

## *BOOK REVIEWS*

### BELLING THE CAT, VIRTUALLY

#### REVIEW OF STUART BIEGEL'S BEYOND OUR CONTROL?

SHUBHA GHOSH

ASSOCIATE PROFESSOR OF LAW

UNIVERSITY AT BUFFALO LAW SCHOOL, SUNY

#### I.

##### SEARCHING FOR A DARK CAT IN A DARK ROOM

At the dawn of the Age of the Internet, almost seven years ago now, