H. DeRosier, Jr., Rocky Mountain College; J. Robert Flores, National Law Center for Children and Families; Albert F. Ganier III, Education Networks of America; Michael E. Horowitz, Department of Justice; Donna Rice Hughes, Author, Kids Online/Founder, Protectkids.com; William M. Parker, Crosswalk.com; C. Lee Peeler, Federal Trade Commission; Gregory L. Rohde, Department of Commerce/NTIA; C. James Schmidt, San Jose State University; William L. Schrader, PSINet Inc.; Larry Shapiro, Walt Disney Internet Group; Srinija Srinivasan, Yahoo! Inc.; Karen Talbert, Nortel Networks and; George Vradenburg III, America Online, Inc. (COPA04 p. 2)

blocking software, labeling and ratings systems, age verification systems, domain level "zoning," and various other "technologies or methods" (Id).

Aligned with the opposition's diagnostic frames, the Commission's report was also concerned with the impact that federally mandated technological systems could have on privacy and "First Amendment Values" (COPA04 p. 7). For the first time, a government body plotted these "adverse impacts" (Id) against the effectiveness and accessibility of these systems. This created a mechanism by which the Commission could reduce its findings to a visual representation of the merit of regulatory systems as a function of the harms potentially caused by requiring their use. For the opposition, the results of this analysis provided vindication of the diagnostic frames they had been attempting to advance. The chart created by the Commission (COPA04 p. 8) is reproduced in its complete form below:

Figure 2 – COPA Commission Scattergram



The analysis of each technology examined by the Commission included a review of a number of independent factors including efficacy, practicality, privacy, and impact on protected speech (Id p. 15). These individual scores resulted in an aggregate total ranging from 10 to -10 such as those plotted on the chart above. As this diagram makes clear, the Commission found that the voluntary use of client-side filtering (as advocated by the opposition) was both effective and accessible while minimizing any adverse impacts to user privacy and First Amendment values as defined by the Commission.[24] The verification of age through credit card information, while effective and accessible to a wide number of content providers, was problematic from the standpoint of privacy and free speech. The use of some form of online identification to verify age was neither effective nor widely accessible and was deeply troubling from the standpoint of privacy and constitutional rights. Although Congress was able to bolster its diagnostic frame that unregulated access harmed minors through some of the Commission's conclusions, the opposition had a clear advantage in terms of both the master and diagnostic frames they had employed as they related to autonomy and access. As the Commission would find, technological access controls had the distinct potential to harm individual choice and to reduce access to protected speech.

Although the Commission thoroughly examined a number of methods, those discussed here will only include those advocated either directly through COPA or by the opposition as a counterpoint to this policy. The first, client-side filtering, received relatively high marks for effectiveness and accessibility (scoring a 6.5 and 6.9 respectively) (COPA04 p. 21). The Commission noted that commercial "filtering can be

[24] First Amendment values "refers to impact on overall First Amendment values concerning the free flow of information, rather than narrowly to actions taken by governmental actors" (COPA04 pp. 15-16).

effective in directly blocking access to global harmful to minors content on the Web, in newsgroups, in email and in chat rooms" and that it was "widely available from retail and other outlets" (Id p. 21). This vindicated the opposition's assertion that the voluntary use of commercial filtering products could be at least as effective as centralized, federal solutions and that they would be less intrusive in the process. This also supported the argument that Congress need not sacrifice the autonomy of the individual in the rush to pursue a "national solution" (COPA17 pp. 13-14). Reasonably effective and widely available, filtering software had the distinct benefit of allowing parents to customize these products "depending on the ages of their children and what type of content they find objectionable" (COPA20 p. 72). Personal choice and user empowerment, as advocated by the opposition, had proven to be features apparent in this type of technological system. The Commission specifically found that "many of these [products] can be customized based on family choice" (COPA04 p. 21).

Despite its advantages of efficacy and empowerment, commercial filtering products had adverse impacts as well. Although these systems scored among the highest of any of those rated by the Commission, this aggregate rating is somewhat misleading. In the areas of privacy and First Amendment values, filtering software scored a -2.1 and -1.7 respectively. In findings reminiscent of the cautionary information released by the CDT, the Commission concluded that "This technology raises First Amendment concerns because of its potential to be over-inclusive in blocking content" (COPA04 p. 21). This analysis also echoed legislative criticisms of filtering products that such systems "could lead to private censorship or inadvertent blocking" (COPA21 p. 19). Both sides, it seemed, took issue with this feature of the technology and recognized that it could prove

detrimental to constitutionally protected speech. The Commission was no different and scored these products accordingly. Again, it is interesting to note that, despite negative scores related to privacy and speech, commercial filtering software was one of the best options relative to other technological alternatives examined in the report.

The opposition also advanced a diagnostic frame arguing that technological barriers to access could cause harm by unnecessarily introducing a level of opacity to the user. This could damage individual rights because trade secret protected blocking criteria in the context of commercial products and manufacturers were under no obligation to make those criteria transparent to the user. It was standard practice that these companies would "not disclose the standards under which they filter or the list of filtered sites" (COPA11b p. 13). The Commission essentially concurred with this assessment and noted that constitutional "[c]oncerns are increased because the extent of blocking is often unclear and not disclosed" by filtering manufacturers (COPA04 p. 21). This diagnostic frame ties directly to the opposition's call for an extended and critical review of any regulatory systems prior to their implementation – especially if that implementation occurred as a direct result of government fiat. The Commission would go on to endorse this point of view as well noting that its mandate, limited scope, and lack of funding were inadequate in this regard. Instead, the Commission "discussed the need for an independent, non- governmental testing facility for child-protection technologies" that would delve into both "search criteria" and "transparency" (COPA10d p. 27). This also touches on the issue of hegemony if private, commercial notions of acceptability mediated access to content without the opportunity for comment or review. As the opposition noted, this could well be the case if individual choice was "replaced by the

decisions made by private companies — many of which are shut off from public scrutiny due to lack of disclosures about the process or guidelines for blocking sites" (COPA11b pp. 13-14). As the opposition made clear, and as the Commission's findings seem to support, any delegation of individual autonomy "to unchecked private entities raises troubling First Amendment issues" (Id). Although Congress had made a step in the right direction by requiring formation of the Commission, from the opposition's perspective, an urgent need remained for critical and sustained review of these technological mechanisms.

The primary affirmative defense offered under COPA was the use of age verification systems. Specifically, COPA provided immunity for those commercial content providers who restricted access "by requiring use of a credit card, debit account, adult access code, or adult personal identification number [or] by accepting a digital certificate that verifies age" (COPA02 p. 2). The Commission dealt with this regulatory scheme as well and their findings appear to justify the opposition's diagnostic frames. In the case of age verification through credit card data, the Commission found that this technology was both effective and easily accessible (COPA04 p. 25). This lent credence to the government's assertion that the use of such systems was already "standard practice" (COPA21 pp. 14-15) among commercial pornographers and that the proprietors of most adult websites "already put most of their material behind age verification screens" (COPA17 p. 47). Although supporters of COPA had argued that age verification was the "most effective" means of mediating access, they had also argued that it was the "least restrictive approach that should be taken given the current state of the technology" (COPA24 pp. 2-3). Here, the Commission sharply disagreed.

First, the Commission found that it "may be difficult or burdensome for small or non-commercial sites to implement card verification systems" (COPA04 p. 25). The opposition had made a similar argument for one of its key diagnostic frames. Specifically, oppositional groups had suggested that "[m]any of the entities likely to be affected by the bill are unable to make use of the age verification techniques that comprise the affirmative defenses due to cost and/or availability" (COPA11b p. 12). The burdensome nature of these systems would have the effect of chilling speech *a priori* due to the inability of speakers to meet the costs incurred through this affirmative defense. Both the Supreme Court and the District Court had made a similar argument in their rulings on the CDA noting that "even many commercial organizations using the Web would find it prohibitively expensive and burdensome to engage in the methods of age verification proposed by the government" (CDA13 p. 39). The Commission went on to give these systems a rating of -5.2 noting that the "Adverse impacts on First Amendment values result from cost to publishers and chilling effect of identifying users before providing access" (COPA04 p. 26).

Although the Commission's report does support the government's definition of the problem and concurs with the assessment that unregulated access to the Internet can harm children, its findings also directly contradict Congress' means for addressing that problem. By detailing the constitutional and ethical deficiencies of age verifications systems and even commercial filtering software, the Commission had done a great deal to support the opposition's arguments. To preserve user autonomy and access to constitutionally protected speech, Congress should not implement technological mechanisms of enforcement such as these without a great deal of care and consideration.

Part V – Legislative Prognostic Frames

Oxley and other supporters of COPA did not respond directly to the Commission's criticisms of age verification technologies, nor did they need to. Due to the fact that the findings were not issued until two years after Congress had passed the policy and President Clinton had signed it into law (COPA03 p. 3), there was no possibility that lawmakers could change this central technological requirement of COPA so long after the fact. The legislative prognostic frame remained in place and Congress argued that only a centralized solution mandating age verification systems could address the harm done to minors by unregulated access to the Internet. All that was left now was to defend that solution as the best and most effective option at the government's disposal. Age verification screens, lawmakers argued, were the only possible solution to the problem because they mediated access to content at the source. As Congress continued to argue, "it is more effective to screen the material prior to it being sent or posted to minors, and that such a restriction imposes minimal burdens on adults" (COPA21 p. 16). This kind of access control was best because "It is always more effective to lock the barn door before the horse is stolen" (Id).

As mentioned previously, Congress saw age verification technology as the most effective and least restrictive mechanism at their disposal because the use of such systems was already "standard practice among some commercial distributors of pornography on the Web" (COPA21 pp. 14-15). This demonstrated, unlike the technologies required by the CDA, that age verification systems were both "technologically and economically feasible" (Id p. 13). Widespread use of these systems seemed to prove that point and COPA did no more than "reorder the process in such a way as to require age verification

before pornography is made available" (Id pp. 14-15). Furthermore, for content providers, economic barriers to entry were relatively low in comparison to those regulatory systems required by the CDA. In fact, some age verification systems provided their services to websites for free. For example, Congress noted that Adult Check offered, "at no cost to a Web site operator, a screen that can be used to block access by minors" (COPA17 pp. 19-20). This, combined with the policy's focus on commercial content, did much to address the courts' previous concerns that the costs associated with regulatory technologies would cause a number of individual and non-profits speakers to remain silent. Age verification was a proven technology that offered a number of advantages over other regulatory systems. This mechanism was easy to use, prevalent and would not significantly impact the economic ability of content providers to make their material widely available. In fact, because COPA required content providers to place all prohibited content, including teasers, behind these screens, Congress argued that age verification would bring in even more money due to the prerequisite that customers pay prior to seeing any illicit images at all. This fact made it "not only economically feasible for commercial content providers to comply with the bill, but profitable for them to do so" (COPA21 pp. 14-15).

Supporters of COPA again pointed to the narrowed focus of COPA as proof of its minimal impact on the right of adults to access constitutionally protected speech. Even the pornographic industry's trade association had endorsed age verification systems and, because these commercial providers would be the only websites affected by the law, this solution was both "effective and appropriate" (COPA24 p. 30). Mandating the use of such a "screening process" was the only sensible answer and Congress could enforce

COPA "Without diminishing free speech" (COPA06 p. 1). COPA's supporters argued that the constitutionality of such age verification systems was self-apparent because they were already in wide use across the pornography industry. By the government's estimate there were already "approximately three million people [that] possess a valid" adult ID number and some "46,000 Web sites accept them" (COPA17 pp. 19-20). Applying for such an ID and paying the cost would, at worst, impose "a modest burden on adult access to pornographic material" (Id p. 26). In the context of the legislative prognostic frame, that burden imposed by age verification technologies would be "outweighed by the government's compelling interest in shielding minors from material that is harmful to them" (Id).

Congress consistently emphasized the minimal financial burden associated with age verification systems. Again, the benefits of the solution provided by these systems were preferable to any costs that might result from requiring their use. Perhaps in response to the COPA Commission's report and almost certainly as a reaction to the Supreme Court's ruling on the CDA, Congress emphasized that adult ID numbers could be purchased for "less than $20 per year" and because "millions of adults had purchased" them already, no constitutional harm seemed to be implicated (COPA17 p. 26). Supporters of COPA argued that any criticism suggesting that a chilling effect would result from placing speech behind fee-based barriers was alarmist and hypothetical at best. From this point of view, the opposition's arguments on this point were only supposition that age verification services "may deter" adults from accessing speech and "may affect" some content providers' ability to speak (Id pp. 19-20). With no direct proof that this regulatory scheme would hinder access to protected speech and with a

wide variety of such systems already in place, COPA's supporters felt confident that the concerns of the opposition and the Commission were unfounded.

COPA's supporters also waved away any privacy concerns raised by the opposition in relation to Congress' preferred technological solution. Specifically, the Commission found that the adverse impacts of these systems on personal privacy "could be high" (COPA04 p. 27) due to the "[c]ollection of individually-identifiable information at central points via this system" (Id p. 25). Although the Commission had scored age verification systems quite low in this category (-4.5 for credit card based systems and -5.5 for adult IDs) (Id pp. 25 & 27), Oxley and others argued that the bill would account for this by limiting the "use and disclosure of personal information collected by those who provide credit-card or adult verification systems" (COPA11c p. 22). These statutory protections for personally identifiable information would remove "disincentives to obtaining an Adult ID by requiring that information collected in that process must be kept confidential" (COPA17 p. 49). Again, these "significant privacy protections" and the fact that "millions of adults have had no difficulty in obtaining and using Adult IDs" bolstered the constitutionality of this provision and the prognostic frame it represented (Id). If some adults felt "reluctance…to obtain an Adult ID" this, in itself, did "not render COPA unconstitutional" (Id).

This conclusion was contradictory to both the Commission's findings and to the opposition's arguments. Support for COPA on this point also did not account for those who would choose not to submit information to age verification services due to the perceived stigma of accessing material that the system had walled off as "harmful to minors." The Commission had made passing reference to an "embarrassment effect"

(COPA04 p. 27) related to this phenomenon and the opposition had specifically noted that "in light of concerns about privacy on the Internet, COPA's requirement that all sites offering any material that may be unsuitable for children must verify their users' ages will discourage adults from accessing material that is appropriate for them" (COPA10e p. 39). From the opposition's perspective, any "[r]eliance on such systems will create records of individuals' First Amendment activities" and an unacceptable hindrance on the individual's willingness to seek out such content (COPA11b p. 12).

The constitutionality of COPA's technological requirements was also self-apparent because it was a natural extension of existing "display laws." These laws placed any magazines, videos or other material deemed "harmful to minors" out of view of children. The appeal to physical analogs of content regulation was comfortable for Congress and made for a compelling argument in this new and uncharted regulatory terrain. Access controls would protect children online just as they had in real world situations and Congress had simply "adopted the same basic approach for the Web that States have adopted for local stores" (COPA17 pp. 33-34). This was not an outright ban on such material and did not hinder the right of adults to access it. Instead, COPA "simply requires that the same kind of material that States require to be placed behind blinder racks must be placed behind adult verification screens" (Id). Similar to the physical metaphors that had underpinned calls for the CDA, here Oxley and others made the case that COPA did not ban teasers or any other pornographic material and did not persecute those seeking it out. Legislators were simply ensuring that content providers put the online equivalents of dirty magazines "behind the counter" (Id). This was both common sense and a necessary technological extension of common decency.

Part VI – Oppositional Prognostic Frames

For the opposition, the solution to the problems presented by COPA and its age verification requirements necessitated that Congress minimize such access controls or remove them entirely. The opposition argued that such systems were so intrusive and so damaging to constitutional rights that lawmakers must scale back on their use or do away with them entirely. Failing that, the courts should strike down COPA and should find its technological enforcement mechanisms unconstitutional. The criticisms of COPA's shortcomings and its affirmative defenses were, like the policy's technical requirements, extraordinarily reminiscent of the CDA.

From this point of view, the law's affirmative defenses did not remedy COPA's constitutional deficiencies for a number of reasons. First, COPA's requirement that adults provide credit card information as a surrogate for age would "prevent many users from accessing" websites that contained constitutionally protected speech (COPA02 p. 3). Second, the requirement that individuals obtain an adult identification number was not only burdensome but could dissuade many adults from seeking out this content at all if they must "disclose their identity in order to access protected speech" (COPA09d pp. 10-11). Third, "use of a credit card will place substantial economic burdens on the web originator" (Id). Therefore, despite assertions to the contrary, even a minimal charge to the content producer was an onerous and unconstitutional precondition for speaking online. While Congressional supporters of COPA had painted a rosy picture of free or low cost age verification systems and increased profits for website owners, the opposition argued that any cost "would impose significant residual or indirect burdens upon Web publishers" (COPA15 pp. 12-13). In the face of these burdens, both content providers

and content consumers faced an unpleasant and potentially unconstitutional dilemma. As the CDT put it, the law posed a "Faustian choice to individuals seeking access to information – protect privacy and lose access or exercise First Amendment freedoms and forego privacy" (COPA11b p. 12). For the opposition, the government could not mandate age verification systems and protect the First Amendment. These access controls, as applied, were inherently unconstitutional and Congress could only solve any problems presented by COPA by foregoing their use.

Again, the COPA Commission's report tended to support this prognostic frame. The Commission found that no technology, even the age verification systems required by COPA, "could adequately serve as an affirmative defense in a manner respectful of the First Amendment" (COPA04 p. 65). Lawrence Lessig, who provided expert testimony to the Commission, concurred with this assessment and noted that age verification schemes were unlikely to pass constitutional muster (COPA05 p. 2). Just as the opposition had argued, Lessig suggested that age verification systems could not be implemented constitutionally because the "burden on adults to carry age-identification is significant; the burden on sites to verify the identification presented is also high" (Id). In fact, the Commission went a step further than the opposition and suggested that *any* technological barriers to access "may have the effect of restricting speech" and "even voluntarily implemented" systems "reduce access to fully protected speech" (COPA04 p. 13). Where the opposition had suggested (albeit with increasing skepticism) that the voluntary use of commercial filtering software would be preferable to the mandated use of age verification systems, the Commission found that "no single technology or method will completely protect children from harmful material online" and remain constitutional in

the process (COPA03 p. 1). Lessig again agreed with this assessment and argued that filtering software, especially if it were to be mandated at the federal level, was "inherently flawed" and would "facilitate a far greater blocking of access to material than the government's legitimate interests reach" (COPA05 p. 2). The state's own findings in this area, through the Commission, buttressed the opposition's prognostic frames. Lawmakers' had to minimize the use of centralized, governmentally-mandated enforcement mechanisms in the interest of both children and the constitution.

The solutions proposed by the COPA Commission were also supportive of those offered by the opposition. While the Commission remained unconvinced of the efficacy of commercial filtering software or any other regulatory system, they agreed with the opposition that low-tech or no-tech options were an important component of any eventual resolution. Again, the opposition had suggested that Congress must revise laws like COPA or that the courts should strike them down entirely if they imposed broad technological barriers. Rather than "passing criminal laws for the Internet" lawmakers should "focus instead on educating users to make their own choices about what content to view or avoid" (COPA09a p. 5). While centralized technical mechanisms would almost invariably function unconstitutionally, the opposition and the Commission argued that education programs would greatly assist both parents and children – ostensibly the two groups who were to benefit most from COPA. The Commission agreed that, while these "family education programs do not themselves directly prevent minors' access to harmful to minors materials…they are an essential part of an overall solution" (COPA04 p. 18).

As noted previously, the Commission had called for further study of filtering software, age verification systems and other regulatory technologies (COPA04 p. 15).

Some members had further requested that Congress extend the Commission's mandate to provide a greater depth of analysis (Id p. 78). This recognition that more significant and extensive review of technology should take place supported the opposition's continued calls for a critical analysis of regulatory systems prior to their inclusion in federal policy. In any solution, there must be a "comparison of the effectiveness of various approaches, their likely impact on speech, and their appropriateness for the Internet" (COPA11b pp. 12-13). While Congress had made some progress in this area by forming the COPA Commission, much work remained to be done. As one member noted, legislators had been deficient in this area and the Commission "has done what Congress has not – it has examined how to protect children online in ways consistent with the Internet's architecture and Constitutional requirements" (COPA04 p. 64). For the opposition, it was also telling that the Commission's report, as "the most thorough and searching analysis" (COPA27 p. 25) of COPA's requirements, disagreed so fundamentally with some of Congress' core assumptions about the policy, the technology and the constitutionality of both. Congress had undergone a frame shift by acquiescing to calls for more research but had negated that shift by essentially ignoring the results. Due to this, the opposition argued that while the Commission's report "served as a substitute for congressional findings," Congress erred by passing "COPA without creating the detailed factual record constitutionally required to support its claim that COPA is the most narrowly tailored means to achieve its intended ends, and without adequately considering less restrictive approaches" (Id). In the absence of such a record, and in the face of evidence to the contrary, Congress continued to push for COPA's passage and insisted on the constitutionality of its technological requirements.

Finally, the opposition's prognostic frame demanded that, if Congress did not heavily revise the law and remove or minimize access controls, the court should strike COPA down entirely. Oppositional groups insisted that the profound similarities between the CDA and COPA made the law incontrovertibly unconstitutional. While Congress had made alterations to the policy, it had not done enough to address the core problems at the heart of the law – problems that had carried over from the CDA. The opposition based the call for a permanent injunction against COPA and its technological affirmative defenses on five key principles. First, age verification systems would deny adults the right to access constitutionally protected speech if they did not possess a credit card (COPA12 p. 3). Second, the law extended to a great deal of speech that the constitution protected. For example, chat rooms where only a portion of the conversations could be considered offensive would all be locked "behind verification screens, even speech that is not 'harmful to minors'" (COPA22 p. 10). Third, adults would be discouraged from even attempting to access protected speech because the technological mechanisms of enforcement would "impose costs on content that would be free, eliminate privacy, and stigmatize content" (COPA12 p. 3). Individuals antagonistic to certain speech or hostile to certain viewpoints could potentially exercise a heckler's veto and force websites to employ age verification systems if they could have the offending website's content declared harmful to minors (Id). Fifth, COPA's affirmative defenses "impose financial burdens on speakers that will cause them to self-censor rather than incur those burdens" (Id). Due to this, the opposition felt it was self-apparent that the courts should find COPA unconstitutional and strike this law down as soon as possible.

The opposition went on to question the efficacy of any government intervention into online speech. Both the CDA and COPA had, to the opposition, demonstrated an extreme tendency for legislative overreach, ignorance about the technical provisions required by these federal policies and a misunderstanding of the medium itself. On these points, the opposition shared a "common concern about the threat…posed by ill-considered, ineffective, and unconstitutional government regulation of the Internet" (COPA18 pp. 10-11). The ACLU in particular was outspoken on these shortcomings and wearily argued that Congress should "end wrongheaded attempts to regulate the unique medium of the Internet" (COPA09c p. 8). They called on lawmakers and the administration to "close the book on this early chapter of Internet history and embrace free speech online" (Id). Again, the similarities between the CDA and COPA made Congressional attempts to regulate an unfamiliar medium with unfamiliar regulatory systems ripe for a constitutional challenge. From the ACLU's point of view, it did not matter "[w]hether you call it the 'Communications Decency Act' or the 'Congress Doesn't Understand the Internet Act,' it is still unconstitutional" (COPA09f p. 21). Any law should be struck down if it "bans a wide range of protected expression" (Id) that is otherwise available online and "Congress' attempt in COPA to remedy the fundamental defects in the Communications Decency Act…is unavailing" (COPA18 p. 13). Without more significant shifts in the scope and enforcement of policies like the CDA and COPA, the result would be the same. For the ACLU and other oppositional groups that was clearly the case here. From this perspective, the "constitutional flaws in this law were identical to the flaws that led the Supreme Court to strike down the Communications Decency Act" (COPA09 p. 1).

Validation for this prognostic frame would again come from an unlikely source. Although Congress had formed the COPA Commission in an effort to bolster the government's credibility in the area of online regulation, the Commission's findings continued to be problematic for COPA's supporters. Several of the Commission's members shared the opposition's distrust of federal policy attempting to regulate content online and were unconvinced that technological mechanisms of enforcement could ever function constitutionally. One Commission member emphasized the unique nature of this new medium and, like the opposition, questioned the viability and constitutionality of attempts to regulate it (COPA04 p. 64). Perhaps unsurprisingly, this member was Jerry Berman, head of the Center for Democracy and Technology (CDT) – one of the key groups opposed to both the CDA and COPA. In this instance he also spoke for other members and noted that the "Commission rejects a legislative approach to protecting children…because laws restricting distribution of or access to harmful to minors materials are Constitutionally suspect" (Id). Other members of the Commission shared this view and they echoed the opposition's call for limitations on governmental intervention on the Internet. William Schrader, CEO of PSINet, Inc. and member of the Commission agreed that COPA was "deeply flawed" (COPA04 p. 84). Schrader believed, "like several other members of the Commission, that the restrictions on speech enacted into law by COPA are unconstitutional" and it was impractical for Congress to assume a solution could be found by "legislating our way out of the problem" (Id). It appeared that this vindicated the opposition's calls for a more critical analysis of this policy because Congress' own Commission on these issues had found that many of the opposition's fears were legitimate.

Part VII – Judicial Opinion

COPA would go on to traverse a torturous path through the courts. Although the opposition filed the original complaint in October of 1998 – within hours of the President signing COPA into law – final adjudication did not come until 2007. For nearly ten years, COPA languished in the judicial system, passed from District to Supreme Court and back again. Due to a preliminary injunction that no court ever lifted, Congress never enforced this policy during the decade it was on trial. Eventually, on March 22, 2007, the judiciary finally issued a permanent injunction against COPA, essentially killing the legislation (COPA02 p. 3). Despite COPA's failures, the government was able to advance several arguments that would become important to future legislation as well as to the future of content regulation on the Internet. The fact that COPA took so long to defeat demonstrates that Congress had undergone enough of a frame shift after the CDA and had undertaken the minimum amount of critical review necessary to fend off the opposition's arguments for years. Where the courts struck down the CDA quickly and unanimously, COPA would sharply divide District Court judges and Supreme Court justices alike, setting the stage for the Children's Internet Protection Act that would soon follow.

Filed in the Eastern District of Pennsylvania, the same venue where the CDA's litigation began, the opposition's complaint represented a number of interests including those of the ACLU, EFF, and Electronic Privacy Information Center (EPIC). In addition to these activist groups, the opposition filed the complaint on behalf of a "broad range of individuals and entities who are speakers, content providers, and users of the Web" including "online magazines, booksellers, media companies, art vendors, and gay and

lesbian content providers" (COPA13 p. 2). The opposition's argument was clear; COPA "directly violates the First Amendment rights of plaintiffs, their members, and tens of millions of other speakers to communicate protected expression on the Web. In addition, the Act violates the rights of millions of Web users to access and view constitutionally protected speech" (Id). Specifically, they argued that COPA's technological requirements prohibited a multitude of speakers and listeners from pursuing constitutionally protected activities online. The age verification systems that the government had put such faith in were neither "technologically or economically available to plaintiffs and other providers of free content on the Web" (COPA13 p. 12). Even if such systems were technologically practical or economically feasible they would, the opposition argued, destroy the vast democratic forum created by the Internet and squander the potential of this new medium. COPA's primary technological enforcement mechanism "would fundamentally alter the nature and values of the new computer communication medium, which is characterized by spontaneous, instantaneous, albeit often unpredictable, communication by hundreds of thousands of individual speakers around the globe, and which provides an affordable and often seamless means of accessing an enormous and diverse body of information, ideas and viewpoints" (Id). These arguments are nearly indistinguishable from those offered during the CDA litigation and, from the opposition's point of view, no deviation in the argument was strictly necessary. Since the technological requirements of both laws were "nearly identical" (COPA16 p. 28), the opposition "welcome[d] the opportunity to demonstrate to the Court that Congress has once again fundamentally misunderstood the nature of the Internet" (COPA09e p. 12).

The District Court would go on to concur with the opposition's master frame that access to constitutionally protected speech must be safeguarded and the diagnostic frame that technological access controls would reduce access to that speech. The court would find that "the First Amendment was designed to prevent the majority, through acts of Congress, from silencing those who would express unpopular or unconventional views" (COPA14 p. 1). COPA, through its technological age verification requirements would undermine this protection and these "unconventional speakers" would be "limited in their ability to promote such speech in the marketplace [of ideas] by the costs or logistics of reaching the masses" (Id). The District Court would also defend the legislative master frame that the government had a compelling interest in protecting children (COPA14 p. 22) and the diagnostic frame that unregulated access to the Internet could harm minors. They noted that the "ease of participation and diversity of content and speakers" make the Internet "a potentially harmful media for children" (Id).

Despite this, the judicial endorsement of these legislative frames did not, in the District Court's opinion, save COPA as constitutionally valid. Although the government had argued that the narrowed scope of enforcement and focus on commercial speakers would ameliorate the deficiencies that had doomed the CDA, the court did not agree. Instead, any website that relied on advertising or sales in any way would be subject to COPA and the burdens associated with age verification systems. Even if these sites conveyed valuable information, that material could conceivably be considered "harmful to minors" and locked away behind age verification screens. The court found that "nothing in the text of COPA…limits its applicability to so-called commercial pornographers only" (COPA14 p. 6) and its restrictions could extend to content including

"resources on obstetrics, gynecology, and sexual health; visual art and poetry; resources designed for gays and lesbians; [and] information about books and stock photographic images offered for sale" (Id pp. 10-11).

The court would also find that the opposition's arguments regarding individual autonomy and user privacy were constitutionally valid and that COPA's requirements were far from the least restrictive means by which the government could achieve its compelling interest. Particularly where information sought by the individual may have been sensitive, COPA had the likelihood of discouraging users from seeking out that information. For example, individuals were less likely to search for content on sexual health and orientation if they could not have "access to this information while preserving their anonymity" (Id p. 12). Overall, COPA's technological requirements "would have a negative effect on users because it will reduce anonymity to obtain speech and reduce the flow experience of the user, resulting in a loss of traffic to Web sites" (Id p. 18). Therefore, as the opposition had argued, COPA would irreparably harm the autonomous ability of the individual to seek out and access constitutionally protected speech.

Based on all of these arguments, the District Court upheld the opposition's initial request for a preliminary injunction against COPA because there was a "substantial likelihood…that COPA imposes a burden on speech that is protected for adults" (Id p. 22). While the judge expressed "personal regret that this preliminary injunction will delay once again the careful protection of our children" he acknowledged the necessity of the court's findings and the "greater good such duty serves" (COPA14 p. 26). In a final thought, the judge took up the opposition's argument that the protection of speech should take priority, especially in this new medium. Without such safeguards, he suggested that

laws like COPA might do more harm to "the minors of this country…if First Amendment protections, which they will with age inherit fully, are chipped away in the name of their protection" (Id).

Where the District Court had found COPA constitutionally offensive because it would repress speech and invade personal privacy, on appeal the Third Circuit found against this policy for a different reason entirely. The Court of Appeals would go on to argue that the policy's "harmful to minors" standard was unconstitutionally overbroad (COPA02 p. 2). Oxley and other legislative supporters of COPA had relied on this language precisely because they felt it would mitigate the overly broad enforcement that would have resulted from the CDA's vague "indecency" standard (COPA17 p. 52). The Court of Appeals, however, argued that COPA's proscription against content was equally unclear and would have the effect of chilling a great deal of speech *a priori*. Specifically, because the definition of what exactly constituted material "harmful to minors" was measured by "contemporary community standards" (COPA15 p. 5), it would force speakers online to tailor their speech to the most conservative community standard in the country without knowing precisely what that meant. While some communities may have found some speech entirely appropriate for minors, that material could still be locked away behind age verification screens in other locations. This scheme was especially troubling to the court because it employed a local standard to judge content potentially intended for a global audience. For this reason, the Court of Appeals upheld the injunction noting that:

> "Because material posted on the Web is accessible by all Internet users worldwide, and because current technology does not permit a Web publisher to restrict access to its site based on the geographic locale of each particular Internet user, COPA essentially requires

> that every Web publisher subject to the statute abide by the most restrictive and conservative state's community standards in order to avoid criminal liability" (COPA15 p. 5).

This was strongly reminiscent of the opposition's argument that Congress simply did not understand that which they were attempting to regulate. The nature of the Internet as a decentralized medium and its potential as a vast democratic forum were foreign territory by regulatory standards. The opposition had argued again and again that Congress had demonstrated a "fundamental misunderstanding of the reach of COPA" (COPA20 pp. 67-68) and any critical "understanding of the scope and diversity of these technologies makes plain the unconstitutionality of COPA" (COPA23 p. 12). In this case, the Court of Appeals would agree.

At this point, the case advanced to the Supreme Court but the Justices would essentially punt the case back to the Court of Appeals. As the Supreme Court would rule, it was incumbent on the Third Circuit to review the merits of the case more thoroughly prior to detailed review by the Supreme Court (COPA19a p. 2). It is interesting to note that the Supreme Court did not agree entirely with the Court of Appeals' rationale for upholding the injunction. Instead, the Court found that COPA's reliance on community standards to define "harmful to minors" content "does not by itself render the statute substantially overbroad for First Amendment purposes" (Id). The Court's rationale for this assertion is, to say the least, novel. In his Opinion, Justice Thomas argued that relying on community standards to judge the merit of content in a global medium was neither overly restrictive nor unreasonable. Thomas argued that, in any hypothetical jury trial on the merits of disputed content, "community standards" would by no means imply that local mores would rule the day. Specifically, Thomas reasoned "that community

standards need not be defined by reference to a precise geographic area" (COPA19 p. 12). In this way, the courts could instruct jurors in any locality to apply a broader standard that would account for more broadminded tastes. Additionally, because COPA narrowed the amount of content that the law affected, Justice Thomas found that the "harmful to minors" standard was sufficiently tailored to avoid constitutional overbreadth (COPA19 p. 14). Setting aside the assumption that a jury trial on each and every item of disputed content would not be burdensome, the Court's logic is somewhat confounding. If juries need not apply community standards to a specific geographic location, then why apply community standards at all? Furthermore, this would in no way ameliorate the confusion over what local standards would apply to globally distributed content. How could a content provider attempting to comply with COPA know if any particular jury would be applying conservative community values or a more amorphous, geographically indistinct set of standards? The Court's lack of clarity on these points may indicate that they too were unsure of how to proceed in this new medium while still protecting children from potentially harmful content.

Following this, COPA would be passed back to the Court of Appeals by the Supreme Court. The Third Circuit would uphold the preliminary injunction and send the case back to the Supreme Court who would also uphold the injunction. From there, the Supreme Court remanded the case to District Court for a full trial on the merits of the case. The Supreme Court intended the trial to "(1) update the factual record to reflect current technological developments, (2) account for any changes in the legal landscape, and (3) to determine whether Internet content filters are more effective than COPA or whether other possible alternatives are less restrictive and more effective than COPA"

(COPA02 p. 2). The results would prove to be interesting from the standpoint of both the legislative and oppositional frames prevalent throughout the debate over COPA.

The District Court's final adjudication would support the opposition's arguments almost entirely. In an 84 page opinion that meant the end for COPA, the court would rule that this policy, through its technological enforcement mechanism, would burden both speakers and listeners online. In the interest of safeguarding constitutionally protected speech in a manner consistent with the opposition's master frame and because age verification systems would harm those rights so significantly, COPA's key provisions could not be enforced. Specifically, the "utilization of [age verification] devices to trigger COPA's affirmative defenses" (COPA20 pp. 67-68) would "deter most users from ever accessing" websites with content some found distasteful (Id p. 54). This also had the direct effect of excluding individuals who did not possess a credit card which would "unduly burden protected speech in violation of the First Amendment" and "unconstitutionally chill free speech" (Id p. 67).

The law's technological affirmative defenses were also harmful to individual rights and autonomy because they would diminish the user's ability to protect his or her privacy. Subjecting individuals to the "age verification process would lead to a distinct loss of personal privacy" and "users are especially unlikely to provide a credit card or personal information to gain access to sensitive, personal, controversial, or stigmatized content on the Web" (Id p. 55). COPA discouraged individuals from participating online simply by requiring the disclosure of personally identifiable information and thus chilled speech preemptively. Due directly to COPA, individuals would refrain from speaking

simply because they were "unwilling to reveal personal and financial information in order to access content" (Id p. 67-68)

COPA would harm online content providers due to the loss of traffic from those who did not wish to access controversial websites (Id p. 54). Due directly to COPA's technological mandate the law "would lead to a significant loss of users" (Id). The threat of COPA's regulatory systems would force content providers to "either self-censor, risk prosecution, or shoulder the large financial burden of age verification" (Id). COPA also had the potential to act as a hegemonic control on the content of speech by essentially approving of some content while locking away other points of view. The law would force website operators to prove that their content was both lawful and acceptable under COPA's broad definitions. Specifically, COPA "raises serious constitutional difficulties by seeking to impose on the [content producer] the burden of proving his speech is not unlawful" (Id p. 67-68). Furthermore, because COPA's affirmative defenses were not entirely bulletproof, website owners may not find out that the law disallowed content they provided until they had run afoul of the law. The court argued that, in this sense, "Under the COPA regime, Web site operators are unable to defend themselves until after they are prosecuted" (Id). For all of these reasons, the court found that neither COPA's technological requirements nor its narrowed focus on commercial speakers were constitutionally sufficient. The nature of age verification systems and the distributed nature of speech on the web extended the reach of COPA beyond that which was legally acceptable (Id).

Finally, the court found that the voluntary use of commercial filtering software was preferable to and less restrictive than the mandated use of a centralized content

regulation scheme. By imposing "selective restrictions on speech at the receiving end rather than universal restrictions at the source", filtering products would "not condemn as criminal any category of speech" (COPA20 p. 69). As the opposition had argued, filters were more protective of speech and individual autonomy and, therefore, "more effective than COPA in furthering Congress' stated goal" of protecting minors (Id p. 72). This argument would open the door for the Children's Internet Protection Act and the court here essentially invited the government to enact "programs to promote the use of filtering software" (Id p. 70).

The opposition had successfully made its case and the courts constitutionally validated the master, diagnostic and prognostic frames they had presented. Individual autonomy and access to protected speech must take precedent in any effort to protect children, especially in this new, decentralized medium. The technological access controls required by COPA would harm that autonomy and would have the direct effect of reducing access to speech. Due to this, Congress must review the policy's technological requirements more critically, minimize them in order to better account for these rights, or remove them entirely. Despite the legislative frame shifts that COPA represented, these modifications were insufficient in the face of the law's remaining constitutional defects. The law's more narrow focus on commercial content providers, its reliance on a slightly less onerous "harmful to minors" standard and its mandated use of age verification systems that were ostensibly already in use all failed to meet the constitutional, democratic and ethical threshold necessary for sound policy.

Table 6 – Child Online Protection Act Frame Analysis Summary

Frames	Legislative Themes
Master (Motivation)	• Due to the constitutional failure of the CDA, children remained at risk when online. • While the protection of children remained a compelling interest of the state, legislators expressed some recognition that they should protect speech in the process. • However, the core belief that the state must protect children remained and the master frame itself was inflexible. Legislators were not significantly open to a critical review of technology.
Diagnostic (Problem)	• Congress continued to maintain that it must act because unregulated access to the Internet caused continuing harm to children. • However, due to the opposition and Supreme Court's position on the CDA, COPA did narrow the focus of enforcement to the primary cause of that harm. Specifically, it targeted commercial content providers. • Again, the diagnostic frame remained essentially unchanged and was not open to significant debate. However, Congress did require the formation of the COPA Commission to study the technological enforcement mechanisms required by the Act.
Prognostic (Solution)	• Congress remained convinced that technological barriers to access, including age verification systems, remained the best "tool" for solving the harm of minors' access to inappropriate content. • Congress largely ignored the COPA Commission's report and the results were not available until after they had passed COPA. • Despite some indications that lawmakers were open to a critical review of regulatory technologies, their primary technological solutions remained largely unchanged and unexamined.

Frames	Oppositional Themes
Master (Motivation)	• COPA did not represent a meaningful improvement over the CDA and continued to prohibit access to a great deal of protected speech. • Centralized content regulation disempowered parents and reduced autonomy. • Just as with the CDA, the opposition insisted that autonomy, freedom, and constitutional guarantees should not be constrained through use of regulatory systems and that Congress must consider this potential prior to implementation.
Diagnostic (Problem)	• Despite the narrowed focus of enforcement, COPA's regulatory systems remained an illegitimate constraint on adult access, parental empowerment, and user autonomy. • COPA and its age verification technologies would extend beyond commercial content providers and restrict a great deal of constitutionally protected speech.
Prognostic (Solution)	• Like the CDA, Congress would apply the technological mechanisms required by COPA too broadly and would damage constitutional freedom and individual autonomy. • The solution offered by the opposition was to consider no-tech or low-tech alternatives or, failing that, have COPA struck down as unconstitutional by the courts. • If Congress must impose regulatory systems, they should be voluntarily and should empower parents to choose material they deemed appropriate for their children.

Child Online Protection Act Documentation Index

COPA01	Child Online Protection Act of 1996, (COPA), Pub. L. No. 105-277 (Tit. XIV), 112 Stat. 2681 (Oct. 23, 1998), codified at 47 U.S.C. § 231.
COPA02	Liberty Counsel. (2007). Child Online Protection Act. Retrieved from http://www.lc.org/profamily/copa.pdf
COPA03	Dittus Communications. (2000). Commission on Online Child Protection (COPA) Unveils Final Report to Congress [Press Release].
COPA04	Commission on Child Online Protection (COPA) Report to Congress, October 20, 2000.
COPA05	Lessig, L. (2000, August 6). *Proposed legislation to zone minors from material deemed harmful to minors* [Memorandum].
COPA06	106 Congressional Record (1999) H542 (statement of Representative Pitts).
COPA07	Oxley, M. (1998). Child Online Protection Act [Press Release].
COPA08	106 Congressional Record (2002) H2393 (statement of Representative Lampson).
COPA09	American Civil Liberties Union. (2002). Maintaining Ban on Internet Censorship Law, Supreme Court Asks Lower Court to Revisit Ruling [Press Release].
COPA09a	American Civil Liberties Union. (2001). ACLU Files Brief in Second Supreme Court Battle Over Internet Censorship [Press Release].
COPA09b	American Civil Liberties Union. (2001). ACLU Ready for Second Supreme Court Battle Over Internet Censorship Law [Press Release].
COPA09c	American Civil Liberties Union. (2000). Appeals Court Rejects Congress' Second Attempt at Cyber-Censorship [Press Release].
COPA09d	American Civil Liberties Union. (1999). Appeals Court to Hear Arguments in Second Battle Over Federal Internet Censorship Law [Press Release].
COPA09e	American Civil Liberties Union. (2001). ACLU Ready for Second Supreme Court Battle Over Internet Censorship Law [Press Release].
COPA09f	American Civil Liberties Union. (1998). ACLU and Others Challenge Internet Censorship Bill Signed by President Clinton [Press Release].
COPA10	Center for Democracy and Technology. (1998). *CDT Policy Post,* 4(25).
COPA10a	Center for Democracy and Technology. (1998). *CDT Policy Post,* 4(16).
COPA10b	Center for Democracy and Technology. (2002). *CDT Policy Post,* 8(11).
COPA10c	Center for Democracy and Technology. (2001). *CDT Policy Post,* 7(15).
COPA10d	Center for Democracy and Technology. (2000). *CDT Policy Post,* 6(19).
COPA10e	Center for Democracy and Technology. (1999). *CDT Policy Post,* 5(2).
COPA11	Center for Democracy and Technology. (2008). CDT Applauds Appeals Court Ruling on COPA: Court Affirms Earlier Decision Ruling COPA Unconstitutional [Press Release].

COPA11a	Center for Democracy and Technology. (1998). Legislative History of COPA [Press Release].
COPA11b	Berman, Jerry. Testimony Before the Subcommittee on Telecommunications, Trade and Consumer Protection. Hearing, September 11, 1998.
COPA11c	Center for Democracy and Technology. (1998). *Constitutional Analysis of the Oxley Bill – The Child Online Protection Act (H.R. 3783).*
COPA12	Electronic Privacy Information Center. (2009). *The Legal Challenge to the Child Online Protection Act*.
COPA12a	Electronic Privacy Information Center. (1998). Rights Groups Prepare Legal Challenge as President Prepares to Sign Internet "Indecency" Bill [Press Release].
COPA13	American Civil Liberties Union, et al. v. Janet Reno, 31 F. Supp.2d 473 (1999). Complaint for Declaratory and Injunctive Relief.
COPA14	American Civil Liberties Union, et al. v. Janet Reno, 31 F. Supp.2d 473 (1999). Memorandum of the Court.
COPA15	American Civil Liberties Union, et al. v. Janet Reno, 217 F.3d 162 (3rd Cir. 2000). Opinion of the Court.
COPA16	John Ashcroft v. American Civil Liberties Union, et al., 535 U.S. 564 (2002). Brief for the Respondents.
COPA17	John Ashcroft v. American Civil Liberties Union, et al., 535 U.S. 564 (2002). Brief for the Petitioner.
COPA18	American Civil Liberties Union, et al. v. Alberto Gonzales, Civil Action No. 98-5591 (3rd Cir. 2007). Brief of Amici Curiae.
COPA19	John Ashcroft v. American Civil Liberties Union, et al., 535 U.S. 564 (2002). Opinion of the Supreme Court of the United States.
COPA19a	John Ashcroft v. American Civil Liberties Union, et al., 535 U.S. 564 (2002). Syllabus of the Supreme Court of the United States.
COPA20	American Civil Liberties Union, et al. v. Alberto Gonzales, Civil Action No. 98-5591 (E.D. Pa. 2007). Final Adjudication.
COPA21	House Report No. 105-775 (Oct. 5, 1998).
COPA22	American Civil Liberties Union, et al. v. Janet Reno, 31 F. Supp.2d 473 (1999). Brief of Plaintffs-Appellees.
COPA23	American Civil Liberties Union, et al. v. Janet Reno, 31 F. Supp.2d 473 (1999). Brief of Amici Curiae.
COPA24	American Civil Liberties Union, et al. v. Janet Reno, 31 F. Supp.2d 473 (1999). Brief of Members of Congress as Amici Curiae.
COPA25	John Ashcroft v. American Civil Liberties Union, et al., 542 U.S. 656 (2004). Opinion of the Supreme Court of the United States.
COPA26	John Ashcroft v. American Civil Liberties Union, et al., 542 U.S. 656 (2004). Brief of Amici Curiae.
COPA27	John Ashcroft v. American Civil Liberties Union, et al., 542 U.S. 656 (2004). Brief Amici Curiae in Support of Respondents.

Chapter 6 – The Children's Internet Protection Act

Introduction

Despite the failure of both the CDA and COPA to pass constitutional muster, legislative support for online content regulation persisted. Many in Congress remained convinced that the Internet, although a vast resource for education and commerce, had the potential to do great harm to America's children. In light of this harm and considering the government's inability to enforce either the CDA or COPA, lawmakers proposed a new regulatory strategy. The Children's Internet Protection Act would represent a drastic shift in how the state pursued its compelling interest in protecting kids. As will be described, this new policy sought to regulate the Internet in what the government perceived to be a much more limited manner than the CDA or even COPA. This new legislation would also call for the use of different technological mechanisms of enforcement than previous policies. Regardless, both the scope of enforcement and the regulatory technologies required by this law would again be the subject of heated debate and strong opposition from a number of groups.

Although the particulars of content regulation had changed, the legislative motivation for this kind of policy had not. Congress would continue to express concern that "Pornography and other material harmful to minors is widespread on the Internet" and that "The danger posed by this material is particularly acute for the nation's children" (CIPA03 p. 3). Due to this continuing harm and in the absence of functional federal policy, it was the state's obligation to step in and provide "the tools necessary to protect children from material inappropriate for their age" (Id). Nevertheless, these "tools" would again have implications for individual autonomy and access to protected speech.

Part I – Legislative Master Frames

COPA had changed the playing field in the government's mission to protect children from inappropriate content online. The narrowed focus of enforcement and demonstrated willingness to undertake some substantive review of regulatory systems had made this policy much harder to strike down as unconstitutional. Just as they had during the debate over the CDA, some members of Congress watched very carefully while COPA laboriously made its way through the courts. They noted that COPA's most significant difficulties involved the breadth of its impact on online speakers and its potentially improper use of age verification systems (COPA15 p. 5). Senator John McCain (R-AZ) was particularly interested in these developments and decided to take action. He would introduce new legislation long before COPA's official demise in the hope that the law would offer children some level of protection from online content that could be harmful to them. His bill, S. 1619, became the Children's Internet Protection Act (CIPA or CHIPA). Like COPA before it, CIPA would represent a drastic frame shift from its predecessor and would accommodate many of the arguments that the opposition employed to doom its predecessors. Nevertheless, CIPA would face many of the same challenges due to its scope and primary technological mechanism of enforcement.

CIPA was a self-conscious departure from previous legislation. Supporters of governmental initiatives to police the Internet purposely refined the target of CIPA in the hope that it would pass constitutional muster and silence those critical of such regulatory schemes. These politicians and supporting organizations acknowledged that, due to the controversy over the CDA and COPA, the scope of enforcement needed to be revised and limited. This acknowledgement led to one of the primary frame shifts that shaped

CIPA's enforcement structure in that McCain targeted his legislation specifically at public schools and libraries (CIPA03 p. 3). Rather than policing content producers and distributors directly, CIPA would attempt to block content at the receiving end in these institutions. Supporters of CIPA believed that this refined target of enforcement and focus on minors' access put this policy on much firmer legal terrain than either the CDA or COPA. After all, CIPA would only block content on computers designated for use by minors and uniquely under the control of the government. Rather than attempting to define a national content standard as they had with the CDA, "Members of Congress…narrowed the scope of the law so that [it] would more adequately apply to the Internet" (CIPA19 p. 24).

Using as his blueprint the Safe Schools Internet Act, the Child Protection Act and the E-Rate Policy and Child Protection Act (see Chapter 5, p. 143), McCain proposed that "schools and libraries that receive federal funding" must use "filtering technologies to block from minors Web pages that contain material that is obscene, child pornography, or harmful to minors" (CIPA07 p. 4).[25] Specifically, any such public institution would be required to implement some "technology protection measure" that guarded against images that were obscene, child pornography, or harmful to minors (CIPA01 pp. 2-3) if

[25] The exact statutory language reads: "No funds made available under this title to a local educational agency for an elementary or secondary school [or library]…may be used to purchase computers used to access the Internet, or to pay for direct costs associated with accessing the Internet, for such school unless the school, school board, local educational agency, or other authority with responsibility for administration of such school both; ``(A)(i) has in place a policy of Internet safety for minors that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are;``(I) obscene; ``(II) child pornography; or ``(III) harmful to minors; and ``(ii) is enforcing the operation of such technology protection measure during any use of such computers by minors; and ``(B)(i) has in place a policy of Internet safety that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are; ``(I) obscene; or ``(II) child pornography; and ``(ii) is enforcing the operation of such technology protection measure during any use of such computers" (CIPA01 pp. 2-3).

they benefited from federal assistance. While Congress vaguely described these technological measures as any "technology that blocks or filters Internet access" (CIPA01 p. 1), most organizations subject to CIPA would interpret this to mean commercially available filtering products (CIPA26 p. 29). Congress was not inclined to disabuse schools and libraries of this interpretation of the law and would go to great lengths to provide information about filtering products while discussing the merits of this policy. For example, on the Senate floor McCain pointed to the efficacy of commercial filtering software as "not only good at protecting children but also well-received and in high demand" (CIPA05 p. 8). Lawmakers argued that filters were the natural choice for schools and libraries because they were effective enough and flexible enough to "to address just about every different value or need relating to child safety on the Internet" (Id).

This emphasis was a direct result of the Supreme Court's rulings on both the CDA and COPA that "suggested that the use of filtering or blocking systems in order to regulate what comes out of the Internet is a more narrowly-tailored method of protecting children from harmful Internet material than an attempt to criminalize what is placed on the Internet" (CIPA03 p. 8). This is a particularly interesting frame shift considering the legislative position on filtering software expressed previously. During the debates over both the CDA and COPA, Congress had taken a dim view of this technology noting that such systems were "not the preferred solution" and "that a national mandate requiring the use of blocking or filtering could lead to private censorship or inadvertent blocking" (COPA21 p. 19). Now, however, Congressional supporters of CIPA would extol the virtues of contemporary commercial filtering software noting that technologically

advanced systems had "risen far above these early products by using computers that scour the Internet coupled with human review to ensure a high level of accuracy" (CIPA19 pp. 50-51). Conveniently, the government noted that many of these "filtering products…have been specifically designed to operate in a more commercial application such as large corporations, schools and libraries" (Id). Due directly to oppositional pressure (and, perhaps, prior endorsement of filtering software) as well as judicial opinion, McCain and other legislators were convinced that "The installation of filtering or blocking systems is the least restrictive means of achieving the government's compelling interest" of protecting children (CIPA03 p. 9). While COPA languished in the courts, it was imperative that Congress act to protect children. Commercial filters seemed the best option for doing so.

Also, even if filters had some flaws and raised some constitutional concerns, like Senator Exon, McCain was "willing to sacrifice some of our civil liberties to protect these children from these terrible things that are being inflicted on them" (CIPA25 p. 45). If the law burdened adult access, it was a small price to pay considering what was at stake. It is interesting to note that McCain and Exon were also similar in that they both had little personal familiarity with either the Internet or the regulatory technologies they had proposed. McCain himself had described his ignorance of such systems noting that he was "an illiterate who has to rely on my wife for all of the assistance that I can get," and that he "never felt the particular need to e-mail" (Terkel, 2008). Despite this, McCain insisted that he did not need personal knowledge to draft sound legislation – even legislation that would drastically impact online access for millions of users across thousands of institutions. As one of McCain's aides noted, "You don't necessarily have

to use a computer to understand how it shapes the country … John McCain is aware of the Internet" (Id). Based on this awareness and based on prior experience with the CDA and COPA, McCain would offer legislation that would take online content regulation in a new direction. While he had little personal knowledge of either the Internet or filtering software, in CIPA McCain had constructed shrewd policy that incorporated key elements of the opposition's arguments. As the opposition would find, these shifts would make CIPA a much more difficult policy to oppose. Despite this, CIPA would remain contentious and filtering would continue to raise constitutional concerns.

Despite this novel shift in CIPA's regulatory approach, the primary motivating force behind this policy was no different from that which Congress had used to justify the CDA and then COPA. Many members of Congress still believed that much of the content available on the Internet was completely inappropriate for children and should be regulated in a manner, which protected minors from it (CIPA03 pp. 3-4). Despite Congress' previous disavowal of similarities between the Internet and broadcast media (see page 153), the suggestion that the pervasive nature of the Internet required government intervention through policy and through technology persisted. These legislative supporters of content regulation remained concerned that the Internet was a "pervasive tool" that was frequently "used by children to research school projects, look for entertainment, or chat with friends" (CIPA07 p. 1). This pervasive nature of the technology left many parents and legislators "concerned that children are encountering unsuitable material – such as pornography – while they use the Internet" and they insisted that new legislation was required (Id). Also, for the first time, concerned lawmakers, conservative religious organizations and other groups supportive of content regulation

argued that pornography was not the only material that must be limited. In order to buttress the master frame that it was a compelling government interest to protect children from the Internet, legislators argued that a multitude of harmful material existed online and that regulation should keep it from kids. In a report submitted to Congress in 1999, McCain and other anxious legislators noted that the Internet was a "tool for spreading hate, illicit drug use information, and bomb-making information" (CIPA05 pp. 6-7). The invasive nature of the medium and the exponential growth of the Internet had "provided an opportunity for those promoting hate to reach a much broader audience" (Id). Precisely because the Internet had the potential to penetrate into every corner of life, government regulation was needed now more than ever to control this dangerous information. The very nature of the medium allowed this content to be distributed widely and, like never before, "these organizations are able to deliver a multimedia hate message through every computer, and potentially into the minds of every child with a computer and a mouse" (Id). As Senator Exon, Representative Oxley and now Senator McCain argued, the worst pornography imaginable, the most illicit endorsement of substance abuse and the most "toxic" hate speech available were now "just one click away from children" (Id). Where the opposition saw this new medium as a vast democratic forum, McCain and his supporters saw the Internet as an existential threat to the innocence of America's children.

When crafting CIPA McCain and his supporters admitted that some of the regulatory metaphors on which they had relied were inapplicable to this new medium. As noted above, McCain introduced CIPA, in part, as an alternative to the CDA, which had depended so heavily on comparisons between the Internet and traditional broadcast

regulation (Id). Also, while the CDA and COPA depended on the centralized regulation of content at the source, here Senator McCain would attempt a drastically different approach. By targeting only those computers in public schools and libraries where the government itself was funding Internet access, CIPA was able to avoid many of the complications that had resulted from "zoning" content at the level of speakers. This was a novel approach and offered a striking counterpoint to those failed attempts discussed previously. This approach also flipped the speaker/listener argument on its head.

First, supporters of CIPA implied that filtering technology was particularly well suited to avoid constitutional difficulties because it only limited content for minors who were at the receiving end of any communication. They argued that courts and oppositional groups could not dispute this point because "Filtering or blocking systems restrict what the user may receive over the Internet, rather than what a speaker may put on to the Internet" (CIPA03 pp. 4-5). Second, supporters of CIPA argued that the law did not harm speakers because the government itself *was* the speaker. This argument would be particularly persuasive in the case of public schools. Since Congress tied CIPA to federal subsidies for computers and Internet connectivity and because Internet content "was to be used in the schools as part of their curriculum, the government, through the school, remains the speaker, or at least the subsidizer of the Internet speech" (CIPA03 p. 7). CIPA was not harming the ability of adults to produce and consume material considered inappropriate for minors; this law was only ensuring that such material did not invade the learning environment. If the Internet introduced such a distraction to impressionable children, it "would tend to 'garble' and 'distort' the educational message the government is seeking to promote" (Id). Schools were welcome to opt out of this

scheme if they deemed it too restrictive but they would forfeit federal funding in the process. McCain and others hoped that budget-conscious schools and libraries would choose CIPA as the more reasonable option and would consider "the required installation of filtering or blocking systems…as an appropriate measure to ensure that the government's message is not distorted" and to ensure that the state's compelling interest in protecting children was served (CIPA03 p. 7).

In order to create an empirical record for Congress to point to if it became necessary to defend these suppositions about filtering and blocking software or the constitutionality of their use, CIPA included a codicil that served the same function as the COPA Commission. Specifically, Section 1703 of CIPA mandated that a study of technology protection measures take place. The primary purpose of this study would be to evaluate "whether or not currently available technology protection measures, including commercial Internet blocking and filtering software, adequately addressed the needs of educational institutions" (CIPA01 p. 1). Despite this and similar to the COPA Commission's report, no study would take place prior to passage of the law. In fact, Congress did not require that the study even begin until 18 months after enactment of the policy (Id). While Congress had again demonstrated at least some willingness to undertake a serious review of the technological enforcement mechanisms they were proposing, the retroactive nature of the study diminished its usefulness to the point of absurdity. It was unlikely that any report, no matter what the conclusions, would force legislators to reconsider the language or requirements of an Act that they had already voted and signed into law. As will be discussed in upcoming sections, this report did reach some surprising findings about the nature of filtering technology, its efficacy, and

its constitutionality. Regardless, these findings would do little to alter McCain's course or the details of his regulatory scheme.

Finally, CIPA offered a significant departure from both the CDA and COPA in one more important and novel way. Due directly to judicial opinion and, by inference, to oppositional pressures, McCain and his supporters emphasized that CIPA would increase the autonomy of local schools and libraries. Where oppositional groups had criticized previous policies for the centralized nature of content regulation and the creation of a national standard to judge content, Congress intended CIPA to place some of those choices back into the hands of communities (see pages 163-164). First, legislative supporters presented this new policy as a way for schools and libraries to protect children as they best saw fit by choosing the technology that would block content. Senator McCain went to great lengths to emphasize the autonomy granted by CIPA and noted in a press release that "This legislation allows local communities to decide what technology they want to use and what to filter out so that our children's minds aren't polluted" (CIPA08 p. 1). The implication seemed to be that, as long as local institutions met the "technology protection measure" requirement of CIPA, local administrators were free to choose from a multitude of options. Despite this, it seems appropriate to mention here that this may have been a false choice. While legislative rhetoric implied that "School and library administrators are free to choose" their preferred technological mechanism of enforcement, lawmakers rhetorically limited that choice to "*any filtering or blocking system* that would best fit their community standards and local needs" (CIPA08 p. 2, emphasis added). Despite this, the government consistently presented this policy as a boon to local decision-making. McCain and other supporters of the law used this master

frame of local autonomy to reinforce the mission of protecting children and continually insisted that "CIPA advances legitimate local library decisions. CIPA permits local library officials to determine which software filter they will use" and how best to safeguard their values (CIPA19 p. 11).

This rhetoric of community autonomy extended beyond local determinations of which filtering software to purchase. In a more meaningful way, Congress intended CIPA to grant decision-making authority to communities by allowing public schools and libraries to decide what content they would filter. The government would argue that "CIPA provides local determination of what the filter will attempt to block by allowing the receiving school or library to decide what could constitute" material inappropriate for minors (CIPA19 p. 27). This was a logical solution to the constitutional inadequacies of both the CDA and COPA. Where these previous policies had run afoul of the First Amendment because they placed undue burdens on speakers and listeners, CIPA purposely avoided making any determinations as to the acceptability of content. In fact, under CIPA "the government is expressly banned from prescribing what material constitutes 'matter deemed to be inappropriate for minors'" (CIPA03 p. 9). Instead, it was "expected that the school and library authorities that install the filtering or blocking systems will clarify and make concrete this standard according to their local community's norms" (Id). In this way, the application of CIPA and the filtering software it required would be no different from the local enforcement of motion picture ratings by schools and libraries. Many of these institutions, supporters argued, already employed MPAA ratings as a guideline for "preventing children from being exposed to films containing excessive sex, violence, or profane language" in an educational environment (Id p. 8). In

this way, communities did not disallow content based on viewpoint, only on a local determination of what would be appropriate for minors in a school or library setting (Id). While this aspect of CIPA appeared to be an improvement over previous iterations of the law and made more accommodations for local autonomy, there were deep flaws in this logic. These flaws are based on several assumptions about the nature of filtering software and its propensity to act as a political object rather than the neutral tool Congress considered it to be.

CIPA's master frame was indistinguishable from the master frames that had motivated both the CDA and COPA. The protection of children was paramount and it was the state's duty to provide that protection through policy and through technology. Like the CDA, CIPA's master frame does not appear to be particularly amenable to a critical review of the regulatory systems the law required. Although CIPA did mandate some study of filtering systems, this review was unlikely to reincorporate any findings critical of filters back into the policy. This is strongly reminiscent of the motivation behind both the CDA and COPA and the propensity for that master frame to leave little room for informed debate. Due to the highly charged nature of this frame, legislators appear to be less likely to engage with critical points of view. Nevertheless, CIPA does represent a significant evolution in federal content regulation. The law's allowances for local autonomy regarding the acceptability of content are vastly different than centralized content standards. CIPA's targeted enforcement, focusing on minors in public institutions, is also a significant improvement over previous policies. Despite these key differences, the opposition would continue to take exception to online content regulation and would point specifically to filters as cause for constitutional concern.

Part II – Oppositional Master Frames

CIPA was a vastly different policy than either the CDA or COPA. At first glance, it would seem that Congress had made accommodations for most of the opposition's and the courts' criticisms. CIPA appeared to allow for local autonomy and Congress had mitigated constitutional concerns regarding the regulation of online content by controlling access at the recipient level. Despite these significant policy alterations, oppositional groups remained skeptical of the government's constitutional ability to put these kinds of barriers in place. In particular, the damage that commercial filtering products could cause concerned these groups in the context of the key master frames they had identified. First, there was concern that CIPA and the filters it required did not account for the autonomy of the individual, nor did it do nearly as much for local autonomy as advertised. Second, the opposition would argue that filtering and blocking systems – particularly commercial products – would introduce a level of opacity for both individual users and the institutions that purchased them. Without a minimum level of transparency the opposition suggested that determinations as to what content the technology filtered and why would remain impervious to critical review. Specifically, due to the categories and keywords on which blocking software relied and the trade secret protections that shielded them from scrutiny, individuals, schools, and libraries would be unable to judge the appropriateness of those blocking decisions. This coincides with the opposition's third master frame that CIPA in general and filters in particular did not allow for adult access to constitutionally protected speech. This point was particularly important in the domain of public libraries, institutions primarily intended to provide access to information.

While CIPA did, at least in principle, leave determinations as to the acceptability of Internet content in the hands of local administrators,[26] the opposition remained unconvinced. As will be described in greater detail in Part IV, the opposition took specific exception to the suggestion that communities had any power to make true decisions about the (un)acceptability of content. The technical specifications of most filtering software, due to determinations made by designers, categorized content as acceptable or not prior to its purchase by public schools or libraries. The opposition expressed concern that this preemptive categorization would disempower institutions from making meaningful decisions in this regard. McCain and his Congressional supporters had insisted that CIPA provided local administrators with "the authority to determine what technology is used" to protect children from harmful material and the ability to formulate the "policies for determining how such technology is used" (CIPA05 p. 10). Despite the suggestion that CIPA empowered local judgments as to content, the opposition argued that the policy, through commercial filters, actually "supersedes those judgments, effectively preventing public libraries from determining, on a local level, what information to provide to their communities" (CIPA16 p. 52). Due to the nature of filtering software and its use of predetermined content categorization, the opposition suggested that this put CIPA in the same category as the CDA and COPA. By removing local autonomy in this way, "Congress has overridden those local decisions, imposing its own, one-size-fits-all solution nationwide" (Id). This was strongly reminiscent of the

[26] CIPA strongly mandated that "A determination regarding what matter is inappropriate for minors shall be made by the school board, local educational agency, library, or other authority responsible for making the determination. No agency or instrumentality of the United States Government may; (A) establish criteria for making such determination; (B) review the determination made by the certifying school, school board, local educational agency, library, or other authority; or (C) consider the criteria employed by the certifying school, school board, local educational agency, library, or other authority" (CIPA01 p. 18)

CDA's stated goal of "establish[ing] a uniform national standard of content regulation" (CDA13 p. 49). In contrast, instead of the state setting that standard, CIPA allowed the private entities that manufactured filtering software to set it for them. From the opposition's point of view, this granted stunning power to commercial technology and those who designed it. Due to their ability to hide blocking decisions behind trade secret protections, these companies could "make their decisions without any input from or regard for the views of librarians or local communities, much less prior judicial review" (CIPA17 pp. 3-4).

Related to its master frame of safeguarding local autonomy, the opposition also argued that CIPA stripped agency from adult citizens. This was particularly problematic in the context of public library patrons who were in no way the target of CIPA. Due to CIPA's requirement that all library computers with Internet access funded by federal subsidy must install filters, the law forced adult users to contend with these systems. The opposition argued that this requirement had the potential to hinder adult access and reduce individual choice by subjecting these users to the same content blocking that Congress intended for minors. This caused difficulties in the context of this master frame because the filters' predetermined content categories could "block library patrons and staff from accessing speech" protected by the constitution (CIPA17 pp. 3-4). This was particularly damaging to autonomy if the filters blocked adults "from accessing speech that does not meet the categories of the law" but only the "broader categories defined by the private companies" (Id). Considering the scope of the law and the potential for the filters to block so many legitimate search requests, the opposition argued that CIPA could "block library patrons and staff from reading constitutionally protected speech literally

millions of times" (Id). Like the CDA, this effect of CIPA "would be to reduce adults to obtaining access by computer to only that information that is fit for children" (CDA11 p. 23) – a prospect that was both constitutionally questionable and damaging to individual autonomy.

McCain and other supporters of CIPA anticipated this criticism and made allowances for just such an eventuality. Although the Act targeted children, lawmakers were also aware that the law might impose filtering software on adults in public library settings. Due to this, CIPA's proponents had included a "disabling provision" intended to avoid any constitutional concerns that might arise in such a situation. Specifically, the disabling provision allowed "An administrator, supervisor, or person authorized by the responsible authority [to] disable the technology protection measure concerned, during use by an adult, to enable access for bona fide research or other lawful purpose" (CIPA01 p. 11). The government argued that this provision provided a remedy for any unauthorized blocking of adult access to constitutionally protected speech and, if such blocking occurred, "the patron need only ask a librarian to unblock the site or (at least in the case of adults) disable the filter" (CIPA14 pp. 44-45). Nevertheless, this provision did not satisfy the opposition's master frame related to individual autonomy. The government's accommodation did not mollify the opposition and these groups argued that this provision was both "hopelessly vague" and granted broad discretionary powers to local librarians and system administrators (CIPA11 p. 5). Specifically, the opposition asserted that this statutory language would "grant library employees unbridled discretion in deciding whether to disable the blocking software 'for bona fide research or other lawful purposes'" (Id). Equally troubling was that the law did nothing to define what

research would qualify as "bona fide" (Id). As will be discussed, through this provision Congress also inadvertently granted an inordinate amount of discretion to filtering manufacturers whose products would make initial determinations as to what content was or was not acceptable and, by extension, what research was or was not bona fide. In the context of adult access to constitutionally protected speech accessed through a public institution, this would have important ramifications for both individual autonomy and First Amendment considerations.

In addition to concerns related to local and individual autonomy, the opposition was also apprehensive about the opaque nature of commercial filtering software. Part IV will discuss the design and technical specifications of these products in more detail but it is useful to introduce the opposition's arguments here briefly. Specifically, the opposition intended one its primary master frames to preserve a level of transparency for any user confronted with government-mandated blocking technology such as that required by CIPA. As noted above, this was particularly important for adult library patrons who had the right to view constitutionally protected speech in these institutions. Failing that, these patrons had the ability to request that librarians disable filters so that they could exercise this right immediately. Despite this, neither library patrons nor librarians themselves were aware of how filters made blocking decisions and had no idea what websites were on blocking lists (CIPA09a pp. 4-5). Due to this, it was impossible for either individuals or local administrators to make true determinations about the acceptability of content based on community standards. This gutted McCain's assertion that CIPA placed power back in the hands of hometown schools and libraries. Instead, the opposition argued that "Blocking decisions made by private filtering companies –

which typically refuse to disclose their blocking criteria or list of blocked sites – are not subject to any review, either by a proper judicial authority, or by the librarians who use the software" (CIPA11 p. 31).

This opacity was cause for serious concern because commercial filtering software had proven itself unreliable in several ways. First, filters were prone to "underblocking," a situation where a school or library's software did not successfully block content that was of concern for minors in the context of CIPA's statutory language (CIPA09a p. 5). This underblocking was substantial and a Consumer Reports study had noted that "most of the products we tested failed to block one objectionable site in five" (CIPA11 pp. 14-17). Studies broadly defined underblocking as "the percentage of 'offensive' sites that the filter fails to block" (Heins & Cho, 2001). While most studies do not give specific examples as to the precise content that was underblocked, these sites did include those that contained the sexually explicit content that motivated Congress to pass CIPA. The opposition repeatedly noted that underblocking was a design flaw of filtering software and one expert witness characterized underblocking as "a fundamental tradeoff faced by blocking companies as they seek to balance overblocking against underblocking. In particular, when judgment calls determine the classification of a site, or when technical or practical constraints prevent perfect classifications, any action is likely to contribute to either overblocking or underblocking…Representatives of blocking companies consistently agree that underblocking affects their products' accuracy" (CIPA06 p. 28).

Even more alarming to the opposition was the propensity of filters to "overblock" vast amounts of online content that was in no way objectionable under the law including educational, medical, political, informational, literary, and artistic material. To contradict

this point, Congress did cite some research suggesting that overblocking – especially overblocking of medical information - was trivial (see Richardson, et al., 2002) and that "when a filter is set to the least restrictive setting, such as the 'pornography' setting on one of the most widely used filters in public libraries (N2H2), it blocks 1.4% of all health sites" (CIPA14 pp. 43-44). Despite this, filtering critics and consumer groups documented the phenomenon much more exhaustively with overblocking being defined as any circumstance where filters arbitrarily "prevent access to a substantial number of sites that do not contain content that fits within the blocking company's stated category definitions" (Id p. 23). The scope and breadth of content overblocked by filters was staggering and examples are plentiful. First, one study showed that filters disallowed large swaths of "educational, cultural, historical, and political information" (EPIC & Peacefire, 2000). More specifically, overblocked content included "sites hosted by the Knights of Columbus, Vision Art Online (which sells wooden religious wall hangings), Wisconsin Right to Life, a Jewish lesbian and gay group, an amputee support group, a California libertarian candidate, a bed and breakfast resort, and a home schooling group" (Smith, 2009, pp. 290-291). This overblocking was widespread among commercial products (CIPA09a p. 5) and, by mandating their implementation, Congress had created a situation where "valuable, useful, and legal information inevitably is blocked" (CIPA10c p. 8). It seemed clear that "all available filtering technology blocks access to a tremendous amount of constitutionally protected expression" and that Congress had presented "public libraries with an impossible choice: either install mechanical, imprecise, and incredibly broad speech restrictions on Internet resources, or forgo vital federal funds to which the libraries are otherwise entitled" (CIPA11 p. 4). Not only was

the opposition concerned that filters erroneously blocked a great deal of constitutionally protected content but that these concerns were "increased because the extent of blocking is often unclear and not disclosed" (CIPA12 pp. 24-25).

Oppositional groups blasted legislators on this point and suggested that "Congress was well aware of the inherent problems of blocking software when it passed CIPA" (Id). There is certainly evidence on this point and even the COPA Commission's report had alerted legislators to this potential problem. Specifically, the Commission's report had noted that filtering technology "raises First Amendment concerns because of its potential to be over-inclusive in blocking content" (COPA04 p. 21). This awareness, in conjunction with CIPA's technological requirements, created "a prior restraint because the blocking decisions made by private filtering companies effectively silence speech prior to its dissemination in public libraries" (CIPA12 p. 31). Again, it is important to note that this potential chilling effect created by the software was not only problematic in itself but was even more dangerous because the blocking criteria employed by filtering manufacturers were completely invisible to the public. Congress predicated CIPA's content blocking on specific statutory language – language based in part on constitutional considerations. Not only did commercial filters fail to block content based on those same legislative criteria but the software could be blocking content based on political bias, private notions of acceptability or religious considerations that should not be imposed on the public (CIPA19 p. 42). No one, not adult library patrons, librarians, school administrators, or even federal legislators could be certain of these criteria or the motivations behind them. The opposition argued vehemently that these kinds of determinations should be transparent to the public if filters were to be compulsory.

Filtering manufacturers should not be able to hide behind trade secret protections and computer code if Congress required that their products be used in these institutions – particularly if these companies were blocking constitutionally protected speech simply because they might "deem the content too controversial" for their customers to view (CIPA12 p. 27). This level of opacity for the user and its chilling effect on speech was entirely unacceptable to the opposition in the context of this master frame.

This argument intertwines with the opposition's third master frame requiring that the government protect access to a wide range of online content. McCain and other Congressional supporters of CIPA had argued from the outset that this policy did not raise constitutional concerns or, at least, that it did not raise as many concerns as the CDA or COPA. First, legislators suggested that because CIPA "would apply only to obscenity, which is not protected by the First Amendment, it would be constitutional" (CIPA02 p. 2). Second, even if this law did infringe on some protected material, the government had the ability to "constitutionally limit minors' access to protected material" (Id). Also, because McCain and others had argued that, within this regulatory scenario, the government itself was the speaker, then "Congress may, to some extent, discriminate on the basis of content of protected speech in choosing what speech to fund" (Id). Congress also tied these arguments for the constitutionality of CIPA to the point made previously that this law, unlike the CDA and COPA, targeted speech at the level of recipients instead of directly at speakers. In this sense, legislators believed filtering was constitutional because these technological "systems restrict what the user may receive over the Internet, rather than what a speaker may put on to the Internet" (CIPA03 pp. 4-5). Supporters of this legislation believed that all of this, in combination with the

disabling provision, ensured the constitutionality of the law and the legal application of filtering software. Despite this, the opposition took exception to this legislative rationale and argued that the law and the technology it required hindered access to protected speech.

A summary of the opposition's discussion on this point follows: First, oppositional groups argued that "the software required to block the material cannot determine which material is protected by free speech" (CIPA07 p. 4). Second, organizations including the American Library Association (ALA) and American Civil Liberties Union (ACLU) argued that "the law is unenforceable" because it "censors speech to adults as well as children, is overbroad and vague" (Id). From a design perspective, these groups believed that "It is currently impossible…to develop a filter that neither underblocks nor overblocks a substantial amount of speech" (Id). The opposition seized on this point to imply that McCain and the rest of Congress did not understand the technology they had imposed upon public schools and libraries. These groups also suggested that this misunderstanding was willful and flew in the face of previous Congressional findings. This is where the COPA Commission's report would again haunt CIPA's supporters. The ACLU in particular pointed out what they saw as political hypocrisy and noted that "Congress approved the censorship law [CIPA] even after its own 18-member panel set up to study ways to protect children online rejected blocking software because of the risk that 'protected, harmless, or innocent speech would be accidentally or inappropriately blocked" (CIPA09 p. 3). Congress, the opposition argued, had failed to address the nature of filtering software and had ignored any findings critical of this technology.

While the ACLU could certainly make this point, they may have been guilty of some hypocrisy as well. Congress had expressly written CIPA in response to the Supreme Court's suggestion that filters may be a constitutional solution to the problem of minors' access to online pornography (CIPA03 p. 8). This, in turn, was the result of the opposition's endorsement of filters during the debate over the CDA and COPA. During the debate over the CDA, oppositional groups had specifically made the case that commercial "filtering technologies provided a less restrictive means to achieve Congress' stated goal of protecting children" (CDA08 p. 2). While that endorsement became more tepid while Congress negotiated COPA, the opposition still argued that "user-controlled filtering and blocking software and other user-controlled technologies were more effective and less restrictive means of protecting children than government mandates" (COPA10 p. 33). While the opposition may simply have been advocating for the voluntary use of filters in contrast to centralized content regulation, they had made their point. Furthermore, Congress had little choice but to employ this strategy when the courts took up this argument. It is not difficult to see why the government turned to filtering products when the District Court's opinion on COPA had practically invited them to do so. Specifically, the court had noted that, "By enacting programs to promote use of filtering software, Congress could give parents that ability [to protect kids] without subjecting protected speech to severe penalties" (COPA20 p. 70). It is no wonder then that Congress had "good reason to believe that the filtering or blocking conditions" set by CIPA "are constitutional" (CIPA03 p. 6). The opposition, therefore, would have a difficult argument to make when criticizing filters on constitutional grounds, especially because they had spent the previous five years singing their praises.

Part III – Legislative Diagnostic Frames

The "problem" as defined by Congress had not changed significantly as these policies evolved. In the case of the CDA, COPA, and now CIPA, the Internet was a problem because it had not only the potential to expose children to harmful content but also the likelihood of doing so. This aspect of the medium and the tendency of online content to be harmful to minors required swift and decisive government intervention. Not surprisingly, the stated purpose of CIPA was to "protect American children from exposure to harmful material while accessing the Internet from a school or library" (CIPA03 p. 3). With the CDA dead and COPA dying, it was crucial that Congress act immediately to mitigate the damage being done every day. McCain's report to Congress emphasized this danger noting that "Pornography and other material harmful to minors is widespread on the Internet…there are currently some 28,000 adult Web sites promoting hard-and-soft-core pornography" (CIPA03 pp. 3-4). Appalled by these numbers, supporters of CIPA were quick to point out that "12-17 year old adolescents are among the larger consumers of porn" (CIPA04 p. 1). Despite the fact that "Congress tried to protect children from obscenity with the 'Child Online Protection Act'…children are still in danger" (Id). If legislators could not directly regulate online content and "protect our children from the obscenity on websites" then "the only solution is to protect them when they use the Internet" (Id).

As noted previously, McCain extended the rhetoric of this legislative diagnostic frame to the harm caused by online hate speech, exposure to illicit drug content and exposure to violence. Using this modified frame, CIPA's supporters painted a dark picture of all the "Web sites [that] depict graphic violence or provide how-to instructions

on drug or bomb-making [and] high stakes gambling" (Id). Perhaps most importantly, Congress also stressed that unregulated access to the Internet had a direct correlation to sexual abuse and the "danger posed by this material is particularly acute for the nation's children, who are unable to guard themselves with the sophistication of an adult" (Id). Not only was the World Wide Web dangerous but, "Because of unfiltered or unsupervised access to the Internet and online services, children are being enticed and lured away from home, sexually molested and victimized through the distribution of child pornography" (CIPA25 p. 14). As expressed by McCain and CIPA's supporters through this diagnostic frame, it was specifically because no regulation existed that these dangers continued to haunt children online.

Precisely because the government had thus far been unable to regulate online content directly, it was imperative that the state safeguard the primary points of access for minors. Schools and libraries became the natural target of enforcement and, as these institutions became "increasingly connected to the Internet, it is incumbent on them to assume a supervisory role in protecting children from harmful material encountered on the Internet" (CIPA03 p. 5). Even if schools and libraries did not leap at the chance to install filters on their computers, Congress expected these publicly funded institutions to at least "participate in the supervision of children's Internet use by taking the steps necessary to prevent children from being exposed to harmful online content" (Id). With that in mind, Congress was determined to "make sure that schools and libraries…have the tools necessary to protect children from material inappropriate for their age or for the school or library environment" (Id). Congress believed that filters were exactly the right "tool" to accomplish this goal and, based on prior court rulings, had "good reason to

believe that the filtering or blocking conditions set on…schools and libraries are constitutional" (Id p. 6).

Based on this frame, filtering products were not only constitutional from a legislative point of view but these systems also had the benefit of being specifically designed to protect children. Congress latched onto the fact that these companies had already done the heavy lifting by designing "technology applications that seek to protect children from exposure to inappropriate material that is disseminated and available on the Internet" (CIPA05 pp. 7-8). Although intended for a commercial audience, filtering and blocking software seemed the perfect fit for achieving the government's compelling interest of protecting children in these public institutions as well. It is unfortunate that legislators' interest in the design process ended there. As they had argued with the age verification screens used by online pornographers, legislators also noted that filters were already in use by public schools and libraries. This went a long way toward legitimizing the software as an option friendly to local autonomy and as an efficient mechanism familiar to these institutions. To prove this point, legislators would come to rely on studies demonstrating that, even prior to CIPA, "many public libraries have installed filtering software that blocks access to pornographic sites" in order to "address the problems associated with online pornography" (CIPA14 pp. 12-13). Without direct government requirements, "Almost 17% of public libraries [already employ filters] on at least some of their Internet-connected computers" (Id). Additionally, 7% of libraries had installed filters on all of their Internet terminals (Id). These systems were ideal for public institutions, lawmakers argued, because schools and libraries had already implemented them with no obvious adverse consequences.

Not only did CIPA allow "for libraries to draw distinctions" about content but it allowed them to do so based on community standards rather than "any particular viewpoint" (CIPA14 pp. 40-41). This policy and the filters it required would allow public institutions to continue their mission of providing access to information without discriminating against certain points of view. This was important, particularly in a public library setting, where viewpoint neutrality was a constitutional necessity.[27] If material was to be restricted for adults, the library could not do so because of some preexisting bias about the content of the message. Congress argued that commercial filtering products, like librarians, were uniquely qualified to accomplish this goal. From the legislative point of view, this technology would only "filter or block material based on its inappropriate content, not based on any particular viewpoint" (CIPA03 p. 7). Congress argued that CIPA, through the use of filters, simply extended the similar role that librarians played into the realm of online content.

Public libraries, Congress argued, were deeply involved in the mission of protecting children from inappropriate material long before the advent of CIPA. Libraries had a distinguished history of choosing what reading and research materials were best for the community they served and were obligated to "to separate out the gold from the garbage, not to preserve everything" (Katz, 1980, p. 6). From this perspective, requiring the use of filtering software in public libraries was no different than recognizing the broad discretionary powers libraries enjoyed when practicing traditional collection

---

[27] In *Kreimer v. Bureau of Police*, 958 F.2d 1242, 1259 (3d Cir. 1992), the court had ruled that public libraries are a limited public forum open to the public for "reading, studying, [and] using the library materials." Although libraries can control any additional activities that take place on the premises, these institutions "must not become engaged in viewpoint discrimination even at the direction of its funding agency. Not only are libraries enjoined from viewpoint discrimination but they are involved in the promotion of access - the protection of the rights of end users to receive ideas" (Latham, 2001).

management. After all, in the context of the legislative diagnostic frame, "The Internet is simply another method for making information available in a school or library. It is no more than a technological extension of the book stack" (CIPA05 p. 9). As such, "The deference owed to public library's collection decisions extends to its judgments about what material to collect from the Internet" (CIPA14 p. 20). Again, libraries seemed the perfect place to confront the problem posed by the Internet. These institutions were already disinclined from providing access to pornography in their physical collections, so they should have no problem restricting access to such material online. McCain and CIPA's supporters pointed out this serendipity time and again, noting that "While libraries retain ultimate control over their book collections, they also retain ultimate control over their Internet collections" (CIPA14 p. 36). As public institutions, "libraries have broad discretion to exclude pornography from their print collections, [just as] they have broad discretion to exclude pornography from their Internet collections" (Id p. 20). The use of commercial filtering and blocking products simply augmented the library's ability to exercise this discretion. The Internet, after all, was rife with both "gold" and "garbage" and more was added every day. How were librarians to keep pace with this onslaught without the help of some technological tool? In this sense, Congress argued that filters would be a boon to public librarians and would help them sift through the massive amounts of inappropriate material that could harm children. Specifically, the government would argue that "because of the vast quantity of material on the Internet and its rapidly changing nature, libraries cannot possibly segregate, on an item-by-item basis, all the Internet material that is appropriate for inclusion in the library's collection from all the material that is not" (Id p. 34). While superficially sensible, the opposition and

librarians themselves would take great exception to this simplification. As will be discussed, the suggestion that filters were in any way comparable to true collection management or that these regulatory technologies aided librarians in their mission of providing unfettered access to information particularly disturbed these groups.

In spite of this, Congress continued to emphasize that libraries were a perfect place to address the harm caused to minors by unregulated access to the Internet. As long as libraries practiced viewpoint neutrality when exercising filtering decisions, no constitutional difficulties would present themselves. Besides, CIPA did not require public librarians to ban constitutionally protected speech, only to choose that content which best served their patrons. If some overblocking or underblocking were to occur as an unavoidable consequence of the technology and even if "filtering software erroneously blocks some constitutionally protected speech" this "does not undermine the reasonableness of its use" (Id p. 21). If some patron took offense to this reasonable use of filters, they had many other avenues available for accessing material online. This is another instance where CIPA's focus on recipients rather than speakers came into play and the government was able to argue that "Any material blocked by a filter remains on the Internet and may be obtained from millions of computers throughout the world. A library's decision not to provide such material through its own computers is a collection decision, not a restraint on private speech" (Id). Simply because the library blocked access did not mean that filters "imposed a 'restraint' on Internet content" (CIPA14 p. 54). Since Congress had directly equated Internet access in public libraries with physical collection management, legislators were able to imply the constitutionality of commercial filtering products by association. If one was constitutional, then the other surely must be.

Based on this analogy, CIPA's supporters were able to argue that "Libraries decline to collect many books that are constitutionally protected, and declining to collect constitutionally protected materials form the Internet is equally unproblematic" (Id p. 21).

Like the CDA and broadcast regulations, with CIPA Congress needed to latch onto some sensible metaphor in order to bolster its diagnostic frame. Comparing technological content filtering with traditional collection management served this purpose well. Inappropriate content undoubtedly existed online and Congress continued to insist that some form of federal legislative response was necessary to regulate minors' access to it. Public libraries, as a clearinghouse for information of all sorts, seemed a natural point for that regulation. Books, magazines, periodicals, and research materials of all kinds, lawmakers argued, were no different from the vast array of information offered on the Internet. If librarians had the constitutional discretion to keep pornography out of their print collections, why could they not do the same when providing Internet access? Although legislators did acknowledge that the "unique nature of the Internet and the problems posed by it to public libraries have no real analogue in First Amendment jurisprudence" (CIPA15 p. 3), the differences were overshadowed by the similarities. Whatever the medium, the government was adamant that "There is no principle of law that can be pressed into service to require…that a library carry Penthouse or other sexually explicit material" (Id). If the state was funding both the library and Internet access within it, "There is simply no legal basis to assume that government libraries are required to provide pornography to their patrons" (Id). In this way, the law could keep inappropriate Internet content from minors without repeating the mistakes of the CDA and COPA.

Part IV – Oppositional Diagnostic Frames

Congress had metaphorically reduced the Internet to the equivalent of an online encyclopedia that public librarians could censor at will. The American Library Association (ALA) took particular exception to what it saw as a gross oversimplification of the library's traditional mission of providing access to information. When confronted with the legislative diagnostic frame comparing mandatory filtering to the historical practice of selecting content for physical collections, the ALA and other groups would offer a powerful counterargument. Specifically, the ALA would argue that CIPA "imposes unprecedented, sweeping Federal speech restrictions on public libraries across the nation. Filters are contrary to the mission of the public library, which is to provide access to the broadest range of information for a community of diverse individuals" (CIPA10b p. 5). Within the context of its diagnostic frames, the opposition would argue that filters were not only antithetical to this mission but that this technological mechanism of enforcement harmed both local and individual autonomy, introduced an unacceptable level of opacity for the user and had the tendency to reduce access to protected speech.

The issue of local autonomy was particularly important to the ALA and other oppositional groups confronted with the technological requirements of CIPA (see pages 163-164). While McCain had vehemently argued that this policy "allows local communities to decide what technology they want to use and what to filter out" (CIPA08 p. 1), librarians would suggest that CIPA had the opposite effect. Often, the law confined local libraries to commercial filtering products in order to fulfill the Act's technological requirements but also, due to constraints of budget, time, and expertise, these institutions

were limited to the predetermined categories of content embedded within filtering software. As the ALA would argue, these products had already demonstrated a propensity for blocking a great deal of valuable content that in no way ran afoul of the law (CIPA10d p. 9). As professionals with the mission of keeping their communities informed, it was of grave concern to public librarians that commercial filters had the proven tendency to "block access to medical information, political information and information related to the arts and literature" (CIPA10b p. 5). The regulatory technologies required by CIPA were damaging to the library's ability to serve their patrons completely and accurately if filters were blocking an array of content useful to them. As the ALA would emphasize, "Librarians play a unique role in our society; we bring people together with the information they need and want. Librarians do this by making sure libraries have information and ideas across the spectrum of social and political thought, so people can choose what they want to read" (CIPA10c p. 8). Despite McCain's assertions to the contrary, filters would actively prevent librarians from serving this unique function.

As with the CDA and COPA, the opposition was extraordinarily concerned with the negative impacts that regulatory systems could have due to their technological specifications. Commercial filtering products were no different in this regard than cyberzoning or age verification systems because they placed decision-making authority with those designing the technology. Filtering software, the opposition argued, was particularly damaging to local autonomy because it would not and could not account for local notions of acceptability. Instead, these systems relied on the manufacturers' values and ideology embedded in the predetermined categories and keywords that made initial

decisions about what content to block. As the ALA would make clear, "This legislation imposes a one-size-fits-all mechanical solution on libraries that are as diverse as our families and takes away local and parental control, ceding it to unaccountable filtering companies" (CIPA10a p. 3). Furthermore, because filtering manufacturers designed these products for a market of concerned parents and employers, they had the tendency to be overly restrictive. Nancy Kranich, then President of the ALA, argued that "If the same standards used in online filters were applied to a library's books the way they are to the Internet, our shelves would be practically empty" (Id). If the mission of librarians was to "help people find exactly the information they need, whether it is online or on paper" then CIPA and the filters it required would make it impossible to fulfill that mission (CIPA09d p. 12).

The ALA eventually advocated for true autonomy by arguing that Congress should discard CIPA's filtering requirement. Instead, the ALA and other oppositional groups suggested that local computer use policies and educational programs would be much more respectful of community empowerment than the imposition of commercial products. CIPA, they argued, failed to respect the diversity of interests and tastes that local libraries must accommodate. Filtering software was a poor fit for community taste and federal regulation. Instead of requiring filters, the law should make accommodations for local autonomy by acquiescing to "Internet-access policies that were developed locally to meet community needs" (Id p. 1). From this point of view, it was insulting for McCain to suggest that technology could "substitute for an informed community, effective librarians and teachers, educated families, and trained Internet users" (CIPA19 p. 38). The ALA and librarians took great umbrage that Congress would remove their

real autonomy and impose a "blunt, indeed crude instrument that cannot respect First Amendment freedom [or] distinguish between the needs of adults and children" (Id p. 40).

The issue of autonomy directly relates to the library's traditional mission of choosing the best materials for their physical collections. The ALA had made its case that, by employing this metaphor, Congress did not truly understand the nature of the regulatory technology they sought to impose or the medium itself. Due to the "vast size of the Internet", it seemed inevitable to public librarians that "the blocking software will operate in practice free of any application of the professional judgment of librarians to particular sites" (CIPA16 p. 23). This problem, and the accompanying diagnostic frame, also extended to the unacceptable level of opacity that filtering software introduced for both library administrators and adult library patrons. Due to commercial considerations, manufacturers withheld from customers the lists of categories and keywords on which filtering software relied (CIPA06 pp. 21-22). While these customers, including public schools and libraries, did hypothetically have the ability to work with software vendors in order to customize blocking lists, this process was neither easy nor encouraged. For these public institutions, it was "nontrivial to…deploy customized site lists to blocking servers" and the "difficulty, cost, and complexity of these tasks is likely to reduce the interest of most companies or institutions in doing so" (Id). While perhaps acceptable in the private market, this feature of the technology became vastly more problematic when government mandate imposed it upon public institutions with limited resources. The opacity of content blocking conflicted deeply with public libraries' ability to provide access to a vast array of information that would otherwise be available. Furthermore, if they could

not readily customize filters as legislators had suggested, then librarians were giving away the power to make truly informed blocking decisions to private entities without consultation or consent.

Filtering manufacturers had a commercial interest in withholding their blocking criteria, categories, keywords, and lists from customers and competitors. These companies had "invested significant resources in the creation of these lists" and, due to this substantial investment of time and money, they sought "to avoid public dissemination of the contents of the lists" (CIPA06 p. 20). For the opposition, financial concerns were, at best, secondary to issues of autonomy and transparency for public schools, libraries, and adult library patrons. For schools, CIPA's filtering requirement had the potential to keep a great deal of valuable material from students and delegated "educational decisions about what students should read and learn to these private companies, which will not even reveal their lists of blocked sites" (CIPA09b p. 6). For libraries, where minor access was only one consideration, this delegation of decision-making authority was even more problematic. Due to the imposition of filters, librarians were no longer able to exercise autonomous authority through local determinations about content or through computer use policies. Instead, librarians granted that authority to private filtering companies who then had "unfettered discretion to determine which Web sites a patron may view" (CIPA13 p. 166).

If adult library patrons, local librarians, and even Congress had no idea what sites filtering software blocked or why, this could be extremely damaging in the context of both individual rights and the formation of sound federal policy. One of the core concerns of the opposition in general and the ALA in particular was that the "unfettered

discretion" given vicariously to private entities may not account for local empowerment, viewpoint neutrality or, perhaps, even for First Amendment speech. The required installation of filtering software would, the opposition argued, distort "the usual functioning of public libraries…by requiring libraries to (1) deny patrons access to constitutionally protected speech that libraries would otherwise provide to patrons; and (2) delegate decision making to private software developers who closely guard their selection criteria as trade secrets and who do not purport to make their decisions on the basis of whether the blocked Web sites are constitutionally protected or would add value to a public library's collection" (CIPA13 p. 190). As noted previously, CIPA regulated minors' access to content that fell under strict legal definitions of that which was harmful to them. These definitions invariably relied on constitutional considerations – considerations that the technical specifications of the filtering software did not embed. In the District Court's eventual ruling on CIPA, it was found that no product "blocks material on the basis of legal categories; all use variously defined categories of their own" (CIPA09a pp. 4-5). Also, where CIPA required the installation of a technology protection measure "that blocks or filters Internet access to visual depictions" (CIPA01 p. 1) of material harmful to minors, of the filtering products reviewed, "None blocks on the basis of visual depictions; all consider and block text as well" (CIPA09a pp. 4-5). When considered alongside the propensity of filters to over and underblock, it seemed clear to the opposition that filters were far too crude to replace the judgment, experience, and expertise of local librarians.

Filters also subverted the viewpoint neutrality that underpinned the library's legitimacy to make content-based decisions when choosing their collections. This

technology, based on its commercial utility and due to its trade secret opacity, had the likelihood of making blocking decisions based on criteria other than those specified within the law. Specifically, the opposition argued that filtering products made "content- and viewpoint-based filtering decisions" that were "subjective" in nature and "seldom made public" (CIPA11 pp. 4, 14-17). Besides, even these legal categories of disallowed content did not apply to adult library users and would, in fact, harm the democratic rights of those patrons if the law forced them to operate under such constraints.

All of these points encompassed the opposition's next diagnostic frame. That is, the opacity of the software's filtering categories, due to trade secret protections, had the propensity to deny access to a great deal of speech that the constitution clearly protected. Furthermore, the subjective nature of blocking categories and keywords did not account for the strict legal definitions of unacceptable content delineated by the law. Lastly, the tendency of commercial filtering software to block content based on arbitrary or subjective criteria eviscerated the viewpoint neutrality required within the limited public forum of the library. Not only did this misrepresent the professional judgment traditionally exercised by librarians when making collection decisions but it also put the library at risk of imposing a prior restraint on free speech. Congress had insisted that there was nothing within CIPA "that necessitates a violation of viewpoint neutrality" (CIPA03 p. 7). Instead, Congress only intended the law "to filter or block material based on its inappropriate content, not based on any particular viewpoint" (Id). Nonetheless, the opposition argued that this instrumental representation of the filtering software was dangerously incorrect and demonstrated a lack of understanding at the legislative level. Instead, the ALA and other oppositional groups were convinced that "All currently

available filtering software is created and maintained by private parties, whose content- and viewpoint-based filtering decisions are seldom made public, do not incorporate individualized determinations of contemporary community standards, and are never subjected to the requisite exacting judicial scrutiny" (CIPA11 p. 4). Worst of all, "all available filtering technology blocks access to a tremendous amount of constitutionally protected expression" (Id).

Not only did filtering software have the tendency to block speech that qualified for First Amendment protection but also, as the opposition argued, designers intended it to do so. Manufacturers deliberately targeted these products for a commercial marketplace where no accommodation for constitutionally protected content was necessary.[28] When imposed on public institutions, this intentional design feature meant that filters would invariably block "substantial amounts of fully protected expression on the Internet based solely on the content and viewpoint of that expression" (CIPA11 pp. 14-17). Manufacturers' definitions of "objectionable content" would unavoidably "curb access to web sites addressing political and social issues" (Id). McCain and Congress repeatedly emphasized that, in the interest of local autonomy and community standards, "the government is expressly banned from prescribing what material constitutes 'matter deemed to be inappropriate for minors'" (CIPA03 p. 9). Supporters took this position to place CIPA above the fray in any conflict over viewpoint neutrality. Nevertheless, the opposition had made a powerful argument that, rather than placing true authority in the hands of individuals and local administrators, Congress had really only delegated that

[28] As of 2013, one market research firm calculated the filtering software market to be worth $1.044 billion. That market has been defined "primarily by parental spending; to a lesser extent, educational institutions, such as schools and public libraries, and information and communication service providers" (ABI, 2013).

power to private filtering manufacturers. Within the context of this frame, access to restricted speech was harmed because "Blocking decisions by private filtering companies…are not subject to any review, either by a proper judicial authority, or by the libraries who use the software" (CIPA12 pp. 23-24). Without real transparency and "In the absence of proper blocking standards…decisions by private filtering companies as to what constitutes, for example, obscenity, amount to an unlawful scheme of 'informal censorship'" (Id).

The only potential saving grace for CIPA was the policy's disabling provision. This could ameliorate many of the opposition's First Amendment concerns. This was especially true for adult access in public libraries where a patron only needed to ask the librarian to disable the software before they could access almost any site they wished. In practice this provision did not alleviate the opposition's concerns and the ALA was convinced that "these completely discretionary provisions create even more constitutional problems than they solve" (CIPA12 p. 26). For example, the requirement that patrons must ask for filters to be disabled might discourage them from doing so. This could qualify as a prior restraint and was a deterrent that did not present itself when a patron wished to peruse the library's physical collection. As the opposition would argue, "The dangerous chilling effect" represented by a disabling request "arises precisely because of the disfavored nature of filtered speech; most people are aware that filters often block access to materials that, although constitutionally protected, are undesirable, offensive, or reprehensible to some" (Id p. 27). As the ALA would point out, "the chilling effect created by CIPA's disabling provisions is particularly problematic because it requires library patrons to petition the government for access to protected speech" (Id p. 28).

Part V – Legislative Prognostic Frames

Despite these oppositional concerns, Congress insisted that "Schools and libraries have the affirmative duty to protect minors while in their custody" and that CIPA helped them exercise this duty (CIPA19 p. 55). The use of filters in these institutions (whether voluntary or not) demonstrated "that educators are taking reasonable steps to protect their kids" (Id). In order to solve the problem of minors' unregulated access to the Internet, the clear choice was commercial blocking and filtering software. In a somewhat circular argument, legislators maintained that "Effective filtering technology exists and is effective" (Id). This would be a consistent theme throughout the legislative prognostic frames and Congressional supporters of CIPA would argue that filters were the best option of any available alternatives, that contemporary filters were vastly improved relative to older versions and that the mere existence of CIPA and its filtering requirement would spur additional innovation in the filtering market. Such advancements would, lawmakers hoped, further ameliorate any constitutional concerns and improve filters' ease of use for schools and libraries.

McCain and his legislative supporters were convinced that commercial filtering products were the best and most obvious solution to the problems they had identified. Time and again, they emphasized that, as opposed to the CDA and COPA which would have imposed "censorship from above," CIPA was preferable because it simply required the use of "technology to make sure kids don't have access to harmful materials" (CIPA25 p. 5). Legislators maintained that filters were "effective" and able to "keep pace with the Internet…very easy-to-use and configure, and can be set to block all variety of objectionable material" (Id). It was obvious that the Internet was a valuable "tool for

business, education, and commerce" but it was undeniable that there was a "significant amount of obscenity and illegal information" online as well (CIPA19 p. 50). If the goal of Congress was "to limit access to this type of material without affecting the overall Internet experience for the user" then CIPA's filtering mandate was "the best alternative to solving these issues" (Id).

CIPA and commercial filtering products were, to Congress, the clear solution in the context of their prognostic frame. When confronted with the question of whether or not filtering technology was capable of meeting the requirements of the law, for CIPA's supporters "The answer is a resounding yes" (CIPA19 p. 55). The government brushed away librarians' First Amendment concerns and Congress referred these naysayers to at least one "recently released study [which] confirms that blocking software has only a negligible impact on access to valuable information" (CIPA14 pp. 43-44). Besides, patrons had a multitude of options to pursue if filters were overly exclusive and "Any information that may be erroneously blocked can often be found on another Web site or on the library's bookshelves" (Id). Congress also relied on studies demonstrating to librarians that they were already using filtering software and were quite happy doing so. In partial response to the ALA's concerns about CIPA's technological requirements, Congress reminded them that "In the past two years, use of software filtering by public libraries has increased 121 percent" and that "90 percent of school librarians and public school librarians are either 'very well' or 'somewhat well satisfied' with filtering software" (CIPA19 p. 11). What they failed to mention was that this 90% only accounted for those librarians who had voluntarily implemented filtering software prior to CIPA's mandate and may have been predisposed to be satisfied with their decision. It does not

appear that Congress ever polled librarians who either had no experience with filtering software or had purposely chosen to refrain from using it. To be fair, CIPA's supporters did rely on the testimony of at least one public librarian who recognized the need for legislative action.[29] Although she acknowledged that she did "not propose to be an expert on filters," this witness presented anecdotal evidence that "librarians who have real experience with them tell me they suit their purposes quite well" (CIPA19 p. 37). In response to the ALA's arguments against overly aggressive filters, this librarian unilaterally declared that these assertions "are simply not true" (Id). While she did agree that "no filter claims to be or is one hundred percent effective", they were more than adequate as a solution to the problem of minors' access to inappropriate content (Id). In fact, she argued that filters were exceptionally effective and that the "odds of accessing an inappropriate site with a filter on is 'about as likely as winning the lottery'" (Id).

Although Congress had been tone deaf to the ALA's primary concerns about the nature of filters, their propensity to overblock protected content and the tendency of these systems to remove decision-making authority from local librarians, CIPA's supporters did at least engage with some contemporary research about filters and did include some testimony from those who would be forced to employ filters in order to remain CIPA-compliant. None of this evidence addressed filters as anything other than an instrumental and viewpoint neutral solution to the problem Congress had identified. Despite this,

---

[29] Prepared Statement of Laura G. Morgan, Public Librarian. "E-Rate and Filtering: A Review of the Children's Internet Protection Act." Hearing Before the Subcommittee on Telecommunications and the Internet of the Committee on Energy and Commerce, April 4, 2001 (CIPA19 pp. 29-48). The testimony of this single librarian differed significantly from the ALA's independent research (see CIPA09a p. 5).

Congress was quick to admit that filters were not technically perfect nor were they likely to be in the foreseeable future.

In an effort to acknowledge this reality while still promoting the efficacy of their preferred solution, Congress would again rely on physical metaphors to bolster their claims. For example, the failure of software to block all harmful material or to allow access to all protected speech was not dissimilar, they argued, to seatbelts and turn signals. Filters, they suggested, were not so different from "the safety equipment on cars, e.g., the brakes, seat belts, and headlights" (CIPA19 p. 11). Automobile regulatory agencies did not "require 100 percent effectiveness by any safety equipment before we use it" and it was ridiculous to assume that filters should be held to such an impossible standard (Id). It was equally ridiculous, and even dangerous, to suggest that children be let out on the road without driver training, seatbelts and airbags simply because these technologies were not entirely effective. Why should Congress allow such risky behavior on the information superhighway when filters could block a wide range of questionable material? Congress appealed to common sense, decency and the ease of implementing this simple solution. Simply put, filters were "the most effective way to safeguard kids from inappropriate content online" and these systems were nothing more or less than "safety technology, like seatbelts, for Internet surfing" (Id p. 43). Furthermore, while "Seatbelts are not 100 percent guaranteed to save a child's life…there is no parent in America that doesn't buckle up when they get in the car" (Id). It would be irresponsible to deny the safety provided by filters simply because the "technology may not be 100 percent fool-proof" (Id). This was a powerful rhetorical turn within the legislative prognostic frame and, from this perspective, the "90 percent effective" rate of some

filters seemed to offer a miraculous solution in the effort to protect kids from offensive material.

With confidence in the ability of filters to regulate content successfully in the vast majority of circumstances, Congress bolstered their claims about this technology by suggesting that it would continue to evolve. Senator McCain noted that most objections about filtering were "based largely on problems associated with earlier versions of client-based software that are admittedly crude and ineffective…filtering has gone through an extensive evolution" (CIPA05 p. 8). Not only had these products shown a tendency to improve over time but the mere presence of CIPA's filtering requirement would encourage even more and faster improvements. In an argument reminiscent of legislative claims made during the fight over the CDA, CIPA's supporters would echo assertions that "the market is encouraged by the presence of a legal obligation" (CDA16 p. 25) and there existed "the potential for even greater control in the future as technology develops" (CDA01 pp. 100-101). Simply by passing CIPA, Congress all but ensured that "filter companies are going to be able to develop the technology with the help of this law so that it will" more accurately carry out its intended function (CIPA19 p. 26). Filters would improve as a direct consequence of the law and Congress emphasized the idea that "CIPA has a future-looking, beneficial purpose of encouraging the development of filter technologies, thus furthering the mass communications and Internet development goals of Congress" (Id p. 29). In this way, CIPA was a self-fulfilling prophecy by which Congress could ensure the safety of today's children through filters and even expand that protection through the incentives it provided to filtering manufacturers. Regulatory technology was the answer today and it would be an even better answer tomorrow.

In conjunction with this argument, CIPA's supporters also pointed to the already increased accuracy and efficiency of filtering software as opposed to the technology of just a few years before. Congress touted the evolutionary leap that filters had taken during this time, suggesting that these products embodied almost none of the flaws of earlier versions. They argued that "Today's technology has risen far above these early products by using computers that scour the Internet coupled with human review to ensure a high level of accuracy…today's technology protection measures are more advanced than ever before" (CIPA19 pp. 50-51). Filtering companies, perhaps aware of the potential for a vastly expanded market, did not disabuse Congress of this assumption. In fact, one filtering manufacturer would point to its opposition of previous legislation as vindication of both the effectiveness of filters and the role this technology could play as a solution to the problem of minors' access. Specifically, CyberPatrol would argue that, during the debate over the CDA, "One of the chief arguments in that case was that filtering technology was more effective than the law in protecting children from inappropriate content on line. It still is. The difference between now and then is that there are vastly more children on line and the technology is vastly better" (Id p. 43). The opposition's prior arguments regarding the efficacy of filters had essentially become ammunition for CIPA's supporters. Equally, where Congress had once eschewed filters as "not the preferred solution" (COPA21 p. 19), they now embraced this technology wholeheartedly. Both sides had undergone a frame shift in the context of filtering technology and had essentially swapped positions when it came to the appropriateness of their use. The key difference for the opposition was that it had advocated for the voluntary use of filters as opposed to CIPA's mandate.

Furthermore, in order to buttress their claim that filters were the obvious solution to the problems posed by minors' unregulated Internet access, legislators would also cast doubt on the opposition's arguments detailing the gross inaccuracy of filters. Here, lawmakers would suggest that the ALA and other groups had "misled the public into believing that filtering does not work, or more accurately, does not work well" (CIPA19 p. 43). When finally released, the Congressionally-mandated report on filters would serve to vindicate this point of view, at least obliquely. Specifically, the report would find "little doubt that technology plays a role in reducing a child's exposure to inappropriate content" and "Nineteen of the twenty-six product tests found filters effective" in this regard (CIPA26 pp. 12-13). Yet this finding is somewhat misleading because it only relates to the ability of filters to block offensive content, not its ability to accommodate educational, valuable, or otherwise protected speech. The comments of Senator Markey (D-MA) during the public hearing on CIPA exemplify this contradiction. Specifically, Mr. Markey insisted that "you can argue that [filters are] an unconstitutional infringement of First Amendment rights of Americans, and at the same time you can argue that it is imperfect in blocking out sites. But you can't have both arguments simultaneously" (CIPA19 p. 68). This demonstrates a misunderstanding of both filtering technology and the opposition's arguments against it. Commercial filters can, in fact, do both at the same time. As the opposition would point out repeatedly, filters both missed a great deal of offensive content (underblocking) and erroneously restricted a great deal of constitutionally protected speech (overblocking). The crux of the opposition's argument was that filters were inadequate in both circumstances simultaneously.

So, while Congress did, at least to some extent, engage with both contemporary research about filters and with the opposition's arguments against filters, they do not appear to have addressed the implications of these products for autonomy, transparency, and access to protected speech. In fact, time and again, legislators passed over a more substantive review of such systems in favor of an instrumental portrayal of these technologies. At no point did McCain's supporters address the potential for embedded bias within these systems or the delegation of decision-making authority to filtering manufacturers. Instead, legislators continued to approach these regulatory technologies as nothing more than useful tools that blocked content based on objective, viewpoint neutral categories instead of subjective judgments based on the values of company owners and product designers. Filters were simply effective tools, comparable to automobile safety equipment and other objects that had no adverse impact on individual rights and autonomy (CIPA25 p. 5). These products were simply a "technology tool" that was "well suited to be able to block that which is defined in this Act" (CIPA19 pp. 88-89). At the same time, there was at least some awareness at the legislative level that filtering technology had the potential to encroach upon individual rights. CIPA's disabling provision is a direct result of this awareness and, at least by subtext, indicates that Congress was cognizant of the potential for inappropriate restrictions on access to information (CIPA26 p. 16). Senator McCain was also directly aware of this facet of the technology and indicated that he shared the opposition's concerns about censorship (CIPA25 p. 45). McCain simply argued that we should accept this downside of the technology and be "willing to sacrifice some of our civil liberties to protect these children from these terrible things that are being inflicted on them" (Id).

Part VI – Oppositional Prognostic Frames

Not surprisingly, the opposition in general and the ALA in particular were unconvinced by the government's suggestion that commercial filtering products were the best and only solution available. In language familiar from the controversy over the CDA and then COPA, the opposition would argue vehemently that the problems presented by the mandatory imposition of filters necessitated immediate action. In order to ameliorate the harms caused by these systems, the opposition proposed three primary solutions. First, because filters were inherently flawed and unable to account for the legal and constitutional considerations that underpinned CIPA, lawmakers should minimize use of these access controls or remove them from the statutory language entirely. Second, any such technology, especially commercial filters, must operate in as transparent a manner as possible if they were to mediate access to such a wide range of online content. Finally, because it was so unlikely that proponents would make such amendments to the policy or that they would remove filtering requirements, the opposition felt it had no alternative but to demand that courts strike down the policy as an unconstitutional restraint of free speech.

This first point, that the use of access controls such as filtering software should be minimized or removed from CIPA's language entirely, was predicated on the critical understanding that filters could not account for the legal definitions of "harmful" content on which CIPA relied. This was a fundamental part of the opposition's argument and the ALA in particular was adamant that "the Children's Internet Protection Act is unconstitutional" and the "filtering mandate imposed by Congress is unworkable in the context of a public institution because it restricts access to constitutionally protected

speech on the users served by libraries" (CIPA10b p. 5). Even more alarming for the opposition was the fact that Congress knew of this feature of the technology and chose to implement CIPA's filtering provision anyway. Due to the COPA Commission's report to Congress (CIPA09 p. 3), legislators should have been conscious of this constitutionally fatal flaw of the technology. As the opposition would point out, "Congress was well aware [that] no technology exists that can effectively block the precise categories of speech enumerated in the Act." (CIPA11 p. 4). The opposition hammered the government on this issue and pointed out again and again that "Filtering software blocks access to Internet content in advance of any judicial test of the legal status of the blocked information and without any assessment by a court or jury as to local community standards. It would be impossible as a legal matter for nongovernmental private filtering companies to determine which websites or visual depictions on the Internet fall within the narrow legal definitions of 'obscenity,' 'child pornography,' and 'harmful to minors'" (Id pp. 14-17). Expert testimony supported this argument and confirmed this portrayal of the technology. When asked to a provide substantive review of filtering systems, this expert would testify that, including the four products he tested specifically, he was "unaware of any other blocking program that uses CIPA's specific categories and definitions" (CIPA06 pp. 15-16). This same expert would point to deposition testimony from major filtering manufacturers who "specifically agreed that their companies cannot speak to the compliance of their systems with CIPA's requirements and that they cannot guarantee that their products block only images targeted by CIPA" (Id).

Nor was it any comfort to the opposition that future filtering technology would hew more closely to the law's definitions of harmful content. While Congress was

convinced that filters had improved significantly and would continue to do so, the opposition strongly disagreed. As they would argue, "The problems with filters are not simply short-term glitches that will be solved by technological advances, as the Government suggests" but instead "the flaws identified with blocking software inhere in the nature of the Web and the necessary tradeoff between the goals of blocking as much content as possible (to prevent underblocking) and correctly categorizing the content of individual Web pages (to prevent overblocking)" (CIPA16 p. 27).

The opposition had made a forceful argument that the technological mechanisms required by CIPA failed to meet the strict statutory definitions set out by Congress. Intertwined with this aspect of the technology was the propensity of these systems to "function as automatic censors that irrationally and arbitrarily" restricted access to a wide range of valuable content (CIPA09d pp. 12-13). Filters denied "access to critical, constitutionally protected speech related to many subject areas" including "medical information, political information and information related to the arts and literature" (CIPA10b p. 5). Due to its inability to account for all (or only) that content defined as harmful by the law, filters would invariably block valuable material based on the ideology embedded within the software by filtering manufacturers and designers. These private actors undoubtedly had ideas of their own about what content warranted filtering either due to their own preconceptions or because they were anticipating what their customers might find offensive (CIPA19 p. 42). If manufacturers did not ground these decisions in constitutional considerations, they were, by definition, not viewpoint neutral. This was the basis for the opposition's argument that filtering "software blocks a host of valuable expressive content and viewpoints on the Internet" (CIPA11 pp. 31-32) in

violation of the neutrality librarians were supposed to exercise when making collection decisions. If filters imposed arbitrary blocking on adults, it would "reduce adults' Internet access to material suitable only for children" (Id). The opposition was certain that "Filtering software blocks substantial amounts of fully protected expression on the Internet based solely on the content and viewpoint of that expression" (CIPA11 p. 16).

The arbitrary nature of filtering products was of even greater concern to the ALA and other oppositional groups because they had no idea what the filters blocked or why. One of the key reasons why these groups demanded that the courts strike the filtering provision from CIPA was because there was no way of knowing what went on inside the software. In the absence of critical study and without the ability to conduct a substantive review of these blocking processes, neither the opposition nor Congress could really know how the exclusion of content took place. In short, "Because most filtering software operates on undisclosed, secret criteria, filtering companies are free to implement their own subjective judgments in their blocking programs" (CIPA11 pp. 14-17). Congress had made it clear that commercial filtering products were the preferred means for schools and libraries to remain CIPA compliant. Despite this, none of the thousands of institutions subject to CIPA truly had any sense of what they were imposing on their communities. The inherent opacity of this technology and its embedded categories troubled the opposition. The filtering provision could not stand, they argued, if "no one but the filtering companies has access to the complete list of URLs in any [blocking] category" and as long as this information was "unavailable for review by customers or the general public" (CIPA13 p. 57). The ACLU would eventually attempt to have these blocking lists and categories disclosed through court action based on the premise that, if

the government were to "mandate the use of blocking programs, the public has a right to know what is being blocked" (CIPA09c p. 8). Regardless, this demand would fall on deaf ears and the court denied the ACLU's request due to filtering companies' strong trade secret protections. For the opposition, this was simply more evidence that CIPA's filtering requirements were ill conceived and misunderstood even by those who had written the law.

Concurrent with their anxieties about the subjectivity and opacity of filters, the ALA expressed concern about the impact this kind of blind filtering could have on adult access. The ALA believed strongly that this policy would spill over into adult Internet use and subject these library patrons to the same kind of filtering that Congress only intended for children. The ALA felt that the "Children's Internet Protection Act is a misnomer" and the "legislation would not strictly limit access for minors, but for adults and all Internet users in a library" (CIPA10b p. 6). Therefore, the opposition argued that while CIPA was "commonly referred to as a 'child protection measure,' it goes further and operates to block adult access as well" (CIPA19 p. 18). By doing so, the opposition suggested that this law would "follow the CDA and COPA along the trail of unconstitutional attempts to censor the Internet" (Id).

In addition to this, the opposition would note that the disabling provision was no remedy for this deficiency. While legislative supporters of CIPA believed that this provision added a layer of constitutional legitimacy to the law, the ALA and other groups were not so sanguine. Again, they pointed to the nature of filtering technology and its inability to accommodate disabling requests with the ease that Congress had implied. On the contrary, careful study had demonstrated that "While blocking programs purport to

have capabilities that would facilitate this [disabling] process, numerous practical problems make it unlikely that, in practice, such a system could be successfully implemented using existing network-based software" (CIPA06 p. 32). The only possible solution to the harm this would inflict on adult patrons' rights and autonomy was the minimization of the use of filters in public libraries or the removal of CIPA's mandate requiring their installation.

This prognosis went hand in hand with the ALA's deep ideological conflict with filtering patrons' access to information. In fact, the ALA's own internal Bill of Rights strongly required that "Materials should not be excluded because of the origin, background, or views of those contributing to their creation. Libraries should provide materials and information presenting all points of view on current and historical issues. Materials should not be proscribed or removed because of partisan or doctrinal disapproval" (CIPA11p. 17). Filtering online content clashed sharply with this philosophy and the ALA was adamant that the public library should remain "an invaluable forum for the communication and receipt of information…for the interest, information, and enlightenment of all people of the community the library serves" (Id). While Congress had insisted that the use of commercial filtering software was on the rise in public libraries and that this technology mostly satisfied librarians (CIPA19 p. 11), the ALA told a much different story. Based on its own research, this oppositional group would argue that "Prior to this law, over 90 percent of American libraries, after careful consideration, decided not to require patrons to use blocking software" (CIPA09a p. 5). Based on a careful and critical review of the potential impact of filtering technology, the ALA argued, public libraries had overwhelmingly chosen not to impose filters on their

communities. Specifically, "Those libraries, after looking at the deficiencies of existing blocking software products, concluded that other means of preventing unwanted Internet content were at least as effective and were more protective of the values shared by libraries and the First Amendment" (Id). Due to these findings and grounded in librarians' deep ideological concerns, "The vast majority of libraries offering public Internet access have opted not to impose content blocking software on patron Internet use" (CIPA11 pp. 18-19). In the infrequent cases where "public libraries have instituted mandatory filtering policies applicable to all patron use" filtering had consistently "raised serious constitutional concerns" (Id).

As a solution to the problems posed by commercial filters, the opposition offered several alternatives of their own. First, as the ACLU pointed out, there was no need to mandate the strict use of this technology. The Congressional study on CIPA's filtering requirement would offer some support in this regard and would find that the Act's insistence on filtering and blocking technology was too restrictive. Specifically, the report would conclude that Congress should amend the statutory language because "many educational institutions default to 'filtering" technology only" (CIPA26 p. 29). The report found this aspect of CIPA unacceptable due to the fact that "filtering and blocking software has not been able to overcome problems of overblocking, inability to generate an updated index for the Internet, and lack of correspondence to statutory definitions and categories" (Id). Clearly, most librarians did not concur with the government's assessment that filters were a natural fit for public libraries. The ALA's evidence undermined the government's reliance on the unsubstantiated testimony of a single witness and cast doubt on the suggestion that librarians would rush to implement filters.

From the opposition's point of view, there were a multitude of alternatives that placed true autonomy in the hands of public libraries and library patrons. For example, while "Some libraries offer optional use of blocking software" many others relied on "training on Internet searches, lists of recommended sites, privacy screens or other methods of assisting patrons in finding the material they want and avoiding material they do not want" (CIPA09a p. 5). The ACLU would repeatedly point to these options, each of which emphasized, "the importance of local control in determining library Internet policies" (Id p. 10). Rather than conflating the use of filtering software with librarians' thoughtful collection decisions, the opposition was resolute that librarians should continue to function as they always had. One library director suggested that "Long before blocking programs ever became an issue, libraries have made it their mission to help people find exactly the information they need, whether it is online or on paper" but CIPA made "it impossible for us to do our jobs" (Id p. 12). The ACLU emphasized that "Librarians are uniquely qualified to teach library patrons how to find the content they want and avoid inappropriate content without the government trying to deputize them into the thought police" (Id). Many librarians took great umbrage that Congress would suggest otherwise, misrepresenting the work librarians did in the process. Nancy Kranich, then president of the ALA, would summarize the role of libraries and librarians: "It is the mission of libraries to provide access to the broadest range of information for a community of diverse individuals. The vast majority of children and adults use the library responsibly and appropriately. We must ensure that they continue to have access to the materials they need to thrive in the 21st-Century information society" (CIPA10 p. 1).

Part VII – Judicial Opinion

Signed into law on December 21, 2000, the Children's Internet Protection Act was the subject of an immediate legal challenge. As with COPA and the CDA before it, the opposition filed a complaint against the government in the United States District Court for the Eastern District of Pennsylvania. The American Library Association and the ACLU led the charge against this policy, alleging that it "imposes unprecedented, sweeping federal speech restrictions on public libraries nationwide" (CIPA11 p. 2). These groups and the government would defend their positions in alignment with the arguments described throughout this chapter. Almost without exception, the District Court would take up the opposition's point that CIPA in general and filtering software in particular were inherently flawed, could not account for constitutionally protected speech and did not accommodate individual or institutional autonomy.

The court initially expressed sympathy for the legislative master frame that the government had a compelling interest in protecting children and its diagnostic frame that unregulated access to the Internet could harm minors. Specifically, the three-judge panel would agree that the Internet could facilitate "the widespread dissemination of hardcore pornography within the easy reach of…children and adolescents to whom it may be quite harmful" (CIPA13 pp. 4-5). This sympathy did not extend to the technological means by which Congress hoped to achieve its compelling interest. The judges would find that "the government's interest in preventing the dissemination of such [harmful] speech cannot justify the use of the technology protection measures mandated by CIPA, which necessarily block substantial amounts of constitutionally protected speech" (Id p. 158).

This perspective strongly echoed the opposition's master and diagnostic frames and would exemplify the court's position on CIPA.

First, similar to the CDA courts, this court would focus on the unique nature of the medium and its potential as a vast democratic forum. Quoting liberally from Internet scholar Lawrence Lessig's work, the court here would argue strongly that the "architecture of the Internet, as it is right now, is perhaps the most important model of free speech since the founding…Two hundred years after the framers ratified the Constitution, the Net has taught us what the First Amendment means" (Id p. 141). Public libraries, like the Internet, were "effective vehicles for free speech" (Id p. 139). When combined, there was a "unique speech-enhancing character of Internet use in public libraries" that "derives from the openness of the public library to any member of the public seeking to receive information, and the openness of the Internet to any member of the public who wishes to speak" (Id p. 140). Like the opposition, the court would suggest that CIPA squandered the potential of both the medium and the institution if filters diminished the freedom to choose and "if we assume the Government is best positioned to make these choices for us" (Id p. 141).

The court was also gravely concerned that filtering software was wholly inadequate for achieving the government's compelling interests while preserving both autonomy and constitutionally protected speech. First and foremost among these concerns was that this technology failed to account for the strict statutory definitions of the law. The court would take up the opposition's argument that "No category definition used by the blocking programs is identical to the legal definitions of obscenity, child pornography, or material harmful to minors…defined by CIPA" (Id pp. 13-14). All of

the filtering programs examined by the court were "intrinsically unable to block only illegal Internet content while simultaneously allowing access to all protected speech" (Id p. 9). Given these "constraints of the technology" and after careful review of an array of filtering software, the court found that "it is currently impossible…to develop a filter that neither underblocks or overblocks a substantial amount of speech" (Id pp. 9-10). Also, like the opposition, the judges would remain unconvinced that future technological advances would ameliorate these deficiencies. Instead, the court would rule that "Given the state of the art in filtering and image recognition technology, and the rapidly changing and expanding nature of the Web, we find that filtering products' shortcomings will not be solved through a technical solution in the foreseeable future" (Id pp. 99-100).

Equally distressing to the judges was the subjective manner in which the software blocked content. The court would find that, because manufacturers primarily designed filters for customers who did not, by law, have to account for constitutional considerations, they were incapable of accomplishing the state's goals. Both automated categorization of content and human review would inevitably fail in this regard due to designers' and reviewers' "boredom or lack of attentiveness, overzealousness, or a desire to 'err on the side of caution'" (Id pp. 65-66). Therefore, the technology would invariably filter some protected material based on the anticipation of what "might be offensive to some customers" (Id). There was no accommodation for the judicial review of disallowed content, no filtering companies trained their staff to account for the strict legal definitions of unacceptable content, and no company "instructs reviewers to take community standards into account when making categorization decisions" (Id). Without these safeguards, filtering software would continue to deny access to religious, political,

medical, and educational content inappropriately (Id pp. 91-94). The subjective nature of this regulatory system would, therefore, result in a situation where "filters single out for exclusion particular speech on the basis of its disfavored content" (Id p. 142). Additionally, because the methods and categories of disallowed speech were proprietary information, they were "unavailable for review by customers or the general public" (Id p. 57). For the court, this opacity was unacceptable, particularly within public libraries where content-based decisions must include viewpoint neutrality.

Next, the three judges addressed the impact this subjectivity and opacity would have on adult library patrons. CIPA, the court found, was not strictly limited to minors in that the law required that "a library must also certify that filtering software is in operation during adult use of the Internet" (Id p. 21). While the government had offered CIPA's disabling provision as proof that the law would not unduly constrain adult access, the court did not agree. Specifically, the court took issue with the fact that any such disabling request would "deter many patrons because they are embarrassed, or desire to protect their privacy or remain anonymous" (Id pp. 15-16). Additionally, there was no guarantee that librarians could disable the software without delay or in a manner that would not significantly hinder adult access. When confronted with the practicalities of filtering software, the court agreed with the opposition that "the unblocking may take days, and may be unavailable, especially in branch libraries, which are often less well staffed than main libraries" (Id). The disabling provision also placed librarians in an inappropriate gatekeeping role in which they now had the discretion to approve or deny such a request "pending a determination of the validity of a Web site blocked by the blocking programs" (Id p. 51). In the court's view, this essentially placed a hegemonic

restriction on speech and unlawfully burdened adult rights and autonomy. Not only could the request itself act as a deterrent if the individual found the material in question to be personally embarrassing (Id pp. 51-52), but "the requirement that library patrons ask a state actor's permission to access disfavored content violates the First Amendment" (Id pp. 174-175). Considering the power that filters had to make initial determinations as to the acceptability of content and the undesirable position that the disabling provision put librarians in, the court felt it had no alternative but to find that CIPA created an "impermissible prior restraint on speech" (Id p. 8). In the court's opinion, they must strike CIPA down because it granted, "filtering companies and library staff unfettered discretion to suppress speech before it has been received by library patrons" (Id).

Finally, the court would find that this law both misrepresented the traditional function of public librarians and "distort[ed] the usual functioning of public libraries" (Id p. 190). By providing access to the Internet, public libraries had essentially opened this "vast democratic forum" for public use and any subsequent decision to narrow the scope of that forum must account for constitutional considerations (Id pp. 12-13). Again, the court implied hegemonic control over speech because "the state's decision selectively to exclude form the forum speech whose content the state disfavors" risks "distorting the marketplace of ideas that the state had facilitated" (Id). This directly contradicted the government's strong insistence that "a public library's decision to limit the content of its digital offerings on the Internet" was analogous to the library's "decisions about what content to make available to its patrons through the library's print collection" (Id p. 115). The court's position differed strikingly from this assessment and the judges would rule that, by providing patrons with any access to the Internet, "the library permits patrons to

receive speech on a virtually unlimited number of topics, from a virtually unlimited number of speakers, without attempting to restrict patrons' access to speech that the library, in the exercise of its professional judgment, determines to be particularly valuable" (Id p. 125). The court's ruling rested heavily on this perspective and what it saw as the proper role of the public library as well as the "severe limitations of filtering technology" (Id pp. 183-184). Due directly to the "inherent limits of the filtering technology mandated by CIPA," the court concluded that "it is not possible for a public library to comply with CIPA without blocking a very substantial amount of constitutionally protected speech" (Id).

Once again, the government would appeal the District Court's ruling and apply for Supreme Court review. Another round of briefing from both sides would ensue and the Supreme Court would issue its final ruling in June of 2003. The result would be a split decision where the majority of the Court found in favor of the government and, for the first time, took exception to most of the points put forward by the opposition. In his majority opinion, Justice Rehnquist prioritized the state's master frame of protecting children above the concerns of the ALA, ACLU and other oppositional groups. The Court agreed that the accessibility of Internet pornography and other material inappropriate for minors "has created serious problems for libraries, which have found that patrons also expose others to pornographic images by leaving them displayed on Internet terminals or printed at library printers" (CIPA18 pp. 2-3). In the Court's view, Congress had no alternative but to put forward legislation to address this ongoing harm particularly if government subsidies provided to libraries were "facilitating access to illegal and harmful pornography" (Id). In his concurring opinion, Justice Kennedy

agreed with this justification for CIPA and that there were "substantial government interests at stake" (CIPA18a pp. 1-2). Specifically, Kennedy found that, in the interest of "protecting young library users from material inappropriate for minors" and considering "the failure to show that the ability of adult library users to have access to the material is burdened in any significant degree, the statute is not unconstitutional on its face" (Id). Besides, from the Court's point of view, "CIPA does not 'penalize' libraries that choose not to install such software, or deny them the right to provide their patrons with unfiltered Internet access" (CIPA18 p. 15). Instead, "CIPA simply reflects Congress' decision not to subsidize their doing so" (Id).[30] This coincided directly with the government's argument that filters were not prohibiting speech because the state itself was the speaker. Specifically, by providing funds for Internet access the state "remains the speaker, or at least the subsidizer of the Internet speech" (CIPA03 p. 7). Therefore, Congress was free to impose CIPA's filtering requirements on public libraries and was constitutionally correct in doing so.

Furthermore, while the Court acknowledged that filtering technology had the potential "to erroneously block access to constitutionally protected speech" (CIPA18 pp. 11-12), this regulatory mechanism remained a "reasonably effective way to prevent" access to inappropriate content (Id pp. 3-4). If some "constitutional difficulties" were to result from such overblocking, the majority of the Court was convinced that "any such concerns are dispelled by the ease with which patrons may have the filtering software disabled" (Id pp. 11-12). The opposition's arguments against the disabling provision did

[30] In this the Court had established precedent to draw from. In particular, in *National Endowment for the Arts v. Finley*, 524 U.S. 569 (1998), the Court had found that the provision of federal funding could be conditioned on judgments as to the "decency" of the content being subsidized by the government.

not sway the Court's opinion and Justice Kennedy concurred that "If, on the request of an adult user, a librarian will unblock filtered material or disable the Internet software filter without significant delay, there is little to this case" (CIPA18a p. 1). Furthermore, the Court believed that this provision was neither a deterrent nor would it result in an adult library user's public embarrassment because "a patron would not have to explain…why he was asking a site to be unblocked or the filtering to be disabled" (CIPA18 pp. 11-12). Although more of a burden than not having to make such a request, to the Court this provision was "no more onerous than traditional library practices associated with segregating library materials in, say, closed stacks, or with interlibrary lending practices that require patrons to make requests that are not anonymous and to wait while the librarian obtains the desired materials from elsewhere" (CIPA18d p. 5).

This was a recurring theme in the Court's opinion and many of the justices would agree that filtering software was nothing more than a tool for extending librarians' traditional role to the Internet. The Court would echo the government's instrumental argument that "[t]he Internet is simply another method for making information available…It is no more than a technological extension of the book stack" (CIPA18 pp. 9-10). While acknowledging that "A library's need to exercise judgment in making collection decisions depends on its traditional role in identifying suitable and worthwhile material" the Court would affirm that the library "is no less entitled to play that role when it collects material from the Internet than when it collects material from any other source" (Id p. 11). Therefore, "A library's decision to use filtering software is a collection decision, not a restraint on private speech" (Id p. 13). The Court discounted the opposition's argument that CIPA subverted this traditional role by delegating decision-

making authority to private software manufacturers. The Court also did not address what the opposition believed was the subjective and opaque manner in which filters accomplished the state's goals. Instead, the Court would find that "it is entirely reasonable for public libraries to…exclude certain categories of content, without making individualized judgments" as to the merit of material within those categories (Id).

The Supreme Court had issued a strong, although divided (6-3), opinion on the constitutionality of CIPA and the mandated use of commercial filtering software. Senator McCain and his supporters had crafted policy that addressed many of the opposition's key arguments against the CDA and COPA. Furthermore, in CIPA, Congress had attempted to balance the power of the government's master frame with the necessary constitutional considerations. In the Court's view, lawmakers narrowly targeted CIPA, the law did not place an undue burden on speakers, and it did not significantly hinder adult access to protected speech. Specifically, public libraries' "use of Internet filtering software does not violate their patrons' First Amendment rights, CIPA does not induce libraries to violate the Constitution, and is a valid exercise of Congress' spending power" (Id p. 17). The government finally had its victory and CIPA remains in force today.

That being said, the Court did leave some room for future legal challenges to this policy. Perhaps in acknowledgment of the opposition's anxieties, some justices would admit that the law may not, in application, function as Congress intended. Based on the use of commercial filtering software in public institutions, the Court expressed some concern that "If some libraries do not have the capacity to unblock specific Web sites or to disable the filter or if it is shown that an adult user's election to view constitutionally

protected Internet material is burdened in some other substantial way, that would be the subject for an as-applied challenge" (CIPA18a p. 1). It was quite clear that if the filters were to demonstrate any of the negative tendencies the opposition had described then, for the Court, "it goes without saying that our decision today would not foreclose an as-applied challenge" (CIPA18b p. 3).

With this in mind, it is important to note that, despite the Supreme Court's ruling, many of the opposition's arguments have proven to be prescient in the years following the passage of CIPA. The harms they identified at the outset of this debate are ongoing (see Mauger, 2012) and, although the technical processes of filtering software have been refined in the intervening years, they have not been perfected. For example, the ten most highly rated filtering products today all continue to rely heavily on URL and keyword-based filtering. Only two of these ten offer "dynamic blocking" or the "ability to block or allow a website based on the ever-changing content on a website as opposed to its URL" (Top Ten Reviews, 2014). Furthermore, as recently as 2012, CyberPatrol (one of the products named specifically in the 1999 Senate Report on CIPA) still invited customers to "block sites by category" and "select pre-set profiles" for inappropriate content (CyberPatrol Online Protection Pro: Features, 2012). Manufacturers continue to market the CyberPatrol software directly to public institutions in order to "make it easy to block adult and obscene material and help keep schools and libraries CIPA compliant" (CyberPatrol Library Web Filtering: CIPA Compliance, 2012). The categories and profiles employed by this software remain undisclosed.

Furthermore, while the software's categorization of websites has undoubtedly become more sophisticated, many products still fail to discern between legitimately

harmful content and constitutionally protected speech. For example, in 2012 a court ordered the Camdenton School District of Central Missouri to cease its use of a filtering product designed to categorize LGBT content as unacceptable. In an effort to comply with CIPA's requirements, the school district had installed filtering software that consistently and methodically "target[ed] the highest-quality informational sites that express a positive viewpoint toward LGBT individuals" (*PFLAG v. Camdenton,* 2012). This kind of categorization bias is not limited to public schools. For instance, an adult patron sued a regional public library consortium in Washington State in federal court on constitutional grounds. In this case, the libraries had installed FortiGuard, a commercial filtering product that blocked access to the website womenandguns.com. This Second Amendment Foundation, a "Washington nonprofit corporation dedicated to issues associated with the constitutional right to keep and bear arms" (*Bradburn v. NCRL*, 2006), published the site. Although considered controversial by local administrators, this site clearly contained material that dealt with constitutional issues.

Commercial filtering products continue to dominate the landscape for institutions subject to CIPA. While these regulatory technologies have undoubtedly blocked access to content inappropriate for minors in the intervening years, it is equally true that filters have blocked material not contemplated by CIPA. It remains to be seen if this technology will continue to dictate the acceptability of content or if constitutional confrontations will require a critical re-evaluation of their use.

Table 7 – Children's Internet Protection Act Frame Analysis Summary

Frames	Legislative Themes
Master (Motivation)	• With the CDA dead and COPA in limbo, Congress intended CIPA to address the continuing issue of protecting children online. • In order to observe constitutional concerns while safeguarding kids, Congress narrows CIPA's target of enforcement to public schools and public libraries. • The master frames remain inflexible and Senator McCain continues to suggest that First Amendment protections are secondary to the protection of children.
Diagnostic (Problem)	• Congress targeted schools and libraries as a point of access for minors that is uniquely within the government's control. • Legislators tied federal funding for Internet access to the requirement that schools and libraries provide a filtered online environment for minors. • Congress has not significantly altered the diagnostic frame. Lawmakers remain convinced that unregulated access is a harm and this perspective does not appear to be open for debate.
Prognostic (Solution)	• Congress shifted the primary enforcement mechanism to commercial filtering software that teachers and librarians must administer. • Lawmakers suggest that commercial filters are the best solution because schools and libraries can customize them to meet community standards of decency and disable them upon request. • By adjusting CIPA's preferred regulatory technology, the government has demonstrated some flexibility in the kinds of technological solutions they are willing to consider.

Frames	Oppositional Themes
Master (Motivation)	• CIPA continued to be a threat to individual autonomy and constitutionally protected speech online. • Although Congress had again narrowed the target of the law's enforcement, the opposition argued that CIPA must still preserve access for adults within public libraries. • The opposition argued that legislators had not carefully considered the implications of commercial filtering systems for rights, autonomy, or transparency.
Diagnostic (Problem)	• The opposition framed commercial filtering systems as biased and overly restrictive mechanisms for the regulation of online content. • The imposition of filtering software at public access points would constrain adult rights and would require adults to request access to protected speech affirmatively. • The opposition argued that the installation of filters, their technological categorization schemes, and trade secret opacity limited rights and autonomy illegitimately.
Prognostic (Solution)	• The primary solutions are either to strike CIPA down as unconstitutional, or to pursue other, less intrusive alternatives such as public education or computer privacy screens. • CIPA was unconstitutional because of both the technological requirements of the law and the burden placed on adults by the "disabling provision". • If libraries voluntarily chose to implement filters, or if adult patrons were able to access unfiltered computers, this offered a better solution than government-mandated filtering through flawed commercial systems.

Children's Internet Protection Act Documentation Index

CIPA01	Children's Internet Protection Act of 2000, (CIPA), Pub. L. No. 106-554 (Tit. XVII), (codified at 20 U.S.C. § 9134 (f) and 47 U.S.C. § 254 (h)).
CIPA02	Cohen, H. (1998, June 29). *Constitutionality of Draft Bill to Require Federally Funded Schools and Libraries to Block Minors' Access to Computer Obscenity* [Memorandum].
CIPA03	Senate Report No. 105-226 (June 25, 1998).
CIPA04	105 Congressional Record (1999) E1602, 1602-1603 (statement of Representative Istook).
CIPA05	Senate Report No. 106-141 (Aug. 5, 1999).
CIPA06	Multnomah County Public Library v. United States, Civil Action No. 01-CV-1322 (E.D. Pa. 2001). Expert Report of Benjamin Edelman.
CIPA06a	Multnomah County Public Library v. United States, Civil Action No. 01-CV-1322 (E.D. Pa. 2001). Expert Rebuttal Report of Benjamin Edelman.
CIPA07	Smith, M.S. (2006, January). *Internet: Status Report on Legislative Attempts to Protect Children from Unsuitable Material on the Web* (CRS Report No. RS21328).
CIPA08	McCain, J. (2000). Children's Internet Protection Act Approved by Senate [Press Release]
CIPA09	American Civil Liberties Union. (2003). ACLU Urges Supreme Court to Reject Law Mandating Internet Censorship in Libraries [Press Release].
CIPA09a	American Civil Liberties Union. (2002). Affirmative Action and Online Free Speech Cases Once Again Loom Large on Supreme Court Docket [Press Release].
CIPA09b	American Civil Liberties Union. (2002). Students, Educators, and Activists Speak Out Against Federally Mandated Blocking Software in Schools [Press Release].
CIPA09c	American Civil Liberties Union. (2002). In Legal First, ACLU Sues Over New Copyright Law: Says Blocking Program Lists Should Be Revealed [Press Release].
CIPA09d	American Civil Liberties Union. (2002). Librarians Take the Stand in First Day of Trial on Government Censorship in Libraries [Press Release].
CIPA10	American Library Association. (2001). American Library Association files lawsuit challenging Children's Internet Protection Act [Press Release].
CIPA10a	American Library Association. (2001). CIPA remarks by Nancy C. Kranich [Press Release].
CIPA10b	American Library Association. (2001). CIPA remarks by John W. Berry [Press Release].
CIPA10c	American Library Association. (2001). CIPA remarks by Judith F. Krug [Press Release].

CIPA10d	American Library Association. (2001). CIPA remarks by Theresa Chmara [Press Release].
CIPA11	American Library Association, et al. v. United States, Civil Action No. 01-CV-1303 (E.D. Pa. 2001). Complaint for Declaratory and Injunctive Relief.
CIPA12	American Library Association, et al. v. United States, Civil Action No. 01-CV-1303 (E.D. Pa. 2001). Response in Opposition of Plaintiffs The American Library Association, et al. to Defendants' Motion to Dismiss Plaintiffs' Complaints.
CIPA13	American Library Association, et al. v. United States, Civil Action No. 01-CV-1303 (E.D. Pa. 2001). Opinion of the Court.
CIPA14	United States, et al. v. American Library Association, et al., 539 U.S. 194 (2003). Brief for the United States.
CIPA15	United States, et al. v. American Library Association, et al., 539 U.S. 194 (2003). Brief Amici Curiae of Senator Trent Lott, Congressman Charles W. "Chip" Pickering, Congressman Mark Souder, and Congressman Roger F. Wicker in Support of Appellants.
CIPA16	United States, et al. v. American Library Association, et al., 539 U.S. 194 (2003). Brief of Appellees American Library Association, et al.
CIPA17	United States, et al. v. American Library Association, et al., 539 U.S. 194 (2003). Brief of Appellees Multnomah County Public Library, et al.
CIPA18	United States, et al. v. American Library Association, et al., 539 U.S. 194 (2003). Opinion of the Supreme Court of the United States.
CIPA18a	United States, et al. v. American Library Association, et al., 539 U.S. 194 (2003). Concurring Opinion of Justice Kennedy.
CIPA18b	United States, et al. v. American Library Association, et al., 539 U.S. 194 (2003). Dissenting Opinion of Justice Souter.
CIPA18c	United States, et al. v. American Library Association, et al., 539 U.S. 194 (2003). Dissenting Opinion of Justice Stevens.
CIPA18d	United States, et al. v. American Library Association, et al., 539 U.S. 194 (2003). Concurring Opinion of Justice Breyer.
CIPA19	U.S. House of Representatives, Subcommittee on Telecommunications and the Internet of the Committee on Energy and Commerce. *E-Rate and Filtering: A Review of the Children's Internet Protection Act*, Hearing, April 4, 2001 (Serial No. 107-33). Washington: Government Printing Office, 2001.
CIPA20	Cohen, L. (2009, January). *Obscenity and Indecency: Constitutional Principles and Federal Statutes* (CRS Report No. 95-804).
CIPA21	Concurrent Resolution Expressing the sense of Congress that the Children's Internet Protection Act is constitutional as it applies to public libraries, H.R. Con. Res. 88, 108th Cong. (2003).
CIPA22	Concurrent Resolution Expressing the sense of Congress that the Children's Internet Protection Act is constitutional as it applies to public libraries, H.R. Con. Res. 441, 107th Cong. (2002).

CIPA23	"Request for Comments on the Effectiveness of Internet Protection Measures and Safety Policies." *Federal Register*, 67:103 (29 May 2002) pp. 37396-37398.
CIPA24	109 Congressional Record (2000) S5629, 5629-5648.
CIPA25	U.S. Senate, Committee on Commerce, Science, and Transportation. *Internet Indecency*, Hearing, Feb. 10, 1998 (ISBN 0-16-058290-3). Washington: Government Printing Office, 1998.
CIPA26	Department of Commerce. National Telecommunications and Information Administration. Children's Internet Protection Act Pub. L. 106-554: Study of Technology Protection Measures in Section 1703. Washington: Government Printing Office, 2003.

Chapter 7 – The Stop Online Piracy Act

Introduction

With the Supreme Court's 2003 decision on CIPA, Congress had finally passed legislation designed to protect children from the dangers of harmful online content. CIPA was the end result of a lengthy and contentious political process that demonstrated the resonance of this master frame but that also exposed the weaknesses of policy that relied on broad technological mechanisms of enforcement. Use of these regulatory systems had a propensity for curtailing individual rights and content regulation schemes that relied on them had negative constitutional implications. This was especially true in the context of the Internet and the vast democratic forum it represented.

Despite the difficulties that had confronted supporters of the CDA, COPA and CIPA, some members of Congress advocated for the expanded use of regulatory technologies in other policy domains. These proponents of content regulation again turned to these systems when confronted with a new threat to America's interests. Specifically, supporters of the Stop Online Piracy Act (SOPA) and the PROTECT Intellectual Property Act (PIPA) argued that technological mechanisms of enforcement were the only solution to the problem of online copyright and counterfeiting violations. Again these legislators would marvel at the continuing "advances of technology, and in particular, those represented by the Internet" (SOPA23 p. 6) while lamenting those bad actors who "facilitate the illegal distribution of copyrighted works through many different forms, including streaming, downloading, or linking to another site or service offering unauthorized content" (SOPA06 p. 73). Congress offered SOPA, PIPA and regulatory technology as the only solution to this problem.

Part I – Legislative Master Frames

The desire to protect intellectual property and to safeguard national security were the primary motivations behind these new policy proposals. Lamar Smith (R-TX) first proposed H.R. 3261, or SOPA, in the House by Representative in October of 2011. Patrick Leahy (D-VT) had introduced a bill nearly identical to SOPA in the Senate in May of that same year. The Senate version would become known as the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 (PROTECT IP Act) or PIPA. Both policies had similar stated goals and Smith presented SOPA as a means "To promote prosperity, creativity, entrepreneurship, and innovation by combating the theft of U.S. property" (SOPA01 p. 1). Again, the language used to promote PIPA was nearly identical and the purpose of this bill was "To prevent online threats to economic creativity and theft of intellectual property" (SOPA02 p. 1).

Both SOPA and PIPA were successors to The Combating Online Infringement and Counterfeits Act of 2010 (COICA). Proposed by Senator Leahy, COICA targeted websites dedicated to infringing activities and provided the blueprint for these new policy proposals. This included COICA's focus on technological mechanisms of enforcement, particularly its requirement that service providers and DNS operators impose a technological barrier to access between users and the domain names of allegedly infringing websites. Specifically, in language that foreshadowed SOPA and PIPA, COICA required that service providers "take technically feasible and reasonable steps designed to prevent a domain name from resolving to that domain name's Internet protocol address" and "the domain name registrar or domain name registry shall suspend operation of, and lock, the domain name" of infringing entities (SOPA27 p. 7).

COICA initially met with support from key members of the Senate and unanimously passed the Senate Judiciary Committee in a 19-0 vote on January 20, 2010 (SOPA28 p. 1). Despite this early approval, COICA eventually met with strong resistance from many of the same lawmakers who would offer similar concerns about SOPA and PIPA. Senator Ron Wyden (D-OR) was instrumental in postponing COICA and, based on his suggestion that this bill was moving too quickly, it was essentially tabled before it could come to a full vote (SOPA29 p. 1). This set the stage for a new round of legislation that would embody many of the same technological requirements and, as the opposition would argue, many of the same flaws as COICA. SOPA and PIPA provide the case for this frame analysis because they both embody and extend many of the same arguments against COICA. Additionally, SOPA and PIPA resulted in some novel oppositional approaches that did not manifest during COICA's brief history.

Supporters of these new policies were convinced that the Internet had become a clearinghouse for all manner of material that pirates had stolen, copied, counterfeited, and distributed without the consent of the copyright or patent holder. This phenomenon occurred to the detriment of American industry and the economy. Many in Congress argued that they must pursue a legislative solution to stem the tide of lost jobs and revenue resulting from stolen intellectual property. For these legislative supporters, both SOPA and PIPA were "fundamentally about jobs and about protecting the jobs that Americans have, creating products that are enjoyed all over the world" (SOPA06 p. 70). It was incumbent on Congress to "pass sound legislation" that would "provide tools to prevent websites…that do nothing but traffic in infringing material or counterfeits from continuing to profit from piracy with impunity" (SOPA23 p. 7).

The "tools" offered by Congress through SOPA and PIPA would invariably include an array of technological mechanisms designed to block access to any website deemed to be infringing. The primary targets of enforcement in this effort were the service providers, domain name systems (DNS), advertisers, and search engines that were, according to legislators, facilitating access to "rogue" websites (SOPA01 pp. 5-6). In the context of this legislation, Smith defined "rogue websites" as "foreign websites that are primarily dedicated to the illegal sale and distribution of counterfeit or pirated goods or foreign websites that market themselves as such" (SOPA04 pp. 1-2).

In order to combat these rogue sites, these policies obligated service providers, advertisers and search engines to "take the least burdensome technically feasible and reasonable measures designed to prevent" further infringement (SOPA02 pp. 9-10). In the case of search engines, Congress intended these technological measures to "prevent the foreign infringing site…from being served as a direct hypertext link" (SOPA01 pp. 16-17). This essentially meant that any rogue site suspected of or found to be violating U.S. intellectual property laws would be invisible in subsequent search results. For service providers and DNS operators, entire domain names were subject to these technological barriers in order "to prevent the domain name…from resolving to that domain name's Internet protocol address" (SOPA02 pp. 9-10). Again, the end result for any user attempting to access the contested site would be the effective removal of that site by the service provider. Both SOPA and PIPA absolved service providers of any action taken in defense of U.S. interests including any "voluntary action against websites stealing American intellectual property" (SOPA02 pp. 24-25). This provision was strongly reminiscent of the CDA's "Good Samaritan" blocking and ensured that there

would be no liability "if the entity acting in good faith and based on credible evidence has a reasonable belief that the Internet site is an Internet site dedicated to infringing activities" (Id). These technological barriers to access and the latitude given to private entities to block websites would be the most contentious issues surrounding this policy initiative.

In a rhetorical flourish that would contradict the statutory language, supporters of these bills would argue that "this legislation is ultimately not about technology" (SOPA06 p. 79). Instead, they argued that this kind of policy "focuses not on technology but on preventing those who engage in criminal behavior from reaching directly into the U.S. market to harm American consumers" (SOPA09 p. 1). Therefore, the need for federal regulation was a common sense extension of existing intellectual property protections. As the Motion Picture Association would suggest, copyright and patent represented "the foundation on which American industry has rested for over two hundred years" (SOPA06 p. 79). This cornerstone of the U.S. economy deserved the highest level of protection whether laws offered that protection online or off. While adequate laws existed for safeguarding physical property, new legislation was needed because "there is no equivalent protection for American companies from foreign online criminals who steal and sell American goods to consumers around the world" (SOPA10 p. 1). Senator Leahy agreed that the medium was unimportant in this quest to protect intellectual property and he asserted that "We cannot excuse the behavior because it happens on the Internet" and if it "existed in the physical world, everyone would agree that they should be shuttered and their proprietors arrested" (SOPA18 p. 189). These rogue websites were "no more than digital stores selling stolen" and "often dangerous products" (Id).

Confronted with such greed and lawlessness, Smith, Leahy and others insisted that lawmakers should extend federal policy to online infringers. Where the CDA, COPA, and CIPA had attempted to police indecent content, Congress intended SOPA and PIPA to regulate infringing content. In this instance, the master frame of protecting intellectual property would encompass legislators' insistence that they must no longer allow such rampant piracy to exist. In this view, the need for regulation trumped the need for unfettered access and freedom on the Internet. As Representative Smith would suggest, "Internet freedom does not and cannot mean Internet lawlessness" and "the goals of freedom and lawfulness are no more incompatible in the Internet space than they are in the physical world" (SOPA06 p. 40). In the interest of addressing Congress' master frame, Smith admitted that "crafting a bill governing the online environment requires attention to technological details" while insisting that by doing so it was entirely possible to "avoid unintended consequences, maintain the integrity of the Internet, and preserve certain freedoms" (Id). This would be a recurring theme throughout the debate over SOPA and PIPA and supporters of these policies would repeatedly assert that the protection of intellectual property online would neither censor speech nor implicate First Amendment rights. Freedom and regulation were not mutually exclusive and responsible legislation could accomplish one while preserving the other. As one supporter would argue, "Freedom of speech is not the same as lawlessness on the Internet. There is no inconsistency between protecting an open Internet and safeguarding intellectual property" (Id pp. 121-122). The opposition would not be as confident in this policy's commitment to free speech or the proposed technological mechanisms of enforcement and would argue vehemently that the net effects of these policies would harm individual rights.

Perhaps in anticipation of potential arguments against SOPA and PIPA, legislators and other groups in favor of regulation argued forcefully from the outset that these policies would not harm protected speech. SOPA and PIPA must be constitutional because they simply targeted "conduct that is already illegal" (SOPA07 p. 1) and, therefore, "Legitimate and lawful websites like Facebook, YouTube, and Twitter have nothing to worry about" (SOPA08 p. 1). There was no protection under the law or the First Amendment for theft and, from the legislative perspective, these bills eliminated threats to the U.S. economy while preserving the potential of the Internet as a public forum. Within this frame, legislators suggested strongly that these bills would "not threaten the Internet as a tool of communication and commerce" but they would "threaten the profits generated by those who willfully steal intellectual property by trafficking in counterfeit or pirated goods" (Id p. 2).

Considering the havoc piracy had wrought on U.S. interests, Smith and Leahy presented technological blocking of these rogue sites as the only answer. Despite their insistence that nothing in SOPA or PIPA was unconstitutional, when confronted with the choice between tough regulation and total freedom online, many legislators invariably chose the former over the latter. Any concerns about negative impacts on speech were summarily swept aside and lawmakers insisted that "it is constitutional to block access to a website that is primarily infringing, even though such blocking may incidentally impact protected speech" (SOPA06 pp. 139-140). Within this master frame, lawmakers must impose technological barriers to access at the DNS level and within search results in order to protect America's workers, artists, and entrepreneurs. Any incidental effect on speech, although regrettable, was not an excuse to sacrifice such vital U.S. interests.

Lawmakers admitted that "Prior restraint and censorship are antithetical to the First Amendment, but doing nothing in the face of rampant online piracy disgraces the goals of freedom of expression as well" (SOPA06 p. 268). The subtext of these arguments seemed to be that many in Congress were aware of the potential adverse effects of SOPA and PIPA for free speech but chose to pursue regulation anyway because economic interests trumped "lawless" freedom.

Legislators had constructed a strong master frame asserting that intellectual property was the cornerstone of the American economy and, in order to protect hard working citizens, it was the duty of the state to safeguard that property. It is no surprise then that Congress had to find a rhetorical solution to the conflict between speech rights and property rights. Time and again legislators made the case that "there is no inconsistency between protecting free speech and an open Internet and safeguarding intellectual property" (Id p. 113). In fact, within this master frame, supporters presented creative endeavors that resulted in copyrighted material as the very epitome of free speech. As such, creators of intellectual property were the "creators of free speech" (Id p. 37) and deserved the highest level of protection. Not only were piracy and counterfeiting illegal but they were an assault on the First Amendment itself. Therefore, "The notion that adopting legislation to combat the theft of intellectual property on the Internet threatens freedom of expression…is thus insupportable" (Id). From this perspective, SOPA and PIPA did not prohibit access or limit free speech, they simply punished "activity that is already illegal" (SOPA04 p. 1). Legislators insisted that "SOPA is a constitutional bill that protects free speech and America's intellectual property" simultaneously (Id). There was nothing special about the Internet that made it immune

from regulation and "simply because illegal activity occurs online does not mean that it is protected speech" (Id). Congress was convinced that these bills and the regulatory technologies they required were precise instruments that would excise only that content that encroached on intellectual property. Legislators would leave everything else as it was so that everyone could enjoy the benefits of a free and open Internet.

Piracy and other intellectual property violations were insidious for reasons above and beyond their impact on American economic interests. Legislators would offer an additional master frame suggesting that such infringement was also a danger to the health, safety, and well-being of American consumers. Supporters of SOPA and PIPA would argue that, while piracy was a major cause for concern, there were more sinister implications of such lawless behavior. Specifically, legislation was required in order to "protect trademark owners and consumers from counterfeit and unsafe products, like fake prescription medicines and misbranded drugs that are often presented to the public by unlicensed online pharmacies" (SOPA06 p. 1). This was nothing less than a menace to public health and these rogue websites did not limit themselves to prescription medication. Often, these illicit sites trafficked in counterfeit "automobile parts…baby formula, and other products that can pose serious threats to the health and safety of American citizens" (Id p. 38). In addition to the dangers posed by adulterated and mislabeled products, this kind of counterfeiting could "deteriorate[] the reputation of the legitimate maker of these goods" (Id). Those who supported such criminals, either directly through advertising or indirectly by including them in search results, were vicariously aiding and abetting behavior that "poses an unacceptable risk of serious bodily injury or death to our citizens" (Id p. 39). It was incumbent on such private

entities to support SOPA and PIPA in order to mitigate the damage that had been done and would continue to be done absent regulation.

Intertwined with this master frame related to public safety was the explicit assumption that counterfeit goods could cause harm to national security. While copyright infringement resulted in serious economic harm, the ready availability of counterfeit and mislabeled products was nothing less than an assault on America's infrastructure. Specifically, legislators argued that "The penetration of hazardous products and goods into the American marketplace, including our military supply chain, poses an unacceptable risk of serious bodily injury or death to our citizens" (SOPA06 p. 39). Rampant intellectual property violations were all symptoms of the same disease and it was necessary for Congress to act immediately to protect domestic interests. As one Senator would argue, "we do have to see this as urgent. It is too important to our economy and to our national security not to see it as urgent" (SOPA18 p. 22). SOPA and PIPA provided the best and most comprehensive solution to these dire problems because these policies specifically protected against the "trafficking in inherently dangerous goods or services" (SOPA01 pp. 60-64). Congress must erase websites dealing in these false and dangerous products from the Internet in order to safeguard public safety and national security. Illicit streaming of copyrighted works, counterfeiting prescription medication and dealing in fake military goods were all part and parcel of the same phenomenon. Therefore, from the legislative perspective, action had to be taken and, for policymakers, the "goal must be to confront the criminal enterprises that are flourishing on the Internet, stealing from the rightsholders, and visiting untold harm on consumers. Doing nothing is not an option" (SOPA06 p. 39).

Congress, then, offered SOPA and PIPA as the best means for countering the onslaught of piracy and counterfeiting. Targeting the "service providers, search engines, payment processors, and advertising networks" that facilitated these crimes was "essential to stopping the economic devastation caused by rogue websites" (Id p. 53). Technological blocking at the level of service providers and search engines was the only way to address this "rampant theft" (Id p. 72) and "blocking access to websites may be the only quick and effective course of action and…is therefore a critical part of the equation" (Id pp. 53-54). Although blocking may have some minor implications for free speech and unfettered access to information, the choice was clear. In the context of this strong and deeply resonant master frame, "It is a choice between illegal and legitimate. It is a choice between a safe, vibrant Internet for everyone and [an] all black-market Internet. It is a choice between protecting American creativity and jobs or protecting thieves. These are simple choices from our perspective" (Id p. 70).

Despite proponents' claims, it was not nearly that simple and groups opposing this legislation would frame these choices quite differently. Nonetheless, for many legislators and intellectual property advocates, the need for regulation was both obvious and immediate. In fact, these master frames were so strong and so intertwined with deep economic interests that they do not appear to have been amenable to alternative or critical assessments of these policies. Although SOPA's statutory language did call for further study, the purpose of that study was not to examine the technological mechanisms of enforcement required by the law. Instead, legislative supporters intended the report to detail the damage done by foreign infringers to the U.S. economy, not the potential damage done by these policies to individual citizens (SOPA01 pp. 53-54).

Part II – Oppositional Master Frames

The oppositional groups that coalesced around SOPA and PIPA represented a broad range of interests and stakeholders. These groups encompassed civil libertarians, network engineers, security experts, consumer groups, human rights advocates educational institutions and venture capitalists (SOPA06 p. 42). Online resources including Wikipedia and Google would also join this oppositional movement arguing that these policies would stifle creativity, entangle legitimate websites in regulatory obligations, and irreparably hinder free speech online. From this perspective, the opposition argued that Congress did not fully understand the regulatory mechanisms they were about to unleash on the Internet and the detrimental impact policies like SOPA and PIPA could have on individual rights. Google was one of the loudest voices in this opposition and, while sympathetic to the problems posed by online infringement, insisted that these laws "would expose law-abiding U.S. Internet and technology companies to new uncertain liabilities, private rights of action, and technology mandates that could require monitoring of web sites and social media" (Id pp. 101-102). The opposition believed that this policy initiative "sets a precedent in favor of Internet censorship" (Id).

The master frame used repeatedly in arguments against SOPA and PIPA emphasized the harm these policies would cause to the free speech and unfettered access to information that underpinned the Internet. By employing technological mechanisms of enforcement such as DNS blocking and filtered search results, Congress had imposed an overly broad mandate that reached into every corner of the Web. Groups including the American Library Association (ALA), Electronic Frontier Foundation (EFF) and Center for Democracy and Technology (CDT) believed that passage of these bills "would come

at too high a cost to Internet communication and noninfringing online expression" and "would set an irreversible precedent that encourages the fracturing of the Internet, undermines freedom of expression worldwide, and has numerous other unintended and harmful consequences" (Id p. 158). Instead of broad technical blocking and filtering, the opposition would argue vehemently that "We want to make sure that when we are dealing with speech, that we use a scalpel" (Id p. 137). SOPA and PIPA, on the other hand, would not only allow but require intermediaries to deny access to a great deal of legitimate content and websites that were in no way "dedicated to the theft of U.S. property" (SOPA01 p. 25). Furthermore, the opposition would make a strong case that the use of such technological "tools" encouraged the repressive behavior of authoritarian regimes that had already demonstrated the ability and willingness to curtail the online speech of their citizens.

The master frame of maintaining a largely free and open Internet was not limited to groups external to Congress. Many members of the Senate and the House expressed concern about the effects of these policies on free speech and the term "legislative frames" as used here is not meant to imply monolithic agreement. For example, Senator Ron Wyden (D-OR) would recognize the uncomfortable parallels between these new policy proposals and failed policies of the past. Senator Wyden essentially articulated some of the frame shifts that had (or had not) taken place in the interim between the CDA and SOPA. Wyden acknowledged that "Over 15 years ago, when Congress first started thinking about Internet regulation the concern was protecting children from pornography…and some argued that Congress should simply censor the Internet and use the government to cut off access to objectionable material" (Id p. 262). Yet Wyden and

others recognized in the interim that there "was value in letting the Internet develop free from corporate or government control" and rather than "having government censor the web" we should develop "an approach that would empower users and technology to address content concerns on their own" (Id). Here Wyden provided an excellent summation of both the government's attempts to pass the CDA and COPA and the oppositional stance that the Internet worked best when left mostly unregulated. Wyden also encapsulated the master frame that freedom and individual autonomy were inextricably bound to the ideals of free and open access. These cyberlibertarian ideals would again form the foundation of the opposition's arguments against SOPA and PIPA and demonstrated, from this point of view, that Congress continued to impose heavy-handed technological tools without clearly understanding the implications of such systems.

One of the opposition's key points was that Congress must act carefully and deliberately when considering copyright legislation – especially when those laws were meant to function in an online environment where discussion, linking, sharing and critical commentary were all intertwined. As the opposition would point out, "By their very nature, laws protecting copyrights constrain free speech and access to information" (SOPA12 p. 2). This was of particular concern if one believed that "access to information of all kinds – even disfavored information – is a fundamental right that must be protected" (Id). While supporters of SOPA and PIPA had insisted that these laws would "not censor legal activity on the Internet" but only "target[] activity that is already illegal" (SOPA04 p. 1), the opposition argued strongly that this conception of the law's impact demonstrated a gross misconception of how websites and social media actually

functioned. This misconception and the broad technological mechanisms that these policies called for would hinder an array of protected speech and stifle critical debate. As the opposition pointed out, "Copyright protection in theory only impacts the speech rights of those who would steal the rights in works entitled to protection. But the implementation of such a system can have an effect that goes far beyond the copyright pirate and restrict perfectly lawful non-infringing content" (SOPA12 p. 2). The requirement that search results be filtered and that DNS providers "delist entire domain names based on the criteria outlined in the bill would have the effect of chilling lawful speech" (SOPA18 p. 135). Essentially, these bills and the regulatory systems they would impose granted "new powers to both law enforcement and private actors to filter the Internet and block access" at the expense of protected speech (SOPA14 p. 4).

By requiring search engines to remove links to sites that inadvertently included infringing content or blocking the domain name of sites that simply linked to "rogue" actors, SOPA and PIPA had enormous potential to entangle vast amounts of legitimate speech. It was true that Congress primarily intended SOPA and PIPA to target foreign websites that represented the "worst of the worst" (SOPA06 p. 220). Nevertheless, because both of these bills allowed liability to extend to any website found to be "enabling or facilitating" (SOPA02 p. 3) infringement, the overall effect was that the law would sweep a great deal of blameless and worthwhile content into the same dragnet. As the opposition would point out, SOPA "targets an entire website even if only a small portion hosts or links to some infringing content" and enforcement "is not limited to foreign sites, or to the worst of the worst" (SOPA14 p. 6). Websites of all kinds would be subject to the vague and expansive statutory language of these bills.

With the inclusion of sweeping terms such as "enabling" and "facilitating," the opposition feared that SOPA and PIPA would force social media sites, blog hosts, video posting sites and many others to police the content uploaded by their users. From this perspective, ancillary service providers would be subject to the same blocking and filtering provisions as Internet service providers (ISPs), DNS providers and search engines. This presumptive requirement directly contradicted the safe harbor provisions of the Digital Millennium Copyright Act (DMCA) of 1998 that had specifically provided immunity for all content providers and hosting services. The DMCA made clear that these intermediaries were merely the conduits through which information flowed and it was in the best interest of Internet users and businesses to shield these entities from liability.[31] SOPA and PIPA offered no such protections and threatened to shut down a number of valuable services that simply hosted or linked out to content that might be infringing. Congressional supporters of SOPA and PIPA had strongly asserted that websites like Facebook and YouTube would not be subject to liability for secondary infringement because they were "not 'primarily dedicated to' illegal activity" (SOPA04 pp. 1-2). Despite reassurance that these services "have nothing to worry about" (Id), the opposition remained unconvinced. They argued that the extensive scope of these new laws would "bypass and effectively overturn the basic framework of the [DMCA], by pushing user-driven sites like Twitter, YouTube, and Facebook to implement ever-more elaborate monitoring systems to 'confirm,' to the satisfaction of the most aggressive and

[31] See DMCA, 17 U.S.C. § 512 - Limitations on liability relating to material online. As long as service providers met certain conditions and responded to reports of infringing content on their networks, these entities would "not be liable for monetary relief, or…for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connection."

litigious rightsholder, whether individual users are exchanging infringing content" (SOPA06 p. 158). SOPA and PIPA would essentially gut the DMCA's safe harbor provision and eviscerate the principle that "intermediaries need not monitor or supervise the communications of users" (Id p. 253).

Like the CDA's "Good Samaritan" blocking, SOPA and PIPA would also grant extraordinary police powers to private entities. Fear of vicarious or even direct liability for intellectual property infringement would encourage these service providers to practice heavy-handed blocking and filtering. Not only could the Department of Justice put direct pressure on providers to curtail access, but SOPA and PIPA also allowed copyright and patent holders to pursue private legal action. In order to "protect themselves, platforms of all kinds would be pressured to actively monitor and police user behavior" (SOPA13 p. 2) and any "rightsholder can pressure a service provider to censor a site…by threatening to sue the service provider with a claim of contributory infringement" (SOPA14 p. 9). Confronted with these direct and indirect threats and with a guarantee of immunity, any "service provider will have a strong incentive to shut down the accused website" (Id).

Oppositional groups and even members of Congress were "very concerned about the voluntary authority and legal immunity" that SOPA and PIPA would "give[] Internet service providers to block access to sites they reasonably believe are infringing sites" (SOPA06 pp. 235-236). With this power and without direct judicial oversight, service providers were likely to block a great deal of content preemptively. SOPA and PIPA not only encouraged but also required these private firms "to substitute their own judgment for that of law-enforcement officials and censor content without consequence" (SOPA18

p. 136). This was of particular concern if "ordinary users" did not have either "the resources or the technical know-how to contact DNS providers and contest the decision to take down lawful websites" (Id). This potential for unchecked private blocking also concerned some lawmakers and one legislator cautioned that service providers "can always err on the side of censorship because there are broad provisions…to censor something because you thought maybe it was a problem" (SOPA21 p. 1). Without some oversight, the opposition believed that the potential for private blocking would have drastic consequences well beyond any worthwhile intent the law might have. Giving this kind of blank check to private entities "to limit and censor Internet service providers and web sites…is like shooting an ant with an elephant gun" (SOPA06 p. 41). Opponents of these bills repeatedly expressed grave concern that the number and variety of websites subject to blocking would be extravagant and illegitimate, particularly if that filtering was the result of broad "voluntary immunity provisions that contain no court review" (Id p. 152).

The end result of this aggressive private blocking would be to condemn a vast number of websites to extermination without any legal recourse. There was no mechanism included within SOPA or PIPA that would guarantee website operators the chance to dispute claims of infringement prior to the delisting of their site or removal from search results. Without due process, these sites were "guilty until proven innocent" (Id p. 151) and would have to initiate a lengthy and potentially expensive court challenge against the service provider and/or rightsholder in order to argue their case. This created "a system that allows a mere accusation [of infringement] without any court review to lead to potentially damaging actions" (Id). This extra-judicial process was extraordinary

and conflicted directly with legislative claims that only those websites subject to an order from the Department of Justice would be "removed" from the Internet (SOPA04 p. 1). Despite these claims and due to SOPA and PIPA's vague language entangling sites (foreign or domestic) that were allegedly "enabling" and "facilitating" infringement, a multitude of service providers, search engines, advertising networks and other private entities would be encouraged to "shut down, block access to, and stop servicing U.S. and foreign websites that copyright and trademark owners allege are illegal without any due process or ability of a wrongfully targeted website to seek restitution" (SOPA14 p. 4). While there was some ability of targeted websites to submit a counter-notice against service providers and rightsholders, it was likely that the site would be removed and blacklisted so quickly that there was little chance to do so (Id p. 6). Also, due to the immunity provisions of these bills, the service provider, search engine or other entity had "no obligation to restore service once it receives a counter-notice" (Id). Essentially, there was "no due process for the innocent website owner to defend themselves before the action is taken or seek restitution after their website has been removed" (SOPA06 p. 222). Therefore, the opposition argued that this "legislation favors the copyright owner's intellectual property rights and, based on unfounded claims of infringement, strips the accused website owners from their property right" (Id).

Not only was the prospect of private blocking without due process a concern in and of itself, but it also set a dangerous global precedent. While the U.S. had strongly criticized the authoritarian Internet policies of countries like China and Iran (Id pp. 44-45), the opposition argued that SOPA and PIPA would impose the same illegitimate restrictions on speech. By implementing DNS blocking and by adulterating search

results, the U.S. was imposing on its own citizens the same repressive technologies it had criticized. Through SOPA and PIPA's technological requirements, the U.S. would be "legitimizing methods of online censorship to enforce its domestic laws" and "Non-democratic regimes could seize on the precedent to justify measures that would hinder online freedom of expression and association" (Id p. 159). If the U.S. were to employ the same technological measures, the opposition argued that it would essentially "abandon the moral high ground in the Administration's efforts to secure the ability for Internet users across the globe to access the legal content of their choice" (SOPA18 pp. 159-160). Once the U.S. had sacrificed that high ground, it essentially invited repressive regimes to "abuse their technological capacity to take down content they find objectionable or threatening" (SOPA12 p. 6). Mandated use of the technological mechanisms of enforcement required by SOPA and PIPA would directly encourage other countries "to use the same mechanisms to enforce a range of domestic policies" whether they be democratic or not (SOPA15 p. 2). Within the context of this master frame, the opposition was adamant that the U.S. "should not adopt a domestic policy that implicitly condones the very kinds of practices we attempt to condemn abroad" (SOPA18 p. 136).

For the opposition, SOPA and PIPA represented an existential threat to a free and open global Internet. This legislation would drastically change the way websites operated and it would force service providers to surveil users. For the opposition, these policies would destroy the democratic potential of the Internet.

Part III – Legislative Diagnostic Frames

Although SOPA and PIPA shifted the focus of content regulation from indecent to infringing content, the primary diagnostic frame remained largely unchanged. From the legislative point of view, a mostly unregulated and lawless Internet was harming American industry, its economy, and its consumers on a daily basis. In the case of intellectual property, supporters of this new legislation argued strongly that Congressional intervention was necessary to staunch the flow of money and jobs being lost due to piracy and counterfeit. The state required new mechanisms to combat this theft because "Technology has created a new front in this battle" (SOPA06 pp. 60-61). Lawmakers would wage this battle on the Internet where "rogue websites…are stealing American property, harming American consumers, hurting the American economic recovery and costing us American jobs" (SOPA23 p. 6). The strong protection of intellectual property was a regulatory necessity, particularly in "the virtual world where the systematic and willful violation of intellectual property rights now poses a clear, present, and growing danger to American creators and innovators, U.S. consumers, and our collective confidence in the Internet ecosystem" (SOPA06 p. 38). Where Senator Exon had warned that, without regulation, online dangers were always just "a few click-click-clicks away" (CDA14 p. 13) from children, supporters of SOPA lamented that American intellectual property was being stolen online "every day, over and over…sometimes with nothing more than the click of a mouse" (SOPA06 p. 72). Clearly, the Internet had exaggerated the harm to U.S. interests and it was incumbent on lawmakers to mitigate that harm with new and aggressive legislation.

When detailing the economic and financial harms embedded within this diagnostic frame, Congressional supporters of this new legislation certainly had a multitude of evidence to support their claims. American dominance in the global marketplace was at least partly "tied to the success of America's intellectual property industries" which "provide an estimated 19 million jobs to American workers and account for more than 60% of U.S. exports" (SOPA05 p. 1). As Representative Smith would argue, the rampant "online theft of America's intellectual property results in billions of dollars in lost revenue and thousands of jobs" (Id). Specifically, Smith contended that these crimes cost the domestic economy about $100 billion annually and these policy proposals would help "stop the flow of revenues to rogue websites" (SOPA06 pp. 2-3). The implication seemed to be that pirates, counterfeiters and trademark infringers were pocketing this vast wealth because the Internet essentially remained ''the wild, wild Web'' (SOPA18 p. 21) in the absence of regulation. This rhetorical definition of the problem also intimated that this enormous amount of money was being fed directly to "the criminals and organized crime cartels who profit from digital piracy and counterfeit products" (SOPA05 p. 1). The monetary harm inflicted by this phenomenon and the brazen outlaws who were profiting from it had to be stopped. Proponents argued that Congressional action was required because "existing tools are not strong enough to root out the worst online pirates beyond our borders" (SOPA23 p. 7).

This reference to the failure of "existing tools" was a pointed criticism of the DMCA and its perceived lack of protection for digital copyright. There was a growing sense among members of the content producing industry and within Congress that the DMCA had failed to accomplish its mission. While they acknowledged that the DMCA

had provided "some relief to copyright owners," they argued that it really only helped "in limited circumstances" (SOPA06 p. 1). These limitations meant that this outdated law provided "no effective relief when a rogue website is foreign-based" and did nothing to "assist copyright owners when rogue websites contribute to the theft of intellectual property on a massive scale" (Id). The DMCA was inadequate to deal with these new and exceptionally virulent forms of online infringement because the "means of willful and commercially destructive infringement" had advanced exponentially "since enactment of these [DMCA] provisions" (Id p. 76). Rightsholders desperately needed SOPA and PIPA to mitigate this harm and to close any "loophole in our nation's intellectual property laws" (Id).

While oppositional groups, including many in the technology industry, decried the loss of the DMCA's safe harbor protections for intermediaries, supporters of these new policies argued specifically that the law should hold these service providers and search engines to account. Those who advocated for new, more comprehensive regulatory mechanisms were convinced that "current legislation does not help us in enforcing our intellectual property" and the "safe harbor provisions of the DMCA, while well intended, have not functioned well" (SOPA18 p. 16). While SOPA and PIPA's staunchest allies railed against the failure of the DMCA and the safe harbor it provided (see footnote 31), more moderate supporters of content regulation offered a different interpretation of these new laws. Specifically, they insisted that search engines, payment and service providers would not be held to a new standard of liability and "cannot be held liable for the illegal or infringing actions taken by the rogue site" operating on their networks (SOPA04 p. 1). Nevertheless, the fact that immunity was contingent on the intermediary's agreement "to

remove the direct link to an illegal site" or "to stop working with the illegal site" (Id) tempered this reassurance. Not surprisingly, this somewhat contradictory point of view did not comfort many of the service providers, payment networks and search engines subject to SOPA and PIPA.

When confronted with oppositional arguments suggesting that SOPA and PIPA subverted the due process afforded to websites that might become entangled in this new regulatory scheme, supporters of this legislation swept aside such concerns and insisted that a great deal of judicial oversight protected entities affected by these policies. Legislators pointed to provisions within both bills that would require the Justice Department to "go to court and lay out the case against the site" and if "the judge finds that the site is primarily engaged in illegal activity, a court order can be issued that authorizes the Justice Department to request that the site be blocked" (SOPA08 pp. 1-2). Supporters argued that the blocking and filtering provisions of these policies would only be "required after significant due process and federal judicial oversight" (SOPA04 p. 3).

Although it is true that SOPA and PIPA included provisions requiring the Justice Department to seek judicial approval prior to technological enforcement, this did not necessarily apply to the ability of individual rightsholders to bring private action against websites or even intermediary service providers. For example, Section 103 of SOPA allowed a "qualifying plaintiff" to pursue independent legal action against anyone they believed were infringing upon their intellectual property. Such a "qualifying plaintiff" was broadly defined as any "holder of an intellectual property right harmed" by infringing activities (SOPA01 p. 27). Supporters of this legislation argued that any private action would be controlled by strict guidelines requiring the copyright owner to

provide "specific facts to support the claim that the Internet site, or portion thereof, is dedicated to the theft of U.S. property" and "clearly show that immediate and irreparable injury, loss, or damage will result" without immediate action (SOPA06 pp. 270-271). Nevertheless, when presented with a demand for action from a private rightsholder (even a demand that may have been unfounded), it remained in the best interest of intermediaries to act swiftly even in the absence of proof or counternotice from the website operator. Immunity from prosecution depended on timely cooperation from the intermediary and the "burden is on the [service provider] to defend its action (or inaction) under the threat of monetary sanctions" (SOPA14 pp. 2-3). In such a circumstance, it was likely that networks would block a site and erase it from search results prior to the presentation of any substantive proof and before the website owner had the ability to respond.

In practice, it was unclear how this private right of action would actually impact websites alleged to be infringing. The testimony of Go Daddy, one of the largest domain name registrars in the world, exemplified these contradictions. When asked to share her views on the Combating Online Infringement and Counterfeits Act of 2010 (COICA), Senator Leahy's first attempt to diminish online infringement and the immediate predecessor of SOPA and PIPA, Go Daddy's Executive Vice President, Christine Jones, offered conflicting testimony. COICA included many of the same blocking and filtering provisions of its successors and would have placed DNS providers like Go Daddy in the position of taking down entire domain names when confronted with a complaint from a private rightsholder. When asked about her company's position on these requirements, Jones asserted that Go Daddy was already "very aggressive in taking action against"

infringing websites but "to allay the fears of the EFF and ACLU", she specified that "our position as a default is to leave the website up" (SOPA18 pp. 8-9). Jones was very clear that her company was "in favor of the open exchange of ideas on the Internet" but that Go Daddy would "not provide a platform for illegal activity" (Id). While this would seem to validate the legislative position that private action would not result in significant overblocking, some confusion remained. In remarks made later in that same hearing, Jones reversed her position and noted that, in practice and "As the company that probably responds to more of these [takedown requests] than anybody else, our position is if there is any offending content, the whole website comes down" (Id pp. 31-32). Jones did note that Go Daddy would put websites back up once operators had removed infringing content but did not indicate how a website owner would be able to notify Go Daddy or prove to the rightsholder that they were in compliance.

Furthermore, the staunchest allies of content regulation felt even this response was too weak. Senator Richard Blumenthal (D-CT) was adamant that the constant removal and replacement of infringing websites was "an insufficient deterrent" and, for serial infringers, was simply "part of the cost of doing business" (Id pp. 32-33). Due directly to the weak and inconsistent response of service providers, Senator Blumenthal argued strongly that "a private right of action, with damages, maybe treble damages, punitive damages, and an effective enforcement mechanism is absolutely necessary" (Id). The implications for wrongly accused sites or for the free speech of sites inappropriately entangled in blocking and filtering requirements was negligible. If there was some "overuse or even abuse" of this system, the danger was "no different…than exists in many of our consumer protection laws where there are private rights of action and where

it imposes costs that are in effect commensurate with the damage that is done" (Id). Essentially, the medium made no difference and, even if lawful sites were harmed and protected speech hindered, the state must enforce laws on the Internet just as they are "enforced in the brick and mortar world…It's not censorship to enforce the law online" (SOPA08 pp. 1-2). In order to mitigate the harm of online infringement and counterfeiting, some in Congress had a made a strong case for expanded intellectual property rights, the need for rightsholders to be able to pursue intermediaries to stop infringement and the need for broad technological mechanisms of enforcement such as DNS blocking and search result filtration.

Perhaps in anticipation of oppositional concerns about First Amendment restrictions related to broad blocking and filtering requirements, legislative supporters of SOPA and PIPA addressed this issue throughout the debate over these two policies. For example, embedded in the opening text of SOPA, legislators guaranteed that "Nothing in this Act shall be construed to impose a prior restraint on free speech or the press protected under the 1st amendment to the Constitution" (SOPA01 p. 2). On the Senate floor, Senator Leahy offered the same promise for PIPA's provisions and reassured concerned groups that the Act would not entangle lawful websites and service providers in regulation that could curtail First Amendment speech. Specifically, Leahy asserted that "Nothing in PROTECT IP can be used to cut off access to a blog. Nothing in PROTECT IP can be used to shut off access to sites like YouTube, Twitter, Facebook, or eBay. Nothing in PROTECT IP requires anyone to monitor their networks. Nothing in PROTECT IP criminalizes links to other websites" (SOPA23 p. 7). Such promises not only addressed oppositional concerns but also strengthened the diagnostic frame that new

regulation and enforcement mechanisms were both necessary and constitutional. As noted previously, legislators insisted that the harm caused by online piracy and counterfeiting was so dire that the benefits of this new regulatory scheme were self-apparent and would only affect those bad actors who would steal America's economic lifeblood. Besides, from this point of view, free speech was "not the same as lawlessness on the Internet" and "Protecting intellectual property is not the same as censorship" (SOPA06 p. 114). Supporters portrayed oppositional arguments against SOPA and PIPA's enforcement mechanisms as alarmist and cast these legislative proposals as saviors of the U.S. economy. When faced with the opposition's arguments related to free speech, supporters of content regulation argued that such criticism was not only untrue but that "more robust enforcement of digital copyrights would likely lead to a stronger Internet ecosystem and more innovative content and services for consumers" (SOPA18 p. 138). To bolster this claim, legislators consulted "First Amendment scholar" Floyd Abrams who affirmed the government's position that nothing in either of these bills "threatens freedom of expression" (SOPA06 p. 25). Abrams laid out the case that "Copyright violations have never been protected by the First Amendment and have been routinely punished wherever they occur, including the Internet. This proposed legislation is not inconsistent with the First Amendment" (Id p. 37).

The perspectives of both the legislative supporters of these bills and those groups opposed to them represented nothing less than competing views about what the Internet should be. As one advocate for content regulation put it, the opposition's points of view betrayed "these groups' and individuals' overarching view of the Internet as a medium whose chief function is to liberate individuals from control by, or dependence on, big

organizations. For these groups, the Internet is first and foremost about individual freedom, not about collective responsibility" (SOPA18 p. 142). SOPA and PIPA's supporters were clearly of the opinion that such a cyberlibertarian conception of this medium was incorrect and dangerous to American interests. Regulation was a necessary part of responsible government and, from the legislative point of view, SOPA and PIPA offered the best of both worlds: through these Acts, Congress could successfully mitigate the harm of online infringement while preserving free and open discourse on the Internet. Technological blocking and filtering was both necessary and consistent with the First Amendment despite what opposition groups, service providers, and search engines might suggest. The legislative diagnostic frame of protecting America's property resonated strongly with these supporters precisely because it was both an economic necessity and a core value. When confronted with views opposing this position, advocates of content regulation were not disposed to take kindly to those groups who they saw as apologists for pirates and counterfeiters (SOPA23 p. 7). It is perhaps because of this and because of the resonance of this diagnostic frame that there was very little critical reflection of the practical and ethical impacts of these legislative proposals. Rather than acknowledging the technical realities of broad blocking and filtering, legislative supporters instead suggested that such arguments were simply obstructionist. Arguments for free speech and against illegitimate restrictions on access were "simply taken from the playbook of those people who have consistently opposed every effort that the Congress has come forward with in the past few years to protect intellectual property" and these groups were simply guilty of making "false and incendiary charges…designed to inflame emotions" (Id).

Part IV – Oppositional Diagnostic Frames

Oppositional groups and concerned members of Congress, while sympathetic to the problems posed by online infringement, were convinced that SOPA and PIPA would cause harms worse than those legislators meant them to address. Not only was the language of these bills vague but the blocking and filtering provisions recommended by Congress would be ineffective in combating online theft. The opposition also argued that the technological mechanisms of enforcement required by these policies would be easily circumvented, harming national security rather than protecting it. Additionally, removal of the DMCA's safe harbor protections would force intermediaries, search engines, and social networking sites to adopt practices that placed them in a monitoring and surveillance role that would ultimately be harmful to both user rights and legitimate free expression. Such requirements and strict content regulation would also encourage authoritarian regimes to continue repressive behavior that was damaging to critical discourse and political speech. As a legislator skeptical of these proposals, Representative Tom McClintock (R-CA) would argue on the House floor that "SOPA and PIPA pose a crippling danger to the Internet because they use legitimate concern over copyright infringement as an excuse for government to intrude upon and regulate the very essence of the Internet – the unrestricted and absolutely free association that links site to site, providing infinite pathways for commerce, discourse, and learning" (SOPA25 p. 1). McClintock would concisely summarize the opposition's chief concerns and diagnostic frames by noting that "Upon mere accusation, these measures would allow the government to shut down Web sites, ruin honest businesses, impound property [and] disrupt legitimate speech" (Id).

One of the primary reasons why the opposition believed SOPA and PIPA to be so harmful was the inclusion of vague and broad language requiring intermediaries to deny access to a wide range of content that was not infringing. SOPA in particular was targeted for this reason and oppositional groups contended that the "problem begins with the sweeping definition of a website 'dedicated to theft of U.S. property'" (SOPA14 p. 5). This language did nothing to define what constituted "dedication" to theft clearly and did nothing to alleviate the concern that the law could sweep primarily legitimate sites into blocking and filtering schemes merely by association through links or other non-substantive connections. It was conceivable that, "Under this definition, a site is 'dedicated to the theft of U.S. property' if even a portion of it 'enables or facilitates' someone else's infringement" (Id). With such a broad and unspecific mandate, intermediaries and service providers would have no clear guidelines for policing infringing content on their networks and, in order to retain immunity protections, would have no incentive to refrain from taking down questionable websites preemptively. Lacking clear instructions and with a potential barrage of complaints from individual rightsholders, the opposition argued that SOPA was "vague and ripe for abuse, particularly when combined with a private right of action for rightsholders" (SOPA06 p. 204). In the context of the opposition's diagnostic frames, this ambiguous standard had the potential to harm a multitude of legitimate websites and silence a great deal of legitimate speech.

In addition to the immediate effects of blocking and filtering, many of those opposed to SOPA and PIPA were concerned that the technological enforcement of these laws would require additional regulatory mechanisms above and beyond those already

described. While service providers were obligated to "take technically feasible and reasonable measures designed to prevent access" to infringing sites (SOPA01 p. 14), including the prevention of access to specific domain names, these entities were not strictly limited to such methods. Due to this and because, "the service provider domain name remedy is not the exclusive remedy, the Attorney General and a judge can require a service provider to create other technology solutions to block access to illegal sites. What else might be required beyond these steps is not specified" (SOPA14 p. 7). The bill provided search engines, service providers, advertisers and payment providers with an affirmative defense if they did not have "the technical means to comply…without incurring an unreasonable economic burden" but, as the opposition would point out, this was "a highly ambiguous standard" (Id p. 8). Furthermore, it was conceivable that these intermediaries would bear the burden of proof when attempting to qualify for this defense and "would presumably be required to provide expert testimony, subject to cross-examination, to establish that it had met its burden" (Id). Again, this ambiguity was distressing to the opposition because it could impose new and invasive technological requirements on them and their customers. In turn, users and legitimate websites would bear the brunt of any overly aggressive blocking and filtering with all of the inherent implications for speech such measures would have.

The opposition would also argue that, in addition to its ambiguity for intermediaries and the collateral harm visited on legitimate websites, neither SOPA nor PIPA would have much impact on digital piracy or counterfeiting. Due to the realities of online infringement, websites truly dedicated to piracy would continue to do business as long as they made a profit. The profitability of infringement all but ensured that "tech

savvy criminals around the world will find ways" to continue their activities whether Congress passed SOPA and PIPA or not and "ordering ISPs and search engines to disappear websites from the Internet will not change this fundamental reality" (SOPA06 p. 100). As will be discussed shortly, the opposition would make a strong case that, although harmful to legitimate speech, the technical blocking and filtering required by these policies were extraordinarily easy to circumvent thus strengthening the argument that pirates and counterfeiters would continue to operate despite SOPA and PIPA. Legislative opposition to these bills also adopted this argument and Congresswoman Zoe Lofgren (D-CA) would echo the sentiment that, if passed, these laws would result in "major costs and unintended consequences, while doing little to achieve the laudable goal of reducing online piracy" (SOPA06 p. 43). The CDT would take this argument one step further, specifying that the DNS filtering required by these policies would incur major costs by interfering "with core Internet infrastructure" while having "little effect on infringement" (SOPA13 p. 2). For the CDT and other groups, the unintended consequence of greatest concern was that "Where DNS filtering does have an effect, for technical reasons its impact is likely to be overbroad and result in blocking lawful expression rather than just infringement" (Id). The technical realities of this regulatory scheme were not only harmful from the opposition's perspective but their inclusion in this legislation underlined a grave misunderstanding of their implications on the part of legislative supporters. The failure of some in Congress to examine the consequences of these technological barriers to access was of deep concern to both the technology industry and civil libertarians. A broad coalition of industry and activist groups argued forcefully that "The proposed DNS technological remedy is not only ineffective and risky

to critical infrastructure; it runs contrary to the U.S. government's commitment to advancing a single, global Internet and free flow of information across it" (SOPA14 p. 10).

As alluded to above, those with the technical ability could easily circumvent the technological blockades mandated by this legislation. Meanwhile, innocent users without such skills and legitimate websites that depended on traffic for reasons of discourse or commerce would suffer the greatest harm from blocking and filtering. Those sites truly dedicated to online infringement and those individuals determined to seek out infringing material would continue to do so whether such sites appeared in search results or not. Similarly, the failure of a site's domain name to resolve due to DNS blocking did not erase it from existence. Although blocking obscured the site's name, the underlying numeric Internet Protocol (IP) address would continue to function quite well. With an IP address, anyone could continue to access an infringing site by entering those numbers in their browser. As Congresswoman Lofgren would point out, "the domain filtering scheme envisioned by [this legislation] will not be effective. Anyone determined to reach a blocked site may do so easily, merely by typing in the website's IP address…Any ten year old could do it" (SOPA06 p. 43).

This was not only the conclusion reached by concerned legislators and activist groups but also of the technology sector. Citing reports from "Leading Internet security engineers," the opposition asserted strongly that "the proposed measures to block the domain name from resolving to the Internet Protocol address ('DNS remedy') will not work because it…is easily circumvented by the user or targeted website" (SOPA14 p. 10). Since technically savvy users could find easy routes around any DNS blocking and

because it was an inconsequential matter for any infringing site to adapt to the block, SOPA and PIPA's enforcement mechanisms would meet with little success. As the CDT would suggest, these "filters will be trivial to circumvent, and will thus have too small and diminishing impact on infringement" to warrant the damage they could do to individual rights and online activity (SOPA13 p. 2). This damage was not simply hypothetical and previous incidents had demonstrated the collateral damage done to innocent websites. For example, in 2011 the Department of Justice mistakenly shut down mooo.com as part of an operation to seize ten domain names suspected of hosting child pornography (Samson, 2011). What federal law enforcement failed to realize was that mooo.com is one of the largest domain sharing projects on the Internet (mooo.com, 2014). In seizing this larger domain, the Justice Department inadvertently blocked "upwards of 84,000 innocent subdomains" which were clearly not trafficking in child pornography (SOPA15 pp. 1-2). Perhaps in reference to this mistake, Go Daddy, one of the largest domain name registrars on the web, would caution the government that ancillary harm "based upon the filtering of lawful sites is a stark reality" (SOPA18 p. 54). Due to these concerns and "combined with the fact that DNS filtering is unlikely to actually stop anyone who wants to visit the websites that contain infringing or counterfeit content" the opposition was convinced that "DNS filtering is an ineffective mechanisms for combating the theft of intellectual property online" (SOPA18 p. 54).

The ease with which users could circumvent these technological measures created an additional harm above and beyond those mentioned above. Due to the likelihood that these laws would block a great deal of material, innocent and infringing, the opposition argued that SOPA and PIPA would frustrate the autonomous ability of the individual to

seek out the content they were looking for. Overly aggressive blocking and filtering would drive many users to circumvention techniques and away from secure DNS servers and other protected service providers. Again, as Go Daddy warned, "The widespread implementation of DNS filtering would absolutely result in a large number of Internet users attempting to circumvent such filtering" (Id). The impact of this exodus from legitimate intermediaries would be extraordinarily destructive to U.S. cybersecurity efforts. While the government had insisted that access to counterfeit goods and adulterated medications would harm national security and consumer safety, the opposition argued that mandated DNS filtering would be even more damaging to a secure Internet. Specifically, this would severely limit the effectiveness of the Domain Name System Security Extensions (DNSSEC), an initiative that had "high-level US Government support and investment" (SOPA06 p. 152). DNSSEC added a layer of security to data sent across various networks by providing "secure authentication" of those packets in a way that was "critical for combating the distribution of malware and other problematic behavior" (Id). Without this authentication and protection, users would be vulnerable to a multitude of bad actors who could exploit this potential gap in U.S. cybersecurity. In addition to forcing users away from secure service providers, SOPA and PIPA's DNS filtering provisions interfered with the authentication process. As the opposition and many involved with national security argued, "Altering DNS results…causes significant problems for cybersecurity" and such filtering would be "inconsistent with DNSSEC…and circumvention of filters will expose U.S. users and networks to increased cybersecurity risk" (SOPA13 p. 2). By attempting to access blocked sites by other means, the law would force users employ systems other than those

protected by DNSSEC. The DNS blocking requirements of SOPA and PIPA "would encourage consumers to use alternate servers, which would promote the development of techniques and software that circumvent the use of the DNS and, therefore, undermine the value, security and resiliency of a single, unified, global communication network" (SOPA06 p. 152). Despite these oppositional and industry concerns, supporters of content regulation would continue to argue that DNS blocking had no such implications for U.S. cybersecurity efforts and there was "no reason to suggest that the use of this technology by intermediaries in the U.S. would lead to" less secure outcomes (Id pp. 76-77).

Based on these concerns, the opposition had outlined strong diagnostic frames indicating that SOPA and PIPA's technological mechanisms of enforcement had the potential to harm free speech, legitimate websites, and U.S. cybersecurity. In particular, the DNS filtering provisions of these bills would drastically change the way that intermediaries, service providers, and social networking sites operated. Rather than enjoying safe harbor protections as conduits for Internet traffic and outlets for information sharing, SOPA and PIPA would force these entities to police the vast amounts of content they hosted in order to avoid strict sanctions from the Department of Justice or from private rightsholders. This created a situation where the law would force these intermediaries to surveil their users and the material that they created or shared with other users (SOPA14 p. 5). In addition to SOPA and PIPA's requirement that intermediaries block access to allegedly infringing sites, these private entities would also "impose new responsibilities on ISPs to scrutinize and screen all user traffic" (SOPA13 p. 2). As the CDT argued, Facebook, Twitter, YouTube and other sites would not be

immune from this requirement and this legislation "would chill the growth of social media and force sites to adopt a new role as content police…To protect themselves, platforms of all kinds would be pressured to actively monitor and police user behavior" (Id). Not only would this surveillance place users under new and intense scrutiny without any semblance of due process but it would also limit the discursive potential of these sites, undermining "social websites' central role in fostering free expression" (Id). This essentially unlimited surveillance and control of online behavior was, for the opposition, uncomfortably close to an authoritarian mechanism of control. These groups argued that, if Congress passed SOPA and PIPA, it was not only damaging to the freedom of U.S. citizens but would also "set the dangerous international precedent that governments seeking to blocking online content that violates domestic law should look to online communications platforms as points of control" (Id).

This argument against surveillance and control underpinned the opposition's point that SOPA and PIPA could encourage authoritarian regimes to continue to repress their citizens. While the U.S. had "long been a strong advocate of for the protection and promotion of an open Internet" the technological blocking and filtering required by these policies "undermines its moral authority to criticize repressive regimes" (SOPA06 p. 160). By signing SOPA and/or PIPA into law, the U.S. would essentially be legitimizing oppressive technological mechanisms of control, sending "an unequivocal message to other nations that it is acceptable to censor speech on the global Internet" (Id). Without some moral high ground from which to criticize repressive regimes, it was entirely conceivable that "foreign governments [could] point to this law in order to rationalize new uses of DNS blocking to suppress internal speech" (Id p. 223). The opposition

argued vehemently that, when considering policies such as SOPA and PIPA, it was equally important to consider the "international ramifications" the use of such technologies "will have on free expression globally" (Id pp. 253-254). It was true that U.S. constitutional guarantees provided some protection for the exercise of individual rights but the opposition remained "concerned with the example that an overly broad online infringement scheme would set for other countries with fewer free speech protections" (SOPA12 p. 6). The harm that would result from these practices was inextricably tied to the regulatory technologies mandated by these policies and oppositional groups were convinced that the "proposed DNS technological remedy…risks setting a precedent for other countries, to use DNS mechanisms to enforce a range of domestic policies…that would hinder online freedom of expression and association" (SOPA14 p. 10). The same was true for the search engine filtering required by this legislation that was essentially, "government-mandated censorship of Internet search results" (Id). Like DNS blocking, the adulteration of search results set "an alarming precedent that undercuts" the ability of the U.S. to criticize similar mechanisms employed by repressive regimes (SOPA14 p. 10). Simply implying moral authority by claiming that SOPA and PIPA were aimed at the infringement of intellectual property rather than legitimate speech was insufficient and did nothing to differentiate it from other "filtering with more sinister motives" (SOPA15 p. 2). By enforcing strict content regulation, the U.S. would be "legitimizing methods of online censorship to enforce its domestic policies" in a way that was extraordinarily similar to authoritarian governments. So, not only could technological blocking and filtering harm the rights of U.S. citizens, but it essentially absolved repressive states of doing the same thing to their people.

Part V – Legislative Prognostic Frames

In the face of these concerns and confronted with such a large and varied coalition of oppositional groups, supporters of SOPA and PIPA began to falter. For the first time, a more nuanced and critical view of the technological mechanisms required by these bills forced legislative support for them to recede prior to intervention by the judiciary. Advocates of content regulation did, however, remain convinced that some legislative action was required to stop the theft of America's intellectual property. As part of the legislative prognostic frame, these supporters insisted that Congress must act in order to solve the problems of piracy and counterfeiting. SOPA and PIPA were necessary because they would "secure creators' rights online" and "help restore the security of copyright online" (SOPA06 p. 268). In order to ensure that U.S. economic interests were protected and to keep those profits out of the hands of bad actors (SOPA08 p. 1), SOPA and PIPA would help "American innovators by protecting U.S. intellectual property from foreign criminals" (SOPA07 p. 1). Lawmakers continued to insist that legitimate websites, intermediaries and social networking sites were in no danger because these bills made "clear that the legislation specifically targets the worst-of-the-worst foreign rogue websites" (SOPA08 p. 1). In the context of this prognostic frame, legislative intervention was also an economic necessity because the "problem of rogue websites is real, immediate and wide-spread. It harms all sectors of the economy" (SOPA09 p. 1). SOPA and PIPA must be part of any solution because, "Protecting America's intellectual property will help our economy, create jobs, and discourage illegal websites" (Id p. 2). The technological "tools" provided by these bills were a crucial part of any such solution.

Despite the insistence of some voices within Congress and from the content producing industry, the master and diagnostic frames offered by the opposition began to take their toll. For the first time, the opposition's point of view created a situation where legislative support for certain provisions within these bills began to erode. Specifically, the opposition had railed against the DNS blocking provision because it had the potential to be so damaging to individual rights and to the normal operation of intermediaries, search engines, and social networking sites. Due to the potential loss of the DMCA's safe harbor protections in favor of immunity contingent on technological blocking, this regulatory mechanism would drastically shift the role of these intermediaries from simple conduit to policed network. Also, because it would drive many users away from legitimate service providers while attempting to circumvent blocking and filtering, the DNS provision could be extraordinarily harmful to U.S. cybersecurity. All of these reasons forced even the staunchest supporters of SOPA and PIPA to back away from mandatory DNS blocking.

On January 13, 2012, Representative Smith issued a press release announcing that he would remove the DNS blocking provisions of SOPA from draft language of the bill. In recognition of the pressure placed on him, Smith acknowledged that "After consultation with industry groups across the country, I feel we should remove Domain Name System blocking from the Stop Online Piracy Act" (SOPA10 p. 1). This announcement came one day after Senator Leahy stripped the DNS provision from PIPA. In his own press release, Leahy also alluded to the barrage of criticism that had confronted this blocking requirement and the arguments put forward by an array of oppositional groups. Senator Leahy grudgingly acknowledged that the harms of this

provision might outweigh its benefits and that more study was needed prior to its inclusion in future drafts of the bill. Leahy admitted that, since introduction of PIPA on the Senate floor, he "and the bill's cosponsors have continued to hear concerns about the Domain Name provision from engineers, human rights groups, and others" (SOPA26 p. 1). Nevertheless, this acknowledgement was, at best, reluctant and Leahy seemed convinced that he had done all that was necessary to seek approval for this provision from the groups that mattered most - in this case, the ISP industry. Leahy seemed to imply that the criticisms of the opposition lacked merit despite the broad coalition of groups they represented. Specifically, he seemed to minimize oppositional concerns and Leahy remained "confident that the ISPs – including the cable industry, which is the largest association of ISPs – would not support the legislation if its enactment created the problems that opponents of this provision suggest" (Id). In a single press release, Leahy had bowed to oppositional pressure and simultaneously dismissed it. This encapsulated the legislative position that SOPA and PIPA remained the best and most appropriate solution to the problem of online infringement. Despite the removal of DNS blocking requirements, Leahy continued to stand behind PIPA and insisted that the "bill remains a strong and balanced approach to protecting intellectual property" (Id). Smith took a similar stance and noted that, even without the DNS provision, SOPA still "cuts off the flow of revenue to these foreign illegal sites and makes it harder for online criminals to market and distribute illegal products to U.S. consumers" (SOPA10 p. 1).

For the first time, legislators made drastic alterations to active bills before the opposition had filed a lawsuit. Even without the insistence of the courts, legislators like Smith and Leahy adopted oppositional concerns and bowed to pressure from a broad

coalition of stakeholders. Unlike the CDA, COPA or CIPA, during the debate over SOPA and PIPA the opposition compelled supporters to amend the technological requirements of these bills based on concerns over free speech and the loss of a mostly unregulated Internet. Advocates of content regulation, perhaps sensing the direction of public opinion, initiated a frame shift of their own and discarded a controversial mechanism in order to preserve the master frame of protecting America's intellectual property. Specifically, support for these bills continued to describe the economic harms that online infringement caused, the lost jobs and compromised safety of American consumers. None of these frames deviated from the narrative that legislators had constructed even though they had scrapped a core provision of these bills. Leahy demonstrated this point most clearly by noting that he was removing the DNS blocking requirement from PIPA because it had become a distraction from the real issues. He was removing this provision not because of its implications for free speech or because the ISP industry felt it was dangerous but "so that we can focus on the other important provisions in this bill, which are essential to protecting American intellectual property online, and the American jobs that are tied to intellectual property" (SOPA26 p. 1).

Most interestingly, as part of this shift both Smith and Leahy acknowledged that the technical aspects of these bills required further study. Finally, they recognized that more critical review was a necessary component for crafting sound legislation and both press releases gave some attention to this issue. Specifically, Smith acknowledged that he was rescinding SOPA's DNS provision so that he and others "can further examine the issues surrounding this provision" (SOPA10 p. 1). The "issues" in this case presumably referred to the many concerns brought forward by the opposition. Senator Leahy was

more expansive on this point and suggested, "that the positive and negative effects of this provision be studied before implemented" (SOPA26 p. 1). Leahy acknowledged that this kind of remedy "is in fact a highly technical issue, and I am prepared to recommend we give it more study before implementing it" (Id). Despite this, Leahy's response seems to imply that the removal of DNS blocking was probably no more than temporary and, in the meantime, he expressed "regret that law enforcement will not have this remedy available to it when websites operating overseas are stealing American property, threatening the safety and security of American consumers" (Id). Perhaps this was simply political grandstanding and a way for Leahy and Smith to save face while regrouping. At the least, it demonstrates a level of pragmatism and a deep commitment to the master and diagnostic frames underpinning this legislation. Both Leahy and Smith, as those who introduced these bills, were willing to sacrifice what was perhaps the key technological mechanism of enforcement in order to ensure that legislation would go forward to protect U.S. intellectual property.

It is also interesting to note that, even though the sponsors had excised the DNS provision from these bills, all of the other controversial technological requirements remained. SOPA and PIPA still required payment providers and advertisers to cease all business arrangements with those sites suspected of infringing activity. Representative Smith was unyielding on this point and touted this aspect of SOPA even as he was admitting defeat on DNS blocking. Smith lamented the loss of the DNS provision but remained confident that SOPA would help resolve the problems of online piracy and counterfeiting by strangling the economic incentive of these bad actors. Even though DNS blocking had failed, Smith reassured concerned supporters that "the bill maintains

provisions that 'follow the money' and cut off the main sources of revenue to foreign illegal sites" (SOPA10 p. 1). SOPA's mandate for search engines also remained and the bill still required these intermediaries to filter search results for any website suspected of hosting, linking to, or being associated with infringing content. Again, Representative Smith made clear that this requirement would remain and that SOPA would continue "to protect consumers from being directed to foreign illegal websites by search engines" (Id). Finally, the private rights of action that had so concerned oppositional groups remained in force. Although domain names were safe for now, SOPA would continue to provide "innovators with a way to bring claims against foreign illegal sites that steal and sell their technology, products, and intellectual property" (Id).

So, while even the strongest of proponents had been forced to back down, they remained convinced that SOPA and PIPA, as well as the remaining technical provisions they included, were the best way to solve the problem of online infringement. Although Smith and Leahy had to publicly step away from DNS blocking due to oppositional pressure, they showed no sign of heeding similar warnings about the other regulatory systems required by these bills. Similarly, none of these legislative advocates seems to have taken seriously many other oppositional concerns such as those related to the entanglement of legitimate websites in overly restrictive enforcement, complications due to actions brought by private rightsholders and the precedent that search result adulteration would set for global Internet governance and for repressive regimes. Removal of the DNS provision from SOPA and PIPA was a victory for the opposition but it would be a small one if the remaining technical requirements were enforced.

Part VI – Oppositional Prognostic Frames

Even though DNS blocking was no longer part of the Congressional solution to the problem of online infringement, oppositional groups continued to express concern about the remaining technological provisions of these bills. As they had when confronted with the CDA, COPA and CIPA, these opponents would argue strongly that Congress must reconsider the technical requirements of such bills prior to passing them into law. Failing that, these groups insisted that the courts strike down such content regulation schemes as unconstitutional due to their detrimental impact on individual rights and speech on the Internet. In addition to arguments that had now become familiar, these groups would also pursue a much more aggressive and public form of activism that placed additional pressure on legislative supporters of these bills. In lieu of waiting to air their grievances in court, those opposed to SOPA and PIPA would take their complaints directly to the online spaces that they argued would be harmed so drastically by these laws. While the opposition to the CDA, COPA and CIPA had mostly consisted of a few activist groups and concerned professional organizations, those fighting against SOPA and PIPA represented a wide range of stakeholders with differing interests. Perhaps because of this breadth, the opposition here was able to fight a campaign against these bills and their technological requirements that was impossible to ignore. Websites as varied as Wikipedia and Reddit were able to place pressure on legislative supporters of these bills alongside Google, Facebook and other massive players in the Internet industry. Individual users also spoke out against SOPA and PIPA and, in the aggregate, were able to change the direction of U.S. policy. Essentially, these groups and individuals would make it impossible for legislators to continue to support these proposals.

As SOPA and PIPA progressed through the legislative process, members of both the House and Senate began to feel the political pressure placed on them by oppositional groups. Due to this pressure, many legislators began to take note of both the opposition's arguments against these bills and the impact that they could have on the Internet. For example, Congressman Henry Johnson, Jr. (D-GA) noted that some of these stakeholders including "the technology industry and payment processors" had "identified some legitimate concerns with SOPA" (SOPA06 p. 44). Johnson acknowledged the wide range of groups opposing these bills and drew attention to the fact that "public interest and civil rights groups such as the American Civil Liberties Union, the Consumers Union, and the Consumer Federation of America, have expressed concerns about this legislation" (Id). Confronted with such a broad yet unified opposition, Congressman Johnson expressed his own "concerns with the legislation in its current form" and strongly recommended that Congress "consider any unintended consequences SOPA may cause" prior to its enactment (Id). Johnson was not alone in his doubts about these bills and other legislators would begin to echo the opposition's calls for serious reconsideration of SOPA and PIPA. Representative J. Randy Forbes (R-VA) summarized this position well and adopted the opposition's criticisms. Forbes noted that "as drafted, SOPA presents serious free speech and free press concerns, and would allow the First Amendment rights of innocent, uninvolved Americans to be curtailed" (Id p. 41). Like the opposition, Forbes strongly suggested that "Congress would be well-served to go back to the drawing board and write a much more narrowly-tailored bill that reaches only the bad actors and offending parties" (Id). Forbes took this position almost verbatim from the opposition's vehement criticism that "SOPA as constructed would come at too high a cost to Internet

communication and noninfringing online expression" (Id p. 158). While the opposition had almost unanimously agreed that online infringement was a serious problem, they also were unanimous in their assertion that Congress should reconsider the language and technical requirements of SOPA and PIPA. Without serious reconsideration, the opposition agreed that "we cannot support SOPA, and in fact we oppose it in its current form, given its broad sweep and its heavy hand that will land largely upon innocent content producers" (SOPA12 p. 3). For the first time, a majority of legislators began to accept the wisdom of these critiques and adjusted their political positions accordingly.

Many legislators had also begun to agree that they could not enact SOPA and PIPA barring major revisions. As mentioned previously, Representative McClintock was one of the early adopters of this oppositional position and was personally convinced that the sponsors of these bills should remove them from consideration in the House and Senate. McClintock was adamant that neither bill should proceed due directly to their mandated technological mechanisms of enforcement. Specifically, McClintock would charge that "these measures would allow the government to shut down Web sites, ruin honest businesses, impound property, disrupt legitimate speech, and dragoon innocent third parties into enforcing laws that may or may not have been broken" (SOPA25 p. 1). Other legislators took up this perspective and argued that "SOPA and PIPA directly threaten the very Internet that has brought humanity great prosperity and even greater peace" (SOPA20 p. 1). Representative Jared Polis (D-CO) would go so far as to request that his colleagues take up the public outcry over these bills and "join in solidarity with Internet users across the world in making sure that we tackle online piracy in a way that doesn't throw out the baby with the bathwater" (Id). The opposition and now a great

many legislators agreed that SOPA and PIPA were "very poorly drafted" (SOPA21 p. 1) and included technological provisions that would almost certainly disrupt speech on the Internet. While it was universally agreed that "selling fake Nikes or movies you don't own is a problem that needs to be addressed," it was also true among a growing number of voices that the problem could be solved "in ways that do not threaten speech, that allow for the legitimate sharing of information and protect the architecture and value of the Internet" (SOPA22 p. 3).

Also for the first time, legislators began to call for a serious and critical review of the technological mechanisms required by SOPA and PIPA. Recognition of this need for sustained and detailed review of these technologies had been partly responsible for the demise of the DNS blocking provision and some legislators had taken note of the lack of technical expertise represented at hearings before Congressional committees. Representative Zoe Lofgren had drawn attention to this issue just two months prior to Leahy and Smith's press releases announcing the removal of this requirement from SOPA and PIPA. During the major hearing on SOPA, Lofgren had noted the one-sided nature of those invited to testify. Of the six witnesses, Lofgren found it troubling that "Five are in favor [of the bill] and only one is against" (SOPA06 p. 201). She also noted the serious "lack of any technical expertise on this panel" and the need for such voices when considering the consequences of "the DNS portions of this bill" (Id). When the technology industry became involved in the process, companies like Verizon had cautioned legislators that "Government-sanctioned website blocking represents a major shift in U.S. policy that requires careful consideration and input from a wide variety and group of stakeholders" (SOPA18 p. 11). Many legislators began to heed these warnings

and chastised their colleagues for not considering the political and constitutional implications of what they were proposing. Senator Ron Wyden (D-OR) noted on the Senate floor that Congress must begin to include a critical review of technological barriers to access prior to imposing them and that lawmakers must include a broad range of stakeholders in such conversations. Perhaps in reference to the broad coalition of groups opposing SOPA and PIPA, Wyden argued that Congress should begin to "construct legislation in a transparent way that responds to our broad collective interests" (SOPA22 p. 3). Wyden was also critical of the penchant of his fellow legislators to deliberate "behind closed doors" (Id) on issues and technologies that they may not fully understand. In Wyden's opinion, it was dangerous for legislators to impose technological barriers to access without some critical study and that there would continue to be "serious unintended consequences when Members of Congress and staff think they have all the answers and rush to construct and pass legislation" (Id). Wyden was adamant that legislators should not impose draconian restrictions on Internet access or "make assumptions about a medium that is still taking shape and that few in Congress fully understand" (SOPA06 p. 261). Other legislators took up this call for more serious deliberation and a more comprehensive understanding of that which Congress proposed to regulate. Senator Jerry Moran (R-KS) would argue that "Congress has the responsibility to remain engaged and up to speed on all issues" especially those involving such regulatory technologies (SOPA22 p. 4). These legislative calls for a critical review of regulatory systems and for a broader engagement with stakeholders and activist groups echoed the opposition. Dating back to the CDA, oppositional groups had repeatedly pointed to the need to engage with all interested parties "before we start imposing

liability in ways that could severely damage electronic communications systems [and] sweep away important constitutional rights" (CDA25 p. 32). In the debate over SOPA and PIPA, it appeared that the majority of legislators were starting to agree with this assessment.

More pragmatically, legislators may have also found it politically expedient to take note of the public criticisms made by a wide array of oppositional groups that had organized against this legislation. Opposition to SOPA and PIPA was both widespread and vocal in a way that had not presented itself during the conflicts over the CDA, COPA, or CIPA. Specifically, many high-profile players such as Wikipedia and Google organized to "black out" their respective services on January 18, 2012 in order to demonstrate that these bills would ruin the ability of intermediaries to function without fear of liability for infringing behavior on their networks. Wikipedia and the community of users it represented used this protest to highlight the potential damage these bills and their attendant technological requirements could inflict on this resource. While its administrators argued that Wikipedia did not actively aid in the infringement of intellectual property, they feared that SOPA and PIPA would eviscerate their ability to continue to link out to the additional sources that strengthened the reliability and authoritativeness of its entries. Importantly, Wikipedia did not represent a single individual or corporate entity but a non-profit community of users representing a large cross-section of individuals (and voters). Legislators took notice when such a large constituency argued so publicly that "SOPA and PIPA endanger free speech…and set a frightening precedent of Internet censorship for the world" (SOPA16 p. 1).

More than one hundred websites, search engines, networks and social media sites joined Wikipedia in an organized strike that drew the attention of the media, the public and, of course, those on Capitol Hill (sopastrike.com, 2014). Wyden again urged his colleagues not to ignore the millions of Americans "who visited Wikipedia [and] took action to influence their members of Congress" or the millions who "signed Google's petition to block consideration of PIPA" (SOPA22 p. 1-2). Through this widespread action, these oppositional groups, companies and individuals were able to draw attention to the dangers posed by SOPA and PIPA's mandated regulatory systems and, "empowered by the Internet" itself, "effected political change" (Id). Just two days later, on January 20th, Smith removed SOPA from consideration in the House indefinitely. PIPA met a similar fate and no legislator has reintroduced either bill in the intervening years. Smith and Leahy were forced to surrender the prognostic frames that had underpinned SOPA and PIPA based on the arguments put forward by the opposition and the immense network of activists that organized to protest these bills, Nonetheless, the master frame expressing the need to protect America's intellectual property remained at the forefront of Smith's rhetoric. In a final press release announcing the demise of SOPA, Smith admitted that "We need to revisit the approach on how best to address the problem" of online infringement, but made clear that he remained "committed to finding a solution to the problem of online piracy that protects American intellectual property and innovation" (Wasserman, 2012). Nevertheless, any future solution would not take the same technological approach nor was Congress likely to be enact it without some critical review of any proposed technological solutions or without input from a variety of interested groups.

Table 8 – Stop Online Piracy Act/PROPTECT IP Act Frame Analysis Summary

Frames	Legislative Themes
Master (Motivation)	• The government was motivated to pass SOPA and PIPA due to the desire to protect intellectual property and national security. • Legislative supporters of SOPA and PIPA were adamant that the law protect property at all costs and that free speech concerns were secondary. • These master frames are deeply entrenched and do not appear to be amenable to technologically critical perspectives
Diagnostic (Problem)	• Congress argued that the Internet was a clearinghouse for stolen intellectual property and for piracy. This caused grave economic harm to U.S. interests. • Supporters portrayed the Internet as a "lawless" medium that required intervention through policy and through technology in order to mitigate this harm. • Core political and economic beliefs form the basis for this diagnostic frame. Alternative interpretations of the Internet and digital rights were not persuasive.
Prognostic (Solution)	• Technological mechanisms such as DNS blocking, ISP filtering and search result adulteration were the best and only means for combating the theft of intellectual property online. • Lawmakers suggested that these regulatory systems would allow the U.S. government and private rightsholders to pursue criminal action against online infringers. • This prognostic frame eventually demonstrated that lawmakers were willing to sacrifice some technological solutions in order to preserve the master and diagnostic frames. This may be the best point for inserting an alternative view of regulatory technologies.

Frames	Oppositional Themes
Master (Motivation)	• SOPA and PIPA had the massive potential to restrict individual rights, autonomy, and constitutionally protected speech. • The technological mechanisms proposed by Congress were intrusive, overly broad, and burdensome for both online speakers and listeners. • Oppositional groups argued that legislators had not considered the implications of these enforcement mechanisms prior to including them in statutory requirements.
Diagnostic (Problem)	• DNS blocking, ISP filtering and search result adulteration would harm the ability of individuals and website administrators to operate without fear of criminal liability. • These technological systems would entangle legitimate websites and individuals in an overly zealous regulatory scheme. • The technical requirements of SOPA and PIPA would force providers and platforms to take on a surveillance and policing role.
Prognostic (Solution)	• The primary solutions were to strike SOPA and PIPA down as unconstitutional or to ensure that neither ever reached a vote in Congress. • For the first time, a grassroots movement of online actors took up protest and dissent as a means to draw attention to these policies and to address the flaws of these regulatory systems. • Through this prognostic frame, the opposition was able to sway public opinion and convince a number of lawmakers that these policies and technologies were damaging to rights, autonomy, and speech.

Stop Online Piracy Act Documentation Index

SOPA01	Stop Online Piracy Act of 2011, H.R. 3261, 112th Cong. (2011).
SOPA02	Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011, S. 968, 112th Cong. (2011).
SOPA03	Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 (Amended), S. 968, 112th Cong. (2011).
SOPA04	U.S. House of Representatives, Judiciary Committee. *Myth vs. Fact: Stop Online Piracy Act* (Undated).
SOPA05	Committee on the Judiciary. (2011). Senate, House Judiciary Committee Leaders Focus On Fighting Online Infringement [Press Release].
SOPA06	U.S. House of Representatives, Committee on the Judiciary. *Stop Online Piracy Act,* Hearing, November 16, 2011 (Serial No. 112-154). Washington: Government Printing Office, 2011.
SOPA07	Smith, L. (2011, December). Lamar Smith defends SOPA [Letter to the editor]. *Politico*, Retrieved from http://www.politico.com/news/stories/1211/70948.html#ixzz2chpINiON
SOPA08	Smith, L. (2011, December). Setting the record straight on SOPA. *The Hill*, Retrieved from http://thehill.com/blogs/congress-blog/technology/199385-setting-the-record-straight-on-sopa#ixzz2chph0Chu
SOPA09	Committee on the Judiciary. (2011). Statement of Judiciary Committee Chairman Lamar Smith Hearing on H.R. 3261, the "Stop Online Piracy Act" [Press Release].
SOPA10	Committee on the Judiciary. (2012). House Judiciary Committee Chairman Drops DNS Provisions from SOPA Legislation [Press Release].
SOPA11	Committee on the Judiciary. (2012). Statement from Chairman Smith on Senate Delay of Vote on PROTECT IP Act [Press Release].
SOPA12	American Civil Liberties Union Report to the Committee on the Judiciary. *Written Statement of the American Civil Liberties Union,* November 15, 2011.
SOPA13	Center for Democracy and Technology. (2011). *The Stop Online Piracy Act: Summary, Problems & Implications*. Retrieved from https://cdt.org/insight/the-stop-online-piracy-act-summary-problems-and-implications-1/4732/
SOPA14	NetCoalition. (2011). *H.R. 3261, "Stop Online Piracy Act" ("SOPA") Explanation of Bill and Summary of Concerns.* Retrieved from https://cdt.org/files/pdfs/NC-Analysis_of_HR3261_FINAL.pdf
SOPA15	American Library Association, et al. (2011). Re: H.R. 3261, the Stop Online Piracy Act [Letter to L. Smith and J. Conyers].
SOPA16	Wikimedia Foundation. (2012). English Wikipedia to go dark January 18 in opposition to SOPA/PIPA [Press Release].

SOPA17	Google. (2014). Two years ago, over 7 million Internet users like you helped defeat the Stop Online Piracy Act (SOPA) [Press Release]. Retrieved from https://takeaction.withgoogle.com/remembering-sopa-gplus
SOPA18	U.S. Senate, Committee on the Judiciary. *Targeting Websites Dedicated to Stealing American Intellectual Property,* Hearing, February 16, 2011 (Serial No. J-112-5). Washington: Government Printing Office, 2011.
SOPA19	Fight for the Future. (2011). The January 18 Blackout/Strike [Press Release]. Retrieved from http://sopastrike.com/numbers/
SOPA20	112 Congressional Record (2012) H45.
SOPA21	112 Congressional Record (2012) H33-H34.
SOPA22	112 Congressional Record (2012) S27-S31.
SOPA23	112 Congressional Record (2012) S16-S27.
SOPA24	112 Congressional Record (2012) S3419-S3420.
SOPA25	112 Congressional Record (2011) H84.
SOPA26	Leahy, P. (2012). Comment Of Senator Patrick Leahy On Internet Service Providers And The PROTECT IP Act" [Press Release].
SOPA27	Combating Online Infringement and Counterfeits Act of 2010, S. 3804, 111th Cong. (2010).
SOPA28	Govtrack. (2011). S. 3804 (111th): Combating Online Infringement and Counterfeits Act [Press Release]. Retrieved from https://www.govtrack.us/congress/bills/111/s3804
SOPA29	Electronic Frontier Foundation. (2010). Victory: Internet Censorship Bill is Delayed, For Now [Press Release]. Retrieved from https://www.eff.org/deeplinks/2010/09/victory-internet-censorship-bill-delayed

Chapter 8 – Theoretical Discussion and Conclusion

Introduction

The preceding frame analysis has described in detail many of the implications of Congressional attempts to regulate content online. Across the CDA, COPA, CIPA, SOPA, and PIPA, lawmakers' master frames all represent the state's goal of protecting children from indecent content and safeguarding intellectual property from theft. Particularly in instances where the primary motivations for these policy initiatives have been grounded in fundamental values such as these, legislators have demonstrated a propensity to rely on technological mechanisms of enforcement that have direct implications for constitutional rights within the U.S. democratic context. When lawmakers directly equate unregulated access to the Internet to the harms identified within diagnostic frames, this magnifies that propensity. Again and again, legislators have approached the Internet as a technological medium that is uniquely responsive to technological regulation. Lawmakers' prognostic frames clearly demonstrate this view of technology and Congress has consistently required the implementation of technological solutions for the problems they have identified.

Despite this approach to technology and to regulation, oppositional groups have continually offered competing points of view. While these groups have remained sympathetic to the worthwhile goals of protecting children and property, they have also been adamant that the state must not sacrifice individual autonomy, regulatory transparency, or access to constitutionally protected speech in the process. Oppositional master frames consistently rely on these core values. The same is true for the opposition's diagnostic frames that have identified the technological solutions imposed

by Congress as having the potential to cause continuing harm to these ideals. In the face of regulatory technologies that may limit individual choice, illegitimately restrict access, or introduce opacity for the user, the opposition has argued that Congress must consider the political and constitutional implications of these systems prior to implementation. As judicial opinion has demonstrated in many of the cases described throughout this dissertation, this oppositional point of view has proven to be more constitutionally sound and more respectful of individual rights. As will be described, many of the opposition's perspectives align closely to concepts articulated throughout STS research.

Despite repeated attempts to regulate through technology, it is clear that there remains some flexibility within legislative prognostic frames for competing points of view and many of the frame shifts identified throughout this research have taken place at this moment within the policy process. Despite entrenched beliefs and confidence in regulatory technologies, lawmakers have demonstrated that they are willing to adapt in order to advance their prevailing master and diagnostic frames. As this dissertation has described, Congress has often narrowed the scope of these policies and has modified their preferred regulatory technologies in response to oppositional pressure. This observation is useful in that it provides a point of entry for inclusion of several perspectives from STS research that will be the focus of the following discussion. Now that this research has identified these frames and frame shifts, it is necessary to discuss how to employ specific concepts from STS to not only articulate the problems inherent in these policy actions but also to demonstrate how they might provide guidance for the policy process moving forward. This chapter will address several of these core concepts including: Congress' reliance on the technical rationality of regulatory systems; the impact of technological

affordances on individual rights; the non-neutral, subjective and potentially biased nature of these systems; the political implications of these systems for liberty, individual autonomy, community autonomy and local knowledge/practice; the potential for cultural and technological hegemony; the imposition and exercise of non-democratic power relations; the consequences of technological ordering; and the implications of Congress' closed relationship to technology. This chapter will conclude with practical recommendations for including these STS perspectives within the policy process so that future lawmakers will be better prepared to address these issues and to ensure that they protect democratic rights from the outset.

Technical Rationality

In the context of the CDA, COPA, CIPA, SOPA, and PIPA, Congress' portrayal of regulatory systems appears to rest on the assumption that such regulatory technologies are simply rational tools that can curb certain behaviors and curtail access to certain speech without significant impact on individual rights. Based on the analysis provided throughout this dissertation, many lawmakers have approached these technologies from a belief that they represent the end product of a rational design process that neither embeds values nor embodies biases. For example, in the case of the CDA and COPA, age verification systems, as the preferred instrument of control, were presented as sterile "enabling tools" that would function invisibly to "filter, screen, allow, or disallow content" (CDA01 p. 102). In the case of CIPA, "technology protection measures" (CIPA01 p. 1) such as commercial filters were presented as apolitical artifacts that controlled access based on objective categorization and "not on the basis of any viewpoint" (CIPA14 p. 31). In each of these policies and within each of the frames

employed by legislative supporters of these Acts, lawmakers essentially presented technology as a black box that provides the best and least restrictive means for realizing the state's goals with little apparent consideration for how they may function in application. This is emblematic of Latour's "blackboxing" where the efficiency and utility of a technological system discourages any deeper investigation into its design, embedded values, or implications. As Latour suggests, it is the very success of these systems that increases their opacity (1999, p. 304).

This is particularly true within the master frames used by legislators to justify both the need for policy and the need for regulatory systems. The normative concerns represented by these master frames are so fundamental that they appear to make it even less likely that lawmakers will question the rationality of these systems. It is important to note that, in relation to efforts to protect children, Congress had legitimate cause for concern and there was (and is) a multitude of sexual material available online. Lawmakers also had an indisputable and well-established responsibility for protecting minors. It was entirely reasonable for lawmakers to believe that "the ultimate responsibility for overall child welfare and legislative protection does still lie with the state and its politics" (Staksrud, 2013, p. 169). The prevalence of this material and the precedent of state responsibility underscored the resonance and power of this master frame. Despite this, the problem described throughout this dissertation is that Congress used its overpowering desire to protect children to justify the imposition of a number of technological mechanisms of control. Equally, during these attempts to accomplish policy goals, considerations of how regulatory systems would actually function were not "in the forefront when considering how and what to regulate" (Id). Instead, legislators

directly tied the utility of these enforcement mechanisms to the normative motivation for the policy. Regulatory systems were "good" because they were effective and, from this point of view, it was better to impose "new and rapidly changing technology" than it was "to leave children unprotected" (CDA14 pp. 18-19).

Legislators repeatedly tied the instrumental utility and apparent objectivity of these artifacts to the ideological motivations for these policies. Use of these "tools" may have seemed self-apparent because they could demonstrably achieve the government's core interests. Perhaps because of this, supporters of these Acts rarely contested these systems at the legislative level and lawmakers appear to have been surprised that the opposition would take issue with their use. When opponents of these policies attempted to challenge the use of these technologies prior to implementation, proponents of regulation called for immediate application of these objective "technology tools" (CIPA19 pp. 88-89) and berated the opposition for requesting "more study" (CDA25 p 28) of their design and implications. This portrayal of regulatory systems implies a reification of scientific and technical expertise that places these artifacts out of the "sphere of legitimate controversy" (Hallin, 1989, p. 116). Technological enforcement was "rarely contestable" from this point of view because these mechanisms appeared "non-arbitrary" and "impersonal" (Ezrahi, 2003, p. 64). The reaction of Exon, McCain, Oxley, and other legislators to the opposition may have been so vehement precisely because the justifications for both these policies and for the use of regulatory systems seemed above reproach.

Oppositional groups repeatedly contested this supposed feature of regulatory technology across all of the policies and across all of the frames identified here. The

application of age verification systems, commercial filtering software, DNS blocks and search result adulteration became "sites of contestation" (Flyverbom, 2011, p. viii) where the technical objectivity and rationality of these systems became the primary issue of contention. These groups consistently and vocally opposed the state's portrayal of such systems as rational, objective, and benign and instead made numerous arguments detailing the arbitrary and distinctly political features of these technologies. For example, the opposition recognized that technologies like filtering software depended on embedded values when categorizing content as acceptable or not and that filtering companies continually rely on "subjective judgments in their blocking programs" (CIPA11 pp. 14-17). This oppositional perspective provided a crucial counterpoint to the legislative approach to technology and, in the majority of instances, that perspective proved to be constitutionally correct from the standpoint of rights and individual autonomy. This validates the prediction that these contests will provide new opportunities for advocacy on the limits and appropriate use of technology in the policy arena (Monberg, 2005, p. 283) and can help guide legislators when considering enforcement mechanisms. If future lawmakers are to avoid the long cycles of legislation and litigation that have characterized these policies, they might adopt this oppositional perspective and, as some in STS suggest, should reconsider any presumptions about the technological rationality of regulatory systems.

Despite this, in the examples described throughout this research, lawmakers have consistently approached regulatory systems as non-arbitrary and apolitical. Implicit within this presentation of the technology is the assumption that these systems would not impede rights or autonomy but would simply isolate users from problematic content.

Congress could safely enact the technical requirements of the CDA, COPA, CIPA, SOPA and PIPA because the underlying enforcement mechanisms were functionally appropriate for accomplishing the state's compelling interests. Even when lawmakers acknowledged technological shortcomings, they consistently portrayed these systems as the best available tools given the current state of the art. Furthermore, legislators not only relied on the self-apparent efficacy of existing technologies but implied that the presence of technologically dependent regulation would spur additional innovation in this area – innovations that would afford even "more ways to comply" in the future (CDA16 p. 25). This implies a recursive relationship wherein the state reifies technical objects and expertise through policy. Imposition of the policy simultaneously encourages the continuation of a rational design process that then produces more of these "tools" that can assist in realizing the state's regulatory goals (see Pfaffenberger, 1992, p. 290). This is a recurring theme throughout these policies and Congress noted that the design process would be "encouraged by the presence of a legal obligation" (CDA16 p. 25). Based on the documentation examined here, at the legislative level there was almost no suggestion that regulatory systems were anything but useful policy instruments that would continue to improve in the future. By imposing more policies and more technologies, lawmakers would be able to perpetuate the "beneficial purpose of encouraging the development of…technologies, thus furthering the mass communications and Internet development goals of Congress" (CIPA19 p. 29).

With this insight, it is possible to describe alternative framings that are useful in circumstances where even the most fundamental motivations for policy are involved. When ideologically and emotionally charged frames (such as those related to the

protection of children and the protection of property) confront those concerned with these policies, it is useful to interject one of the core STS themes presented throughout this dissertation. Specifically, that technological artifacts, such as those enforcement mechanisms at issue here, are socially constructed and non-neutral. As lawmakers debate the merits of these policies in the future and as they consider regulatory mechanisms, it is extraordinarily useful to remember that these "tools" embody the value judgments and biases of those who design them. Particularly in circumstances where lawmakers employ them in a regulatory context, they should consider these systems as objects that can function to constrain individual rights and autonomy. Within these policies, lawmakers have imbued technological mechanisms of enforcement with "constitutional force" (Jasanoff, 2003, p. 175) and that force is part of what makes these mechanisms political objects. By mandating the use of such systems in a regulatory environment, they become coercive objects that exercise legal authority on the state's behalf. What STS perspectives tell us is that use of this force "should be explicitly authorized" (Id). That authorization is less than explicit when the state delegates power to these systems without first understanding the value-laden and subjective nature of the design process. While this reminder may not serve to blunt the resonance of their master frames, it can help lawmakers begin to consider the implications of the technologies they might impose. The policy process in these instances should include such a reminder and lawmakers would benefit from an understanding of technology that includes the contingent nature of technological design. This is the first and most basic requirement for "unpacking the politics of artifacts" (Bijker, 1997, p. 281) at the legislative level and for the formulation of sound policy.

In contrast, oppositional groups have consistently emphasized that these enforcement mechanisms are more than just useful objects and it could serve Congress well to remember these points when considering such policies in the future. Specifically, when confronted with legislative assertions as to the neutrality of regulatory systems, the opposition has countered with arguments that echo the fundamental principle that these systems are anything but impartial. The opposition repeatedly relied on the requirement that any policy should, first and foremost, guarantee rights and access to protected speech. This extended to the assertion that many of the technological solutions offered by Congress were, by design, incapable of such protections. Oppositional groups hinted at the non-neutral nature of the design process when, for example, they criticized commercial filters for imposing "content- and viewpoint-based filtering decisions" that were "subjective" in nature (CIPA11 pp. 4, 14-17). More explicitly, the opposition affirmatively recognized that the Internet itself was the product of a socially constructed design process that purposefully embedded certain ideological considerations. As the ACLU would suggest, the Internet, as a conscious design feature, "embodies the values that underlie the First Amendment by nurturing the robust exchange of ideas and equalizing the distribution of information" (CDA15 p. 2). This is not simply wishful thinking on the part of the opposition that these are the values that designers should embed in the Internet's architecture. In fact, this understanding aligns directly with the philosophy of the World Wide Web's original designer, Tim Berners-Lee. From the inception of the Web, Berners-Lee conceived of and designed this system to allow for the broad dissemination and receipt of information without prioritizing (or discriminating

against) messages based on their content (Berners-Lee, 2010). The ACLU's point speaks directly to the idea that the technological design process can embody values.

Although STS is not a monolithic body of work, the opposition's statements in this regard are strikingly similar to the position shared by many scholars within STS that technology, "is value-laden [and] that technologies are developed in a social context that pushes and pulls and shapes its development" (Johnson, 1997, p. 20). This research suggests that the policy process in general and the framing process in particular should include some understanding by lawmakers that technology's apparent rationality overlays a number of political and ideological commitments. If such considerations were at the forefront during legislative debate, lawmakers could explicitly address this aspect of technology and benefit from this theoretical insight. As noted earlier, this recognition will not necessarily curb the desire to enact laws based on emotionally and ideologically charged master frames but concerned organizations and individuals can usefully insert these ideas into legislative diagnostic and prognostic frames. For example, instead of consistently portraying the Internet as a problem that required government intervention, lawmakers might approach online communication quite differently. With an understanding of embedded values and the design process, legislator might begin to consider Internet communication as something more than an opportunity for pornographers and thieves to harm children or steal intellectual property. Instead, to use the Supreme Court's phrase, the Internet is a "vast democratic forum" where speech of many different kinds is a primary good (CDA18, p. 16). Unregulated access, from this perspective, is not a flaw in the system, but a conscious design feature harmed by centralized content management and control.

In turn, this perspective can guide the prognostic solutions offered by Congress when legislation is required. It can also assist legislators when choosing the means for enforcing regulation. In situations where online content is the target of regulation, Congress can benefit from the reminder that technological mechanisms of enforcement have the distinct potential to act in contradiction to democratic and constitutional principles. While objects like age verification systems may seem to be expedient tools for the realization of policy goals, they have the ideological potential to impede a number of beneficial societal activities. Especially when buttressed by the force of law, Congress should consider the effects of those impediments prior to implementation. This alteration to the policy process may serve to reverse some U.S. precedent in this area and, as Richard Sclove suggests, can help to avoid future situations where lawmakers allow for "the introduction of many technologies having the potential for profound societywide impacts without any evaluation of their social or political ramifications" (1995, p. 219). The policies at issue here have consistently run afoul of constitutional requirements because they did not consider technology, for good or bad, to be objects embodying values and ideology.

Technological Affordances

In order to address the socially constructed nature of technology and regulatory systems, the process of policy formulation should also include an understanding of technological affordances. Lawmakers should actively consider that the design features of some technologies allow or disallow certain activities. Designers build affordances (or the lack thereof) directly into the architecture of a technical system and these features have the potential to constrain a number of activities. As discussed in the engineering

literature, affordances are self-conscious design choices that "encourage us [i.e. designers] to consider devices, technologies, and media in terms of the actions they make possible and obvious. It can guide us in designing artifacts which emphasize desired affordances and deemphasize undesired ones" (Id p. 83). As Latour (1992) suggests, the interactions allowed or disallowed by designers can guide and limit a user's range of available actions and constrain a variety of possibilities. Therefore, technological affordances are a "property of an artifact that suggests how it should be used" (Pfaffenberger, 1992, p. 284). Lawmakers should actively consider how use of that artifact can limit individual autonomy by denying certain actions or access to certain content. By incorporating an understanding of affordances into the policy process, lawmakers can begin to assess how certain regulatory systems may impact the exercise of rights and unduly constrain access to protected speech. Legislators may take quite a different view of technological regulation and may choose different regulatory mechanisms if they consider these systems as artifacts that mediate the ability of the individual to pursue a number of activities online and that can be designed/deployed in ways that enhance or detract from constitutional rights.

For example, in the case of age verification systems that require credit card information as a condition of access, lawmakers would have had an enhanced ability to consider how this requirement constrains constitutional action if they had been able to address the concept of technological affordances explicitly. Most notably, supporters of the CDA and COPA may have hesitated to impose these systems if they had considered that the ability of a consenting adult to access constitutionally protected speech was not a given if that adult did not qualify for or wish to carry a credit card. An intentional design

feature of this system afforded access only upon entry of a credit card number. Constitutional guarantees include no such prerequisite for access to protected speech. As Latour, Pfaffenberger, Brey, and others have argued, any technological system that "discourages or prevents a user from behaving in certain ways while using an artifact" (Brey, 2006, p. 73) implicates the autonomy and rights of the individual. When considered in the context of technological affordances and constitutional rights, lawmakers could have improved the policy process by incorporating an understanding of this concept.

By contrast, oppositional groups frequently adopted language against these policies and these technologies that demonstrated some understanding of technological affordances. Taking again the example of age verification systems, the opposition was quite clear that the design of these systems was troubling in that it conditioned access to protected speech on the provision of personal information including credit card data. Specifically, the Center for Democracy and Technology based its argument against these systems on the observation that they would "require individuals to disclose personal information (e.g., name, address, social security number, credit card) to a third party prior to being afforded access to constitutionally-protected speech" (COPA23 p. 9). Alternatively, the opposition endorsed the "development of user-controlled technologies that afford the least restrictive means by which to protect minors from material on the Internet deemed harmful to them, while ensuring that children have rich, educational, and entertaining experiences on the Internet" (Id pp. 3-4). The opposition predicated its point in this instance on an understanding of regulatory systems as artifacts with the potential to function in ways that affirmatively protect rights and autonomy. The design process is

not a predetermined course that inevitably results in the best and most rational tools. As such, it is important for legislators to consider how certain systems and technological arrangements are, by design, more restrictive than others. This consideration should extend to the legitimacy of those restrictions in the context of democratic rights.

Based on the frame analysis conducted here, STS perspectives sensitive to technological affordances can be included to greatest effect during articulation of and debate over legislative prognostic frames. It is at this point in the policy process that Congress is most amenable to alternative points of view about the solutions included within policy requirements. Time and again throughout the policies at issue here, legislators have demonstrated that they are capable of adapting the regulatory and technological solutions they have proposed. While this did not often occur *during* the negotiation of discrete policies, it did happen *between* policies. This means that, after a policy has failed, the legislative master and diagnostic frames tend to carry over into the next policy with a new and often more narrow enforcement structure. For example, when the Supreme Court struck down the CDA, many members of Congress did not abandon the core belief that certain online content was a danger to minors. Similarly, these same lawmakers continued to assert that unregulated access to the Internet was the cause of this harm and it was the state's duty to intervene. When COPA failed to pass constitutional muster, Congress repeated the process and focused a new regulatory mechanism much more specifically on children's Internet access in public schools and libraries. Legislative motives did not change, nor did problem definition. Instead, lawmakers' proposed technological solution to these issues shifted to better account for arguments against technical limitations on access and speech put forward by the opposition and the

courts. SOPA and PIPA best demonstrate this phenomenon of prognostic frame adaptation where legislators withdrew support for DNS blocking during policy negotiation. Political, oppositional, and public pressure, forced legislators to acknowledge that this barrier did not afford individuals the necessary opportunity to communicate or receive protected speech. Due to this lack of affordances and the constitutional and ethical implications of this technological mechanism, lawmakers chose to excise it from statutory requirements. These arguments also echo many of the same perspectives offered by some STS scholars and, if incorporated into the policy process from the outset, could help avoid any need for the continual adaptation and frame shifts described throughout this research.

Neutrality, Subjectivity, and Bias

In addition to the technological affordances that allow or disallow certain activities, regulatory systems may also constrain autonomy and access due to the normative positions or biases of designers. The subjective nature of technological design embeds the values of those who create such systems. While some affordances may be an intentional but non-political design feature, others are direct features of an ideological motivation. Some of the regulatory systems described throughout this analysis have demonstrated design bias when categorizing online content as "acceptable" or "unacceptable." Again, however, due to the perceived rationality and neutrality of its design, legislators often presented technologies like commercial filters as tools that simply served a useful function. Based on this analysis, legislators presumed the design of such tools to be free of moral judgment or political bias because the designers themselves focused solely on accomplishing an instrumental goal. For example, when

filtering technologies were employed in the legislative and regulatory context of CIPA, the assumption was that they were merely "effective tools" (CIPA25 p. 5) for achieving the government's interests. In contrast, as some in STS have suggested, reliance on technical solutions has consequences beyond its utility. Lawmakers often presented objects like filters as neutral tools because they demonstrated a "promiscuous utility" that obscured the values embodied within them (Winner, 1986, p. 6). The usefulness of things like filtering software often hides the impact it can have.

Due to its "promiscuous utility," Congress deployed regulatory technologies under the assumption that they embodied no values or biases. Using again the example of CIPA, this appears to be the case when, for instance, the government asserted that "the commercial filtering products used by public libraries draw distinctions based on whether the material falls into a category…not on the basis of any viewpoint" (CIPA14 p. 31). This is extraordinarily telling because it presumes that such a category does not itself represent a viewpoint. Such a statement suggests that, in and of themselves, categories are neutral heuristics – nothing but useful shortcuts for organizing content into inclusive or exclusive domains. This also suggests that the filtering software itself is drawing such distinctions, not the designers or manufacturers who created such categories and defined their boundaries in the first place. Yet the act of categorization is a political process (see Suchman, 1994) and those creating these domains may have been anything but neutral when delineating these kinds of borders. In fact, critics have consistently argued against filtering software due to its definitively non-neutral design.

For instance, religious and political bias may be a design feature opaque to the user but prevalent in the philosophy of those writing the code. Commercial filtering

products in particular have demonstrated these inherent biases and the categories of content that are blocked are instructive in this regard. In one survey exploring the depth and breadth of commercial filters, "The political attitudes of the different filter manufacturers were reflected in blocking decisions, particularly with respect to such subjects as homosexuality, human rights, and criticism of filtering software" (Heins, et al., 2006, p. 1). Researchers have also found religious bias in commercial products and many filtering manufacturers "have filtering categories in which they are blocking web sites presenting information known to be of concern to people with conservative religious values" (Willard, 2002). This religious connotation "raises the concern that filtering products used in schools [and libraries] are inappropriately preventing students from accessing certain materials based on religious or other inappropriate bias" (Id). This kind of "preexisting bias" (Friedman & Nissenbaum, 1996, p. 332) is deeply problematic in the context of public institutions that are required to install filtering software in order to remain compliant with CIPA. Forced to implement filters that legislators mistakenly assume are value neutral, this creates a situation in which public institutions unwittingly and vicariously assume the moral and political points of view of filtering companies. These ideological commitments may be constitutionally unsound and may go beyond the definitions of harmful content delineated by the law. This potential of the technology has been recognized by some in STS who argue that "Those who use or purchase the technology, in effect, support or endorse or promote the values that create it" (Johnson 1997, p. 22).

Armed with the knowledge that objects like commercial filters can embody these kinds of biases, lawmakers can proceed to explore whether those biases and embedded

values conflict with the ideals of individual autonomy and the preservation of access to protected speech. They can also examine whether those viewpoints are appropriate for public venues like schools and libraries. When considering future policies, it would serve Congress well to make explicit inquiries into the substance of criteria that delineate access for users – especially adult citizens and public library patrons. In circumstances where these systems may deny access due to the normative perspectives of designers and manufacturers, lawmakers should question the appropriateness of those perspectives in the context of federal regulation. Lacking a clear and cognizant investigation into the conditions of access defined by the mandatory imposition of regulatory systems, Congress will be unable to make informed choices about the best and most democratic means for achieving policy goals.

Technology is Political - Liberty

This, then, leads to the recommendation that legislators approach regulatory technologies as political objects when negotiating future policies. Armed with an understanding of design affordances and the non-neutral, potentially biased nature of these systems, lawmakers can begin to address the political implications of technology. These artifacts are "political" in more than one sense. As mentioned above, these objects are political in that the policy process has imbued them with the legal, regulatory, and constitutional force of the state. Delegation of this force is of concern when legislators do it without explicit understanding of the underlying nature of the technology. As will be discussed shortly, these systems are also political because they can dictate the structure and hierarchy of social power relationships in ways that can erode the ability of the individual to function autonomously. Individual interests may become subservient to

the motivations of those designing or deploying the technology. More fundamentally, these technologies have the potential to function politically because they may directly control the liberties of individuals within the U.S. constitutional context. This may occur in two ways.

First, this implicates the negative liberty (Berlin, 1969, p. 2) of the individual when regulatory technologies illegitimately interfere with the user's ability to seek out the information that he or she wishes to access. When considering policies like those at issue here, Congress should explicitly ask at what point the state's imposition of regulatory systems becomes an improper hindrance on a citizen's ability to, essentially, be left alone. If individual access does not conflict directly with legal prohibitions on content (such as child pornography) and falls within constitutional protections, the threshold for restricting online speech should be set quite high (see below regarding *Griswold v. Connecticut,* 1965). As the Supreme Court found in regard to the CDA, "we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it" (CDA18 p. 26). Despite this, throughout the analysis conducted here, these policies have demonstrated that the imposition of these technologies has tended to hinder the individual's liberty to act without interference. Again, age verification systems impose an artificial barrier to access that interferes with activities otherwise allowed for adult users. Requiring credit card information as a condition of access compounds this interference. Commercial filters hinder the adult library patron's ability to seek out information without first requesting that filters be disabled and/or legitimizing their interest as "bona fide research" (CIPA01 p. 11). DNS blocks and search result adulteration interfere with the individual's

liberty to access or even locate desired websites. Considering these factors and the high bar set for individual access, lawmakers must accommodate the adult citizen's right to be free of having to negotiate technological barriers.

These technologies are also political in instances where they implicate the positive liberty (Id, p. 2) of the individual. Positive liberty goes beyond the ability to act free from external interference and extends to the freedom to pursue goals and realize one's potential. Access to information, as a means for realizing a good and full life (see Nickel, 2007), then, should be affirmatively protected by the state. When state action erodes access and self-actualization through regulatory systems, citizens and lawmakers should explicitly question that erosion. As Berlin (1969, p. 2) suggests, these questions should address the nature of any impediment that limits individual potential. Congress must consider the impediments they would impose on the individual and the legitimacy of those criteria that allow or disallow access. Again, this must include an investigation into the subjectivity of the design process, the substance of technological affordances and the content of embodied values or bias. As Richard Sclove suggests, "From the viewpoint of strong democracy, it is vital to challenge any social structure that sacrifices opportunities for self-actualization" (Sclove, 1995, p. 87).

Technology is Political - Autonomy

Inextricably intertwined with the concept of liberty is personal autonomy. Autonomy is a key requirement for democratic society and the ability to function autonomously allows individuals and communities to determine for themselves what information is necessary and appropriate. In the U.S. context, this right falls within the penumbra of protections afforded by the 14th Amendment that is intended to safeguard

"the freedom of individuals to choose whether or not to perform certain acts or subject themselves to certain experiences" (Cornell Legal Information Institute, 2014). The government's imposition of technological mechanisms between individuals and those experiences diminishes autonomy. This is also true when discussing the autonomous ability of the individual to access information and U.S. Constitutional law provides guidance on this point. Specifically, the U.S. Supreme Court has noted that, "[T]he State may not, consistently with the spirit of the First Amendment, contract the spectrum of available knowledge" (see *Griswold v. Connecticut,* 1965). Here, the Constitution directly ties autonomy to the speech rights of individuals and technological mechanisms have the potential to restrict individual choice and access illegitimately. Perspectives from STS are also useful here because, above and beyond U.S. constitutional commitments, freedom and autonomy are presented as the basic prerequisites of democracy that are "a fundamental precondition of all our willful acts, and hence of pursuing all other goods" (Sclove, 1995, p. 34). When the state inhibits the exercise of autonomy, including informational autonomy, it contracts the ability of citizens to pursue a number of ancillary goods and to realize their own goals. Regulatory systems become social structures that impede autonomy when the state imposes them on individual in a manner that hinders the ability to receive and impart information.

While some in STS have argued that technological systems can and should empower users, bolster self-expression and enhance democracy (see Jasanaoff, 2003 and Sclove, 1995), the policy actions described throughout this dissertation have tended to have the opposite effect. In addition to the minimal affordances provided by age verification systems, commercial filters, DNS blocks, etc., the centralized regulation of

content by the state has directly disempowered individuals, parents, librarians, and communities. Within this frame analysis, legislative supporters of these policies consistently argued that centralized regulation through technical systems was the only solution for piracy and childhood access to indecent content. These mechanisms, Congress suggested, were the sole means for accomplishing policy goals because they were the only way to ensure consistency and pervasiveness throughout the Internet ecosystem.

This reduces autonomy because it removes the individual's ability to make determinations about the acceptability of content and grants that choice to the state. It is especially true that this implicates fundamental speech rights when regulatory systems mediate access. The ability of the adult citizen to realize their own goals and to seek out the information they deem valuable becomes contingent on the state's approval and that approval is, in turn, dependent on successfully negotiating the technological barriers to access imposed by the state. This is troubling when "these technological constraints occur in the context of cultural and informational content basic to human flourishing, a further insult to the autonomous choice of the individual." (Burke & Gillespie, 2006, p. 244). When the state imposes regulatory technologies from above at a centralized core, it removes individual choice from the equation. By recognizing the power these systems have to limit autonomy, Congress might begin to ameliorate this harm by allowing individuals to decide when (and if) to filter information and then employ regulatory technology accordingly. This is particularly true in situations when the target of regulation is childhood access but where the diminishment of adult access becomes an unintended consequence. In the case of CIPA, for example, if adult users were able to

choose where and how filtering takes place, it could re-focus power with the individual and remove it from technical systems. By considering this principle, Congress could begin to protect the autonomy of the individual affirmatively when considering future regulation. First Amendment scholar Jack Balkin has suggested just such an approach in his best practices model for filtering Internet content. Here the emphasis is on user autonomy and Congress should approach regulation from the position that "facilitation of end-user choice through technology provides a better solution" than centralized, government-mandated systems (Balkin, et al., 1999, p. 2).

This principle applies equally to parental autonomy and Congress could look to the oppositional groups who took the position that, if the law was to employ technological systems, parents should be able to use them voluntarily to protect their children. By making use voluntary, this would reverse the power relationship and parents could now affirmatively choose to use technology in ways they felt were appropriate and allowed access to information based on their own normative criteria. That the opposition took to calling these voluntary systems "user empowerment tools" (COPA18 p. 20) is telling because it distinguishes them from the mandatory authority represented by age verification systems, commercial filters, etc. Here the opposition directly echoed Richard Sclove's suggestion that technologies, including regulatory systems, have become an important part of the "social structure" (1995, p. 27). As such, it is important that "technological design and practice should be democratized" (Id). As the opposition argued, if regulatory systems were to be included in the policy landscape, then the state should employ them in a way that it is empowering. Specifically, the use of such systems should be "a voluntary decision by concerned parents to use these products for their

children" (COPA16 p. 46). This would satisfy both Sclove's requirement for the democratization of technological practice and the opposition's call for user empowerment.

A key criticism of STS is the failure of policymakers "to include local knowledges and stakeholders" within technological policy debates or within deliberations about the appropriate use and limits of technology (Gomart & Hajer, 2003, p. 36). Local knowledge has often been a powerful force in defining and contesting the limits of what policies and technologies should do (see Mukerji, 2009). Acknowledgment of this local wisdom and of local practice can help ensure more democratic outcomes for citizens. As will be discussed, this can also help avoid many of the pitfalls that may result when Congress imposes technology that, in application, orders the lives of individuals in ways that bear little resemblance to the realities of daily life (see Scott, 1998 and Jasanoff, 2003). CIPA provides perhaps the best example of how the state discounted community autonomy, local knowledge, and practice. This diminishment of local autonomy occurred in two major ways.

First, at least theoretically, CIPA depends on notions of "community standards" to define the boundaries of acceptable content. Yet the law stripped these determinations from local communities and delegated them to the technical categorization processes embedded within filtering software. As mentioned previously, the 10th Amendment of the Constitutional formally guarantees the right of self-determination for communities and forbids the federal government from exercising any power over local communities above and beyond those specific powers already designated to the state. This principle ties together with the ideals of local autonomy, community standards, and home rule (see

pages 163-164). Local librarians were disturbed that technology became the arbiter of decency in the context of online content and that the state, through filters, had imposed subjective restrictions on access on their communities and their patrons. Congress could have explored this aspect of the technology prior to hindering the ability of local librarians to provide access to the information that best suits the needs of their communities. The state demoted the needs of patrons at the local level in the interest of protecting children through technological blocking and filtering. Lawmakers discarded local practice in favor of a technological solution, imposed from above, and designed with commercial interests in mind.

Second, CIPA impacted the professional autonomy of the local librarian through the imposition of regulatory systems. Congress repeatedly presented filtering software as a technological extension of the traditional expertise employed by librarians to manage physical collections for the benefit of their communities. Lawmakers conflated local practice and expertise with the blunt ability of filtering software to sift through vast amounts of material. Also, manufacturers design filters to exclude digital content, not select material for inclusion in a library's collection. Librarians only exclude content based on thoughtful collection policies and with viewpoint neutrality. Not only did CIPA subvert the exercise of librarians' crucial content management role but it also usurped the authority librarians have traditionally enjoyed in selecting the information that best serves their patrons. That filtering software may employ subjective or biased criteria when categorizing content only exacerbates this harm to professional judgment and community standards. Again, considering the constitutional, ethical and normative implications of imposing potentially biased technical systems from above, the state should examine how

this kind of "impersonal rule" (Mukerji, 2009, p. 205) may disenfranchise and disregard local expertise and sensibilities. When negotiating future policies that have the potential to impact local practice, community standards and professional autonomy, Congress should engage with the individuals and municipalities they are attempting to regulate.

Hegemony

Congress intended age verification systems, commercial filtering software, DNS blocking and search result filtration to bar access to online content based on criteria pre-determined by the state. By definition, these criteria are non-neutral and imply value judgments about the kinds of speech that have, or do not have, merit. As noted throughout this research, the framing employed by Congress in the context of these policies has repeatedly portrayed technology as a neutral tool. These "tools" serve to accomplish this important categorization function on behalf of the government by delimiting the boundaries of acceptable online content in a presumably objective manner. Despite this assumption of objectivity, the act of imposing a regulatory system between users and websites containing "indecent" content implies that the state essentially favors certain material. Acceptable content is freely accessible while these systems lock unacceptable content behind technological gates. This technological arrangement can be harmful because it both deters users from seeking out such content and discourages content producers from creating it in the first place. By declaring some material to be beyond the boundaries of "a uniform national standard of content regulation" (CDA13 p. 49), any speech falling outside that standard appears to be of lower value. That Congress would mediate access to that content through the mandated use of technological gateways adds another layer of deterrence to accessing it at all. If designers embed their normative

considerations within these gateways, and those considerations become the means for delineating between the acceptability and unacceptability of content, they may become hegemonic mechanisms of control. In this sense, regulatory systems may become the hegemonic technologies described by Pfaffenberger. Such systems are "specifically designed to exercise force, that is, to coerce obedience and suppress deviance" (1992, p. 283).

If Congress employs technological mechanisms of enforcement without first exploring the affordances, values and biases embedded within them, lawmakers essentially consent to the delegation of state power to these systems without a full understanding of the potential implications. Also, within the context of legislative frames, the scope of regulation was often so broadly defined that "indecent" material could consist of anything ranging from hard core pornography to foul language. Based on the presumed neutrality of these instruments and the scope of these laws, the pervasive use of these mechanisms had the potential to extend to a vast amount of content. It was conceivable that the law would force websites providing access to health information to implement the same barriers to access as sites containing extreme violent or sexually explicit content. Congress, through regulatory systems, might have imposed an artificial barrier to access on a great deal of material that was informative, artistic, or educational. Without incorporating some understanding of technological design, affordances, and bias into the policy process, legislators were poised to delegate a great deal of normative and legal power to the technology. If delegated to regulatory technologies and, by inference, to those who designed them, this power can become a form of hegemonic control.

This serves as another example of how the policy process can usefully apply perspectives from STS literature during policy negotiation, formulation, and implementation. For example, perspectives from STS can help explicate the risks of cultural and technological hegemony. Cultural hegemony is undesirable because it is the control of social life, thought, opinion, norms and values by some dominant force (see Gramsci, 1971/2005). Government policies that impose this dominance on the public may be harmful if they reduce the diversity of opinion and quell unpopular speech. As those opposed to these policies recognized, "Laws of this sort pose the inherent risk that the Government seeks not to advance a legitimate regulatory goal, but to suppress unpopular ideas or information or manipulate the public debate through coercion rather than persuasion" (CDA13 pp. 67-68). Simply attempting to impose a national standard for online content hints at this coercive potential. Additionally, the use of regulatory technologies in these instances can result in the imposition of technological hegemony. Here, the state delegates the suppression of unpopular ideas and determinations as to the kinds of speech that are societally acceptable to regulatory systems. Not only are these systems categorizing speech as favored or disfavored but the legal, constitutional, and coercive force of government is essentially given over to enforcement mechanisms with very few questions being asked.

Feenberg's work can serve as a reminder to Congress that, "[M]odern forms of hegemony are based on the technical mediation of a variety of social activities" (1992, p. 2). In the context of these policies, technologies may become objects of hegemonic control by illegitimately imposing content-based judgments as to the suitability of online content. The values implicit in regulatory systems can co-opt diversity of thought and

opinion if these values remain unexamined. This potential is disturbing enough when the state essentially endorses some kinds of speech while removing others from the marketplace of ideas. It is even more alarming when the state gives that power to those who design technological mechanisms of enforcement with no oversight or judicial review. By including some examination of these circumstances within the policy process from the outset, it may be possible to negotiate thoughtful terms of access that truly represent the government's (and the people's) interests.

Congress should also examine the potential for hegemonic control where the exercise of state power is, in part, dependent on the consent of those who would be subject to "the general direction imposed on social life" (Gramsci, 1971/2005, p. 12). Here, the people vicariously give that consent to the state through representative democracy. The state has the responsibility to honor that consent and to exercise that power in good faith. One of the key mechanisms for the use of legislative power is "primarily through domination – that is, by monopolizing the instruments of coercion" (Lears, 1985, p. 568). As Feenberg suggests, the regulatory mechanisms chosen by Congress in the policies at issue here all have the potential to hegemonically coerce individual behavior by suppressing "deviant" content. Where Gramsci suggests that the state is in control of these coercive instruments, in the case of the policies examined here, this relationship is reversed. Legislators who mandate their use do not dominate regulatory systems nor do those citizens that function under them. Instead, design criteria, normative positions of manufacturers, embedded values, and bias control access to and/or suppression of online content. Lacking a political process sensitive to the subjective nature of technological design, lawmakers risk forfeiting true consent (both their own and

that of those they represent) to these systems. If lawmakers incorporated this concept into legislative considerations, it would improve the policy process and reduce the potential for this kind of illegitimate delegation of power. Lawmakers might be reticent to forfeit their power and the power of the democratic process without first asking pointed questions about the use of that power.

Two examples from the policies described here demonstrate the potential for technological hegemony. The first instance occurs when the state gives its power to block content to Internet service providers and other network administrators. In the cases of both the CDA and SOPA/PIPA, Congress provided those operating these conduits with a great deal of latitude when deciding when and how to mediate access to problematic content. It is important to remember that the CDA's Good Samaritan provision not only allowed ISPs to proactively deny access to a great deal of online content but shielded them from any legal consequences "for any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, *whether or not such material is constitutionally protected*" (CDA01 p. 101, emphasis added). Here the normative position of an ISP's administrators becomes the standard for judging content and this imposes those subjective criteria on those who rely on these networks for access to online material. Due to the vast amounts of content travelling through these networks, the ISP was essentially required to pass this blocking function on to automated systems that would "filter, screen, allow, or disallow content" on their behalf (CDA01 p. 102). Within this analysis, Congress gave no indication that the criteria used by either ISPs or these automated systems might conflict

with constitutional guarantees. In fact, the statutory language implies that it was not only possible that constitutional speech would be swept into this blocking scheme but acceptable. This demonstrates the potential for technological hegemony when legislative authority is delegated to network operators and the regulatory systems they implement to meet the statutory requirements of policies like the CDA.

While Congress did not intend SOPA and PIPA to mediate access to indecent or obscene content, their focus on infringing content had the same potential for the imposition of technological hegemony. Like the CDA, SOPA and PIPA included broad provisions that allowed ISPs to block access preemptively to entire websites in instances where infringing activity was alleged. These voluntary blocking provisions provided ISPs with legal immunity and were not subject to any judicial review (SOPA06 p. 152). In fact, it was in the best interest of ISPs to act aggressively for fear that courts would hold them liable for contributory infringement. Charges of infringement could come either directly from the Justice Department or from private rightsholders and this created "a system that allows a mere accusation [of infringement] without any court review to lead to potentially damaging actions" including the suppression of problematic speech (Id p. 151). Again, the realities of Internet communication essentially required ISPs to undertake this blocking and filtering through automated systems. Regardless of whether the criteria used to block content came from the ISP or from the designers of regulatory systems, this policy had the potential to hegemonically control the direction of social life on the Web as well as the content of speech. Congress has the responsibility to examine the potential for illegitimate suppression of protected content and should exercise caution when granting this kind of authority to networks that provide access to an enormous

number of individuals. Lawmakers should also consider that ISPs often pass these decisions to automated systems that embed the subjective and normative positions of those who design and deploy them. These policy actions have the potential to promote private interests above the individual's right to access constitutionally protected speech.

The possibility that the state would delegate its power to control access to content to these private entities is disturbing. The opacity of these systems due to technical complexity or, in the case of commercial filtering software, trade secret protections can compound this concern. When legislators do not include a provision for judicial review and when citizens are unable to question the specifications of those technologies imposed on them, the capacity for informed consent or dissent disappears into the black box of technology. From the standpoint of democracy, it would be in Congress' best interest to move the internal design criteria of these filtering and blocking mechanisms to the foreground so that citizens, communities, and public institutions may comment on the appropriateness of their use. Lacking a clear articulation of these features, Congress, "Shielded by the conviction that technology is neutral and tool-like," may impose improper restrains on its people "without the slightest public awareness or opportunity to dispute the character of the changes underway" (Winner,1977, p. 324).

Non-Democratic Power Relations

The policies and technologies at issue here allow those in power to regulate the kinds of activities individuals may pursue online. This technical mediation is a political phenomenon because of the values embedded in technology and the social relationships it perpetuates. It is important to keep in mind that politics are essentially "arrangements of power and authority in human associations as well as the activities that take place within

those arrangements" (Winner, 1986, p. 22). The use of regulatory technology to implement policy creates a mechanism whereby non-democratic outcomes may result. The user must comply with the legal and technological requirements of the system or face the consequences. The individual also remains at the low end of the hierarchical power structure that this use of technology reinforces.

This kind of hierarchy relates directly to the imposition of regulatory systems that may result in "the formation of coercive power relations, and the curtailment of human freedom and autonomy" (Brey 1998, p. 2). This, then, is the basis for the assertion that regulatory systems have the potential to become non-democratic mechanisms of control. As some in STS have suggested, "a technology may have: (a) intractable properties that require democratic patterns of authority; (b) intractable properties that require non-democratic (or anti-democratic) patterns of authority; or (c) flexible properties that are compatible with either pattern of authority" (Johnson 1997, p. 21). Based on the tendency of the systems described throughout this dissertation to inhibit autonomy and access to protected speech, these systems often seem to require non-democratic systems to fulfill the purposes for which they were designed.

The exercise of constitutional rights becomes dependent on the specifications of these technological mechanisms of enforcement and subjective determinations as to the acceptability of problematic content. In addition to making individual interests subordinate to these features of the technology, the deployment of these barriers between adult citizens and protected speech creates a structural impediment to the exercise of rights. Hierarchically and materially, regulatory systems may illegitimately constrain and mediate a variety of online activities. In the case of CIPA, for instance, the Supreme

Court insisted that librarians "disable the Internet software filter without significant delay on an adult user's request" in order for the law to remain constitutional (and for the software to function constitutionally) (*U.S. v ALA* 2003, Syllabus at pp. 3-4). This suggests an intractable and non-democratic property of filtering software in that librarians must turn it off in order to ensure democratic rights for adult patrons.

Even when deployed in the democratic context of the U.S., technologies like age verification systems and commercial filtering software centralize power. For example, an adult patron who confronts filtering software in a public library must actively request that the librarian disable the software in order to access material that the filter had erroneously blocked. In this social relationship, control is given to librarians who are then authorized (and presumably able) to turn off the filter. Nevertheless, despite the Supreme Court's assertions to the contrary, even this outcome is uncertain. Remember that CIPA's disabling provision grants additional authority to librarians to accept only those requests deemed to be legitimate and "for bona fide research" (CIPA01 p. 11). It can be assumed that the categories embedded within filtering software make the initial judgment as to what content is "bona fide" and the librarian then has the option to confirm or refute that assessment. Patrons are subservient to both the software and to the librarian's assessment. In turn, librarians are subservient to software administrators who have the power to re-classify websites as acceptable (or not) based on the request. When such power is delegated to the system and subsequent activity is dependent on the administrator's authorization, the "autonomy of users is consequently eroded, and users may come to feel dependent and constrained in their actions" (Brey, 1998, p. 8). By requiring that "technology protection measures" (CIPA01 p. 2) be used to mediate the

acceptability of content in public libraries, Congress essentially legislated that the power to enforce the law be left with the designers, manufacturers and administrators of filtering software.

Due to the nature of their design and the context of their deployment, technologies like those required by the CDA, COPA, CIPA, SOPA and PIPA appear to be most compatible with and supportive of non-democratic political systems. SOPA and PIPA directly support this observation where critics condemned lawmakers for mandating the use of technologies employed by a number of authoritarian and repressive regimes. DNS blocking and the manipulation of search engine results are common tactics employed by countries like China, Saudi Arabia and others where the goal is to suppress the dissemination of politically dangerous or religiously offensive content (see Faris & Villenueve, 2008, p. 10). The use of similar systems in the U.S. context is problematic precisely because it implies a non-democratic relationship between the state and its people – a relationship where technological systems mediate access to information. Mandated use of systems like DNS blocking was, for the opposition, not only non-democratic in a domestic sense but also in a global context where repressive states might be encouraged to "abuse their technological capacity to take down content they find objectionable or threatening" (SOPA12 p. 6). It is important to remember Langdon Winner's warning that "the adoption of a given technical system unavoidably brings with it conditions for human relationships that have a distinctive political cast – for example, centralized or decentralized, egalitarian or inegalitarian, repressive or liberating…to choose them is to choose unalterably a particular form of political life" (1986, p. 29). By imposing the policies and technologies described throughout this research, Congress

risked choosing a political life for the United States that was distinctly non-democratic, unconstitutionally hierarchical and potentially damaging to individual rights.

Technological Ordering

The history of these policies demonstrates Congress' relationship with regulatory technology. Legislative supporters of the CDA, COPA, CIPA, SOPA, and PIPA demonstrated the tendency of the high modern society (Scott, 1998) to order the lives and Internet access of individuals according to the state's interests and through the use of unexamined regulatory systems. While Scott critiques the high modern society for its reliance on scientific technique to isolate and organize nature, human behavior or economic production, this analysis critiques the state's attempt to control the flow of information through mechanisms meant to restrict access. This attempt at ordering is deeply disruptive to the complex relationships and technical arrangements that define communication on the Internet. Such situations are constitutionally problematic because the state's presumptions about how best to accomplish its instrumental goals are often grounded in a faulty premise. This premise suggests that the state can only regulate the technological medium of the Internet through the use of technological barriers to access. Many of the sponsors of these policy initiatives have also demonstrated that they have very little understanding of or personal experience with the medium they would regulate. Therefore, the imposition of technological "tools" to mediate access appears to them as a proper solution that brings to bear the products of technical expertise for the benefit of minors, parents and the state itself. In such circumstances, to paraphrase Scott, everything that interferes with the goal of protecting intellectual property or protecting children from harmful content is set aside. The state disregards everything that does not

seem related to its goals. This includes oppositional arguments against regulation and for the protection of individual rights and autonomy.

The "cyberzoning" metaphors employed by Congress to justify the CDA provide one illustration of this ordering identified by Scott. By relying on this physical analog as justification for the imposition of age verification systems, the state was essentially using this technological mechanism to shape behavior online in a manner similar to the one it had used for years in neighborhoods, near schools and near churches. If the nation was to realize the educational and commercial potential of the Internet, Congress argued, it was incumbent on the state to order online behavior in ways that would not threaten these interests. Due to this, lawmakers portrayed age verification systems as a beneficial and unbiased tool of scientific and technical progress that they could harmlessly interject into the online ecosystem. Physical zoning laws had proven effective in accomplishing the "government's interests in reducing crime, maintaining property values, and preserving the quality of urban life" (CDA14 p. 27). Age verification systems were the means by which the state could transfer this control of human activity onto the Internet for the benefit of children and commerce and to the detriment of those who dealt in "smut" (CDA19 p. 2). Nevertheless, as Scott suggests, this kind of ordering fails to accommodate "the autonomy of existing social life" that falls outside the state's conceptions of appropriate behavior (1998, p. 93). As the opposition would suggest, these systems and the concept of cyberzoning were inappropriate for this new medium because they became gateways to access that stifled the spontaneous and free flow of information. These enforcement mechanisms were nothing less than checkpoints that

would force individuals to identify themselves prior to entry. In the presence of this new ordering, it was unsurprising that adult users would hesitate to cross that threshold.

Again, Scott's insight is helpful in addressing the state's attempt to isolate and order behavior according to seemingly rational criteria. While both the means and ends for such technical ordering may seem self-apparent from a certain point of view, when taken in context, this ordering both ignores and disrupts a wider, more complex network of relationships. For example, legislators believed they could neatly separate "appropriate" from "inappropriate" speech. In the case of COPA, part of the legislative criteria for such separation was, simply put, the difference between commercial and non-commercial speakers. Commercial speakers were those that were "engaged in the business of transferring or selling" information online (COPA11 p. 11) and, if that business was "designed to appeal to the prurient interest of minors" (COPA17 p. 52), then it was locked behind age verification screens. Non-commercial speakers were, within this scheme, protected from regulation because they did not sell potentially prurient material. Nevertheless, non-profit and educational outlets would be entangled in this same regulatory standard if the content offered on their sites could, in any way, be considered sexually explicit, titillating or otherwise harmful to minors based on some intangible and ill-defined standard.

This was especially true in circumstances where advertisements, self-promotion, fundraising, or other commercial material may have been included on websites that were not actually selling content. By COPA's definitions, any site that operated in this way was transacting business in a manner that qualified for technological regulation. The law would place educational, informational, and activist websites in the same regulatory

category as hard core pornography. What was, from the legislative perspective, a clear and rational means for delimiting access and curbing certain online behaviors was actually a much more complicated technical arrangement. By relying on the ability of regulatory systems to demarcate the state's boundaries for acceptability, lawmakers had assumed that they could draw such borders in the first place. Congress had also erred by presuming that some online content had no redeeming value for minors simply because it included some material that was sexual in nature. Regulatory systems could not categorize and control websites, the Internet, and individual activity as neatly as lawmakers seem to have believed. Congress must keep in mind that it is never a simple matter to regulate and order something as messy as online communication. With some understanding of how policy and technology can impact these complex arrangements, Congress can mitigate some of these unintended consequences before they occur.

The Legislative Relationship to Technology

Within this frame analysis, lawmakers continued to insist that technological regulation was the only solution to the problems they had identified and that regulation itself was a simple exercise in categorization and organization. Systems made decisions about the suitability or legality of online content in an objective, impersonal manner that were "not based on any particular viewpoint" (CIPA03 p. 7). Across all of the policies at issue here, Congress still maintained a certain relationship to technology that does not adequately recognize the core of the systems they chose to impose upon users. When negotiating future policies, lawmakers must consider the embedded values and biases designed into any technical system if they are to employ it in a regulatory context. While, for instance, bodies like the COPA Commission could have articulated some of these

considerations and unpacked some of the political implications of these artifacts, many in Congress chose not to listen and their commitments remained firmly in place. The Internet was a tool that was subject to regulation and ordering by the state. As a technological medium, it was uniquely suitable for control through technological mechanisms of enforcement. These mechanisms, as the product of a rational design process, were above reproach and could mediate access in a manner that did not implicate individual rights or autonomy. Content itself could be classified, walled off, and controlled.

This also relates directly to the state's perception of the Internet as a technological tool that was uniquely responsive to technical regulation. This implies a rigid understanding where the solution to technological problems is invariably technological. By maintaining the neutrality of technology as a given, legislators may have been incapable of addressing the implications of both regulatory systems and the problems inherent in any technological solution. This is reminiscent of Heidegger's warnings about a limited and closed relationship with technology where we risk even greater harm when we fail to examine the essence of technology (1977, p. 3). As many in STS have described, this failure to understand the socially constructed nature and biases embedded in technology can lead to even deeper problems when we apply it to curb and control behavior. Heidegger's point is directly relevant to Congress' use of regulatory systems within these policies because they took the neutrality of these systems for granted and because lawmakers' conception of technological "problems" left little room for anything but technological "solutions". When Congress mandates the use of regulatory technologies to order behavior and, in these cases, curtail access, we are limited not only

by the technology but by this worldview. Heidegger cautioned that the technologically ordered society, even one with benevolent intentions, is not the solution to our problems but the problematic result of this approach (see Dreyfus, 1995).

This closed relationship to technology is most apparent in circumstances where Congress declined to consider the no-tech or low-tech solutions offered by the opposition that would have circumvented the need for centralized mechanisms of control. For example, Congress could have implemented local use policies that were truly respectful of community standards in public places where children had access to the Internet. The opposition also suggested that Congress develop educational opportunities where parents and children could learn how to use the Internet respectfully and responsibly in ways that best reflected their individual values. Although the opposition suggested both of these options as the two primary alternatives to technological regulation, neither gained traction with lawmakers. Perhaps due to the state's reification of expert knowledge and technical solutions, these alternatives were dismissed as ineffective and insufficient (CDA16 p. 22). From the government's view, it was imperative that the state impose technological systems in order to manage problematic content.

Not only did Congress decline to consider alternatives that did not include technological enforcement mechanisms but they often did not heed the warnings of their own investigations. For example, the COPA Commission's findings, and Congress' reaction to it, demonstrate that lawmakers were unwilling to address the problem of childhood access to questionable material with anything but their preferred technological solutions. Although the Commission took the unprecedented step of critiquing various regulatory technologies on the basis of the values they could promote or demote, most of

Congress did not directly address the Commission's findings. Again, this implies a certain relationship to technology and a dependence on the portrayal of regulatory systems as instrumental tools above reproach. Even when confronted with direct evidence that technologies like age verification systems and commercial filters were demonstrably non-neutral, lawmakers essentially refused to reconsider their position on technology. Furthermore, the fact that the Commission was unfunded and would not publish its findings until two years after Congress had passed the law says something about Congress' willingness to entertain any perspectives that would contradict their view of technology.

Investigations like the one conducted by the COPA Commission can provide insight into, as Heidegger would put it, the essence of technology (1977). When this essence and the social processes that underpin it are laid out for examination, only then can Congress unpack "the politics of artifacts" (Bijker, 1997, p. 281). As the opposition would note, the Commission was able to examine "how to protect children online in ways consistent with the Internet's architecture and Constitutional requirements" (COPA04 p. 64). This is a crucial distinction because it demonstrates that a truly critical review goes beyond lawmakers' more instrumental understanding where "good" regulatory systems are those that are simply the most effective. For the Commission, regulatory systems were good not simply because they were an effective barrier to access but because they accomplished the goal of protecting children while simultaneously enhancing the "privacy" and "First Amendment values" of individual citizens (COPA04 p. 15). For the first time, Congress had to confront the reality that the technologies they had considered to be apolitical were anything but. Despite this, the report does not appear to have shaken

their relationship to technology. Going forward, Congress should undertake more of these types of sustained review and should be more responsive to the results. This could help meet Richard Sclove's requirement that any government-mandated technology should be subject to studies that account for that technology's "compatibility with democracy as a highest order evaluative consideration" (1995, p. 222).

Recommendations and Conclusion

Solutions to the complex problem of Internet content regulation are more complex than they might first appear. As long as Congress considers the use of technological artifacts to be rational and self-apparent, issues of neutrality, autonomy, hegemony, rights, and power will persist. This is particularly true in circumstances where emotionally and ideologically charged master frames may compel lawmakers to implement technological systems where the efficacy of those systems is the primary consideration. Efficiency and constitutionality are not necessarily synonymous and Congress must undertake a more rigorous effort to understand the potentially subjective and restrictive nature of these systems prior to imposing them in a regulatory environment. Equally, the act of problem definition that takes place within diagnostic framing requires room for more nuanced insight into the nature of these problems. Although the problematic content identified by Congress has the potential to harm children, the economic interests of intellectual property rightsholders and even national security, regulation itself may be as damaging as the problem initially identified. Congress exacerbates this possibility when it mandates the use of poorly understood regulatory systems as the best and only solution within prognostic frames. Despite this, it is likely that lawmakers will continue to devise new schemes to regulate the content and

conditions of online communications. With such a possibility on the horizon, it is useful to interject the core STS themes identified throughout this dissertation into that policy process. While the opposition has consistently and clearly articulated alternative framings that describe the detrimental implications of these technologies, a more explicit articulation of these STS concepts can guide future policy initiatives. Including these concepts within the policy process will help to avoid the continuous cycle of legislation and litigation discussed throughout this dissertation while simultaneously protecting individual rights.

One way to ask meaningful questions about the technology we choose to deploy in a regulatory context is to interrogate the conditions created by use of that technology, the values that these technologies embody, and their direct impact on access to information. If the preceding frame analysis is any indication, Congress should take additional time to analyze regulatory systems prior to implementation in order to identify any aspects of technologies and technological practices that have the potential to be politically, constitutionally, or ethically problematic. By examining the potential for harmful outcomes prior to deployment, legislators and concerned citizens can make normative judgments about technological systems and protect individual rights from the outset. Age verification systems, commercial filtering software, DNS blocking, and other regulatory technologies all, in one way or another, restrict information flows and hinder the autonomous ability of the individual to acquire, possess, or distribute information. These technologies then become the target of a normative analysis of the values they *should* embody. Since designers primarily intended many of the systems identified here to serve as a means for restricting access to information and/or monitoring use, we can

evaluate them as negative in the context of democratic values such as autonomy and individual constitutional rights.

Now that this frame analysis has identified opportunities within the policy process for including specific perspectives from STS, it is necessary to recommend the means for accomplishing that task. Based on this research, the primary solution recommended here is the establishment of an investigative agency to explore these issues prior to the deployment of potentially biased and restrictive regulatory technologies. This agency should remain external to Congress and, as much as possible, exist outside the political process. Although any public agency runs the risk of regulatory capture due to the influence of political, commercial, financial, or other interests, by focusing this organization's mission strictly on the impact and nature of proposed regulatory systems, this outside influence may be reduced. The composition of this agency should include, at least in part, experts from academia, civil rights organizations, and technology policy advocacy groups that are familiar with the non-democratic potential of technological enforcement mechanisms. Again, based on this research, these groups have already demonstrated the ability to recognize the potential of these mechanisms to harm individual rights and autonomy. Additionally, these oppositional groups have consistently taken positions that acknowledge the non-neutral and subjective nature of technology as well as the affordances that may limit the range of possible actions for users. In the context of U.S. constitutional rights, these organizations have also, through their master frames, prioritized the preservation of autonomy, transparency, and access to protected speech. This, in addition to including the STS concepts discussed throughout this chapter, can provide a strong foundation for helping Congress formulate sound

policy in the future. Without some acknowledgment of these principles and without room for critical voices, legislative history may simply repeat itself.

There is precedent for just such an agency and legislative bodies have benefited from this kind of advice both domestically and internationally. For example, in 1972 Congress tasked the U.S. Office of Technology Assessment (OTA) with a mission similar to that proposed here. Specifically, in establishing the OTA, Congress recognized that, "As technology continues to change and expand rapidly, its applications are large and growing in scale; and increasingly extensive, pervasive, and critical in their impact, beneficial and adverse, on the natural and social environment" (Public Law 92-484, 1972, p. 797). In order to mitigate any potentially adverse impacts of these increasingly pervasive technologies, the OTA was intended to explore "the consequences of technological applications" so that they may be "anticipated, understood, and considered in determination of public policy on existing and emerging national problems" (Id). Unfortunately, due to a variety of political motivations, Congress defunded and decommissioned the OTA in 1995 (see Bimber, 1996). Despite this, an organization like the OTA, founded on the principles outlined throughout this dissertation, could provide useful recommendations to Congress on these issues.

The Parliament of the European Union currently employs a European Technology Assessment Group (ETAG) that is meant to examine the "social, environmental and economic aspects of new technological and scientific developments" and provide advice regarding the "complex social, ecological and economic implications of modern technology and scientific research" (ETAG, 2014). Although this current iteration was founded in 2005, the European Parliament (a different body than the EU Parliament) has

relied on recommendations of this sort since the late 1980s (Id). In its current form, the ETAG is comprised of several cooperating academic and governmental bodies that, in addition to providing advice to the EU, conduct similar analyses in their home countries. Again, the U.S. Congress can look to these organizations as blueprints for conducting the kind of rigorous and critical studies recommended here.

Any group or agency may fail to accomplish its goals or its warnings may go unheeded by the legislative body it reports to. In addition to the possibility of regulatory capture alluded to above, these organizations may also fall prey to internal politics or honest disagreements about how technological means may accomplish regulatory ends. Despite this, it is important to invest some group with the power to conduct these kinds of studies because, as it stands now, Congress has no consistent mechanism for examining these issues. Until lawmakers explicitly address problems of neutrality, autonomy, hegemony, rights and power, they may continue to create the same conditions that led to such deep disagreements over the CDA, COPA, CIPA, SOPA, and PIPA. Nevertheless, with these issues in mind, Congress will be able to formulate sound policy that employs technology appropriately and in ways that respect democratic processes, constitutional rights and the autonomy of the individual.

REFERENCES

141 Congressional Record (1995) S8088, daily ed. (Statement of Senator James Exon).

ABI Research. (2013). *Parental Control Software and Filtering Technologies to Drive Child Online Protection Market.* Retrieved from, https://www.abiresearch.com/press/parental-control-software-and-filtering-technologi.

About EFF. (2014). Retrieved from, https://www.eff.org/about.

ACLU Plaintiffs' Post-Trial Brief in Support of Their Motion for a Preliminary Injunction, 1996. Retrieved February 25, 2013, from http://www.aclu.org/technology-and-liberty/aclu-v-reno-post-trial-brief.

Allen, M., & Long, J. (2004). Domesticating the Internet: Content regulation, virtual nation-building and the Family. *Virtual Nation: The Internet in Australia*, Goggin (Ed.). Sydney: University of New South Wales Press.

Ammori, M. (2011). Should Copyright Be Allowed to Override Speech Rights? *The Atlantic*. Retrieved April 8, 2013, from http://www.theatlantic.com/politics/archive/2011/12/should-copyright-be-allowed-to-override-speech-rights/249910/.

Balkin, J., Noveck, B., & Roosevelt, K. (1999). *Filtering the Internet: A Best Practices Model.* Information Society Project, Yale Law School.

Barker, J., & Downing, C. (1985). Word processing and the transformation of patriarchal relations of control in the office. *The social shaping of technology: How the refrigerator got its hum*, MacKenzie & Wacjman (Eds.). Philadelphia: Open University Press.

Barlow, J. (1996). *A Declaration of the Independence of Cyberspace*. Retrieved from, https://projects.eff.org/~barlow/Declaration-Final.html.

Benford, R., & Snow, D. (2000). Framing Processes and Social Movements: An Overview and Assessment. *Annual Review of Sociology*, 26, 611-639.

Berlin, I. (1969). *Four Essays on Liberty*. Oxford: Oxford University Press.

Berners-Lee, T. (1999). *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by its Inventor*. San Francisco: Harper.

Berners-Lee, T. (2010). Long Live the Web. *Scientific American*, 303, 80-85.

Bijker, W. (1997). *Of Bicycles, Bakelites, and Bulbs: Toward a Theory of Sociotechnical Change*. Cambridge: MIT Press.

Bimber, B. (1996). *The Politics of Expertise in Congress: The Rise and Fall of the Office of Technology Assessment*. Albany: State University of New York Press.

Bimber, B. (1998). The Internet and Political Transformation: Populism, Community, and Accelerated Pluralism. *Polity*, 31(1), 133-160.

Bradburn, et al. v. North Central Regional Library District, 2:06-cv-00327-EFS (2006).

Brey, P. (1998). The Politics of Computer Systems and the Ethics of Design. *Computer Ethics: Philosophical Enquiry*, van den Hoven (Ed.). Rotterdam: Rotterdam University Press.

Brey, P. (2000). Disclosive Computer Ethics. *Computer and Society*, 10-16.

Brey, P. (2006). Ethical Aspects of Behavior Steering Technology. *User Behavior and Technology Development*, Verbeek & Slob (Eds), Amsterdam: Kluwer Publishing.

Brey, P. (2010). Values in technology and disclosive computer ethics. *The Cambridge Handbook of Information and Computer Ethics*, Floridi (Ed.). Cambridge: Cambridge University Press.

Burk, D., & Gillespie, T. (2006). Autonomy and Morality in DRM and Anti-Circumvention Law. *Triple C,* 4(2), 239-245.

Cannon, R. (1996). The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway. *Federal Communications Law Journal*, 49(1), 51-94.

Carroll, J. (1977). Participatory Technology. *Technology and Man's Future*, Teich (Ed.). New York: St. Martin's Press.

CDT. (2014). CDT Mission and Principles. Retrieved from, https://cdt.org/mission/.

Child Online Protection Act of 1996, (COPA), Pub. L. No. 105-277 (Tit. XIV), 112 Stat. 2681 (Oct. 23, 1998), codified at 47 U.S.C. § 231.

Children's Internet Protection Act of 2000, (CIPA), Pub. L. No. 106-554 (Title XVII), (Dec. 21, 2000), codified at 20 U.S.C. § 9134 (f) and 47 U.S.C. § 254 (h)).

Christensen, L. (1995). Cyberporn Study: more heat than light? Metanews. Retrieved from, http://www.columbia.edu/cu/21stC/issue-1.2/Cyber.htm.

Cohen, J. (2007). Cyberspace As/And Space. *Columbia Law Review*, 107(1), 210-256.

Combating Online Infringement and Counterfeits Act of 2010, (COICA), S. 3804, 111th Cong. (2010).

Communications Decency Act of 1996, (CDA), Pub. L. No. 104-104 (Title V), 110 Stat. 133 (Feb. 8, 1996), codified at 47 U.S.C. § 231.

Cornell Legal Information Institute. (2014). *Personal Autonomy*. Retrieved from, http://www.law.cornell.edu/wex/personal_autonomy.

Cowhey, P., & Mueller, M. (2009). Delegation, Networks, and Internet Governance. *Networked Politics: Agency, Power, and Governance*, Kahler (Ed.). Ithaca: Cornell University Press.

CyberPatrol Online Protection Pro: Features. Retrieved July 2, 2012, from http://www.cyberpatrol.com/cponlineprotectionpro.asp.

CyberPatrol Library Web Filtering: CIPA Compliance. Retrieved July 2, 2012, from http://www.cyberpatrol.com/library.asp.

Deibert, R., & Rohozinski, R. (2010). Beyond Denial: Introducing Next-Generation Information Access Controls. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, Deibert, Palfrey, Rohozinski & Zittrain (Eds.). Cambridge: MIT Press.

DeNardis, L. (2014). *The Global War for Internet Governance*. New Haven: Yale University Press.

Digital Millennium Copyright Act of 1998, (DMCA), Pub.L. No. 105−304 (Title XVII), 112 Stat. (Oct. 12, 1998), codified at 17 U.S.C. § 501-513.

Doe v. MySpace, 528 F.3d 413 - 5th Cir. (2008).

Drahos, P. (1996). *A Philosophy of Intellectual Property*. Brookfield: Dartmouth Press.

Dreyfus, H. (1995). Heidegger on Gaining a Free Relation to Technology. *Technology and the Politics of Knowledge*, Feenberg & Hannay (Eds.). Bloomington: Indiana University Press

Easterbrook, F. (1996). *Cyberspace and the Law of the Horse*. 1996 University of Chicago Legal Forum.

Edelman, B. (2001). Expert Report of Benjamin Edelman: Multnomah County Public Library et al., vs. United States of America et al. (01-CV-1322).

Electronic Frontier Foundation (EFF) - SOPA/PIPA: Internet Blacklist Legislation. Retrieved April 2, 2013, from https://www.eff.org/issues/coica-internet-censorship-and-copyright-bill.

Electronic Privacy Information Center (EPIC). (2009). The Legal Challenge to the Child Online Protection Act. Retrieved February 22, 2013, from http://epic.org/free_speech/copa/.

Elmer-DeWitt, P. (1995, July 3). Cyberporn – On a Screen Near You. *Time*.

EPIC & Peacefire. (2000). Mandated Mediocrity: Blocking Software Gets a Failing Grade. Retrieved June 15, 2012, from http://peacefire.org/censorware/BESS/MM/.

European Technology Assessment Group (ETAG). (2014). Retrieved from, http://www.itas.kit.edu/english/etag.php

Exon, J. (1995, April 9). Keep Internet Safe for Families [Editorial]. Dallas Morning News.

Exon, J. (1995, June 22). Interview by E. Farnsworth, *The MacNeil/Lehrer NewsHour* [Television Broadcast]. Washington, D.C.: Public Broadcasting Service.

Ezrahi, Y. (2003). Science and the Postmodern Shift in Contemporary Democracies. *Social Studies of Science and Technology: Looking Back, Ahead*, Joerges & Nowotny (Eds.). Netherlands: Kluwer Academic Publishers.

Faris, R., & Villenueve, N. (2008). Measuring Global Internet Filtering. In *Access Denied: The Practice and Policy of Global Internet Filtering*, Deibert, Palfrey, Rohozinski & Zittrain (Eds.). Cambridge: MIT Press.

Farlex. (2014). Least Restrictive Means Test. In *Farlex Legal Dictionary*. Retrieved from, http://ciec.org/.

FCC v. Pacifica Foundation, 438 U.S. 726 (1978).

Feenberg, A. (1991). *Critical Theory of Technology*. Oxford: Oxford University Press.

Feenberg, A. (1992). Subversive Rationalization: Technology, Power and Democracy. *Inquiry*, 35(3), 1-17.

Fisher, K. (1997). Locating Frames in the Discursive Universe. *Sociological Research Online*, 2(3).

Flyverbom, M. (2011). *The Power of Networks: Organizing the Global Politics of the Internet*. Cheltenham, UK: Edward Elgar Publishing Ltd.

Foucault, M. (1976/1980). *Power/Knowledge: Selected Interviews & Other Writings 1972-1977*, Gordon (Ed.). New York: Pantheon Books.

Friedman, B., & Nissenbaum, H. (1996). Bias in Computer Systems. *ACM Transactions on Information Systems*, 14(3), 330-347.

Gaver, W. (1991). Technology Affordances. *CHI '91 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. New York: ACM Press.

Ginsberg v. New York, 390 U.S. 629 (1968).

Gitlin, T. (2003). *The Whole World is Watching: Mass Media in the Making and Unmaking of the New Left*. Berkeley: University of California Press

Goffman, E. (1974). *Frame Analysis: An Essay on the Organization of Experience*. London: Harper Row.

Goggin, M., & Mooney, C. (2001). Congressional Use of Policy Information on Fact and Value Issues. *The Public Clash of Private Values: The Politics of Morality Policy*, C. Mooney (Ed.). Chatham, NJ: Chatham House.

Gomart, E., & Hajer, M. (2003). Is *That* Politics? *Social Studies of Science and Technology: Looking Back, Ahead*, Joerges & Nowotny (Eds.). Netherlands: Kluwer Academic Publishers.

governingwithcode. (2004). Case Study: Platform for Internet Content Selection. Retrieved from, http://www.governingwithcode.org/case_studies/pdf/PICS.pdf.

Gramsci, A. (1971/2005). *Selections from the Prison Notebooks*. New York: International Publishers.

Griswold v. Connecticut, 381 U.S. 479, 482 (1965).

Guggenheim, M., & Nowotny, H. (2003). The Present State of STS. *Social Studies of Science and Technology: Looking Back, Ahead*, Joerges & Nowotny (Eds.). Netherlands: Kluwer Academic Publishers.

Hackett, E., et al. (2008). Introduction. *The Handbook of Science and Technology Studies*, Hackett, Amsterdamska, Lynch, & Wajcman (Eds.). Cambridge: MIT Press.

Hallin, D. (1989). *The "Uncensored War": The Media and Vietnam*. Berkeley: University of California Press.

Hamade, S. (2008). Internet Filtering and Censorship. *Fifth International Conference on Information Technology: New Generations,* 1081-1086.

Hecht, G. (1998). *The Radiance of France: Nuclear Power and National Identity after World War II*. Cambridge: MIT Press.

Heidegger, M. (1977). *The Question Concerning Technology and Other Essays*. New York: Harper & Row.

Heins, M. (2001). *Not in Front of the Children: "Indecency," Censorship, and the Innocence of Youth*. New York: Hill and Wang.

Heins, M., & Cho, C. (2001). *Internet Filters: A Public Policy Report*. Free Expression Policy Project, National Coalition against Censorship.

Heins, M., Cho, C., & Feldman, A. (2006). *Internet Filters: A Public Policy Report*. Brennan Center for Justice, NYU School of Law. Retrieved June 30, 2012, from http://www.fepproject.org/policyreports/filters2.pdf.

Ingram, H., Schneider, A., & deLeon, P. (2007). Social Construction in Policy Design. *Theories of the Policy Process*, Sabatier (Ed.). Boulder: Westview Press.

Jasanoff, S. (2003). In a Constitutional Moment: Science and Social Order at the Millennium. *Social Studies of Science and Technology: Looking Back, Ahead*, Joerges & Nowotny (Eds.). Netherlands: Kluwer Academic Publishers.

Johnson, D. and Post, D. (1997). The Rise of Law on the Global Network. *Borders in Cyberspace*, Kahin & Nesson (Eds.). Cambridge: MIT Press.

Johnson, D. (1997). Is the Global Information Infrastructure a Democratic Technology? *Computers and Society*, 20-26.

Johnston, H. (1995). A Methodology for Frame Analysis: From Discourse to Cognitive Schemata. *Social Movements and Culture*, Johnston, & Klandermans, B. (Eds.). Minneapolis: University of Minnesota Press.

Jordan, T. (2001). Language and libertarianism: the politics of cyberculture and the culture of cyberpolitics. *The Sociological Review*, 49(1), 1-17.

Katz, W. (1980). *Collection Development: The Selection of Materials for Libraries*. NY: Holt, Rinehart & Winston.

Kingdon, J. (1995). *Agendas, Alternatives, and Public Policies*. NY.: Longman.

Klandermans, B. (1984). Mobilization and participation: Social-Psychological expansions of resource mobilization theory. *American Sociological Review*, 49, 583-600.

Klandermans, B. (1986). New Social Movements and Resource Mobilization: The European and American Approach. *International Journal of Mass Emergencies and Disasters*, 4, 13-37.

Kreimer v. Bureau of Police, 958 F.2d 1242, 1259 (3d Cir. 1992).

Laswell, H. (1951). The Policy Orientation. *The Policy Sciences*, Lerner, D. & Laswell, H. (Eds.). Stanford: Stanford University Press.

Latham, J. (2001). Positioning the Public Library in the Modern State: The Opportunity of the Children's Internet Protection Act (CIPA). *First Monday*, 6(7). Retrieved from http://www.firstmonday.org/ojs/index.php/fm/article/view/873/782.

Latour, B. (1992). Where are the Missing Masses? The Sociology of a Few Mundane Artifacts. *Shaping Technology/Building Society: Studies in Sociotechnical Change*, Bijker & Law (Eds.). Cambridge: MIT Press.

Latour, B. (1999). *Pandora's hope: essays on the reality of science studies.* Cambridge: Harvard University Press.

Lears, T.J. (1985). The Concept of Cultural Hegemony: Problems and Possibilities. *The American Historical Review*, 90(3), 567-593.

Lessig, L. (1999). *Code and Other Laws of Cyberspace*. New York: Basic Books.

Majone, G. (1989). *Evidence, Argument, & Persuasion in the Policy Process.* New Haven: Yale University Press.

Mathiesen, K. (2008). Access to Information as a Human Right. Retrieved September 17, 2014, from, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1264666

Mauger, J. (2012). Collection Management, Conceptual Anachronisms, and CIPA. *Progressive Librarian*, 38/39, 25-33.

Meiklejohn, A. (1948/2004). *Free Speech and Its Relation to Self-Government*. Clark, NJ: The Lawbook Exchange Ltd.

Milan, S., & Hintz, A. (2013). Networked Collective Action and the Institutionalized Policy Debate: Bringing Cyberactivism to the Policy Arena? *Policy and Internet*, 5(1), 7-26.

Mill, J.S. (1859/2008). *On Liberty.* Charleston, SC: BiblioBazaar.

Miller v. California, 413 U.S. 15 (1973).

Monberg, J. (2005). Science and Technology Studies Approaches to Internet Research. *The Information Society*, 21, 281-284.

Mooo.com. (2014). Welcome! Retrieved from, http://mooo.com/.

Mumford, L. (1964). Authoritarian and Democratic Technics. *Technology and Culture*, 5, 1-8.

Munro, W. B. (1930). Home rule. Encyclopaedia of the social sciences, 7, 434-436.

Mukerji, C. (1997). *Territorial ambitions and the gardens of Versailles*. Cambridge: Cambridge University Press.

Mukerji, C. (2009). *Impossible Engineering: Technology and Territoriality on the Canal du Midi.* Princeton: Princeton University Press.

Musiani, F. (2013). Network architecture as internet governance. *Internet Policy Review*, 2(4).

National Endowment for the Arts v. Finley, 524 U.S. 569 (1998).

NetCoalition. (2011). H.R. 3261, "SOPA" Explanation of Bill and Summary of Concerns. Retrieved April 4, 2013, from https://www.cdt.org/files/pdfs/NC-Analysis_of_HR3261_FINAL.pdf.

Nickel, James. (2007) Human Rights. *The Stanford Encyclopedia of Philosophy*. E. Zalta (Ed.). Retrieved from, http://plato.stanford.edu/archives/sum2007/entries/rights-human/

Nisbet, M. (2010). Knowledge into Action: Framing the Debates over Climate Change and Poverty. *Doing News Framing Analysis: Empirical and Theoretical Perspectives*, D'Angelo & Kuypers (Eds.). New York: Routledge.

Noble, D. (1986). *Forces of production: A social history of industrial automation*. New York: Oxford University Press.

Pan, Z., & Kosicki, G. (1993). Framing Analysis: An Approach to News Discourse. *Political Communication*, 10, 55-75.

Pfaffenberger, B. (1992). Technological Dramas. *Science, Technology, & Human Values*, 17(3), 282-312.

PFLAG v. Camdenton R-III School District, 853 F. Supp. 2d 888 - Dist. Court, WD Missouri (2012).

Pitt, J. (2000). *Thinking About Technology: Foundations of the Philosophy of Technology*. New York, NY: Seven Bridges Press.

Postigo, H. (2012). *The Digital Rights Movement: The Role of Technology in Subverting Digital Copyright*. Cambridge: MIT Press.

Public Law 92-484, 1972. An Act to Establish an Office of Technology Assessment.

Rein, M., & Schon, D. (1991). Frame reflective discourse. *Social Sciences and Modern States*, Wagner, Weiss, Wittrock & Wollman (Eds.). Cambridge: Cambridge University Press.

Reno v. ACLU, 521 U.S. 844 (1997). Retrieved June 12, 2012, from http://www.law.cornell.edu/supct/html/historics/USSC_CR_0521_0844_ZS.html.

Renton v. Playtime Theatres, Inc., 475 U.S. 41 (1986).

Richardson, C., et al. (2002). Does Pornography-Blocking Software Block Access to Health Information on the Internet? *The Journal of the American Medical Association,* 288(22), 2887-2894.

Rimm, M. (1995). Marketing Pornography on the Information Superhighway: A Survey of 917,410 Images, Descriptions, Short Stories, and Animations Downloaded 8.5 Million Times by Consumers in Over 2000 Cities in Forty Countries, Provinces, and Territories. *Georgetown Law Journal*, 83(5), 1849-1915.

Samson, T. (2011). Feds wrongly link 84,000 seized sites to child porn. *Infoworld*. Retrieved from, http://www.infoworld.com/article/2623453/federal-regulations/feds-wrongly-links-84-000-seized-sites-to-child-porn.html

Schon, D., & Rein, M. (1994). *Frame Reflection: Toward the Resolution of Intractable Policy Controversies*. New York: Basic Books.

Sclove, R. (1995). *Democracy and Technology*. New York: The Guilford Press.

Scott, J. (1998). *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*. New Haven: Yale University Press.

Senate Report 104-230 – Telecommunications Competition and Deregulation Act of 1995.

Senate Report 106-141 – Children's Internet Protection Act.

Smith, B. (2009). *Mandatory Internet Filtering in Public Libraries: The Disconnect Between Law and Technology* (Unpublished doctoral dissertation). University of Florida, Gainesville, Florida.

Snow, D., et al. (1986). Frame Alignment Processes, Micromobilization, and Movement Participation. *American Sociological Review*, 51, 464-481.

Snow, D., & Benford R. (1988). Ideology, Frame Resonance, and Participant Mobilization. *International Social Movement Research*, 1, 197-217.

Solum, L. (2008). *Models of Internet Governance*. University of Illinois Public Law Research Paper No. 07-25 and University of Illinois Law & Economics Research Paper No. LE08-027).

Sopastrike.com. (2014). Victory! Retrieved from, http://www.sopastrike.com/.

Staksrud, E. (2013). *Children in the Online World: Risk, Regulation, Rights*. Surrey, UK: Ashgate Publishing, Ltd.

Stop Online Piracy Act of 2011, (SOPA), H.R. 3261, 112th Cong. (2011).

Strauss, A., & Corbin, J. (1998). *Qualitative Analysis for Social Scientists*. New York: Cambridge University Press.

Suchman, L. (1994). Do Categories Have Politics? The language/action perspective reconsidered. *Computer Supported Cooperative Work*, 2, 177-190.

Terkel, A. (2008, August 13). John McCain, Internet dunce. *Salon*. Retrieved from http://www.salon.com/2008/08/13/john_mccain_technology/.

Thorpe, C. (2008). Political Theory in Science and Technology Studies. *The Handbook of Science and Technology Studies*, Hackett, Amsterdamska, Lynch, & Wajcman (Eds.). Cambridge: MIT Press.

Top Ten Reviews. (2014). 2014 Best: Internet Filter Software Review. Retrieved from, http://internet-filter-review.toptenreviews.com/.

Trauth, E. (1986). An integrative approach to information policy research. *Telecommunications Policy*, 41-50.

United States v. American Library Association, 539 U.S. 194 (2003).

Warburton, N. (2009). *Free Speech: A Very Short Introduction*. Oxford: Oxford University Press.

Wasserman, T. (2012). SOPA Is Dead: Smith Pulls Bill. *Mashable*. Retrieved from, http://mashable.com/2012/01/20/sopa-is-dead-smith-pulls-bill/.

Weimer, D., & Vining, A. (2005). *Policy Analysis: Concepts and Practice, 4th Edition.* Upper Saddle River, NJ: Prentice Hall.

Weimer, D., & Vining, A. (2011). *Policy Analysis: Concepts and Practice, 5th Edition*. Boston: Longman.

Willard, N. (2002). *Filtering Software: The Religious Connection*. Center for Advanced Technology in Education. Retrieved July 6, 2012, from http://www.ntia.doc.gov/legacy/ntiahome/ntiageneral/cipacomments/pre/willard/FSRCreport.htm.

Williams, R., & Benford, R. (2000). Two Faces of Collective Action Frames: A Theoretical Consideration. *Current Perspectives in Social Theory*, 20, 127-151.

Winner, L. (1977). *Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought*. Cambridge: MIT Press.

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

Zald, M. (1996). Culture, ideology, and strategic framing. *Comparative Perspectives on Social Movements; Political Opportunities, Mobilizing Structures, and Cultural Framings*, McAdam, McCarthy, & Zald (Eds.), Cambridge: Cambridge University Press.

CURRICULUM VITAE

Jeremy Mauger

Place of Birth: Morgantown, West Virginia

Education

B.A., Gustavus Adolphus College, May 1999
Major: Sociology and Anthropology
Minor: Criminal Justice

M.L.I.S., University of Wisconsin-Milwaukee, May 2010
Major: Information Law, Policy, and Ethics

Ph.D., University of Wisconsin-Milwaukee, December 2014 (anticipated)
Major: Information Law, Policy, and Ethics
Minor: Political Science

Dissertation Title: Framing the Policy Debate: Competing Portrayals of Technology in Online Content Regulation and Lessons from Science and Technology Studies

Publications

Mauger, J. (2014). The Children's Internet Protection Act and Commercial Filtering Software: Perspectives from Science and Technology Studies. *First Monday*, In Review.

Mauger, J. (2012). Book Review: The Digital Rights Movement, by Hector Postigo. *Center for Information Policy Research*, December 12, 2012.

Mauger, J. (2012). Collection Management, Conceptual Anachronisms, and CIPA. *Progressive Librarian*, 38/39, 25-33.

Mauger, J. (2012). Internet Filtering in Public Libraries – New Decision in the Bradburn Case. *Center for Information Policy Research*, April 19, 2012.

Mauger, J. (2011). Google Book Search: The Decision Not to Digitize. *Michaelzimmer.org*, January 7, 2011.

Teaching Experience

Guest Lecturer for Dr. Maria Haigh, summer 2013:
"Internet Filtering, Sovereignty & Intermediaries" and
"Cyberwarfare and Information Security"

Teaching Assistant for Dr. Iris Xie, fall 2012:
Digital Libraries

Teaching Assistant for Dr. Michael Zimmer, spring 2012:
Introduction to Information Science

Guest Lecturer for Dr. Iris Xie, spring 2010:
"Creating a Digital Library: The Internet Research Ethics Digital Library"

Presentations

2014 Telecommunications Policy Research Conference
Invited Participant, Graduate Student Consortium
September 2014 - George Mason Law School, Washington, D.C.

2012 Conference of the Association of Internet Researchers
Peer Reviewed & Invited Presentation
"Internet Filtering in Denmark: The Case of Pirate Bay"
October 2012 - Salford University, Manchester, UK

2012 SLIS/SOIS Research Forum
Peer Reviewed & Invited Presentation
"CIPA: Internet Filtering as Collection Management"
April 2012 - University of Wisconsin-Madison

2011 IACAP Conference
Peer Reviewed & Invited Presentation
"Internet Research Ethics: Core Challenges, New Directions"
July, 2011 - Aarhus Universitet, Aarhus, Denmark

2010 Student Research Day
Peer-Reviewed & Invited Poster
"CIPA as Applied – Questions of Practice and Constitutionality"
November, 2010 - University of Wisconsin–Milwaukee

2010 Conference of the Association of Internet Researchers
Peer-Reviewed & Invited Presentation
"The Internet Research Ethics Digital Library, Resource Center, and Commons"
October, 2010 - Chalmers University of Technology, Gothenburg, Sweden

Awards

Doctoral Research Award Grant: spring 2014
Selected for award by the School of Information Studies Doctoral Committee

Chancellor's Award: Received annually 2011, 2012, 2013, and 2014
Selected for award by the School of Information Studies Doctoral Committee

Dean's Scholarship: September 2010 through May 2011
Selected for award by the School of Information Studies Doctoral Committee

Service

Treasurer: 2013 to 2014
Social Studies of Information Research Group, School of Information Studies
University of Wisconsin-Milwaukee

International Association for Computing & Philosophy
Conference Organizing Committee: July 2011
Aarhus, Denmark

Computer Ethics Philosophical Enquiry
Conference Organizing Committee: June 2011
Milwaukee, Wisconsin

Association of Internet Researchers
Conference Organizing Committee: October 2009
Milwaukee, Wisconsin

Other Relevant Work Experience

Visiting Scholar: Summer 2011
Department of Information and Media Studies, Aarhus University, Denmark

Assistant Editor: May 2010
European Science Foundation, EUROCORES Programme
"Eurocores Theme Proposal 2010 –Bridging domains"

Litigation Data Management Specialist: February 2002 through June 2008
Halleland Lewis Nilan & Johnson, P.A.
Minneapolis, Minnesota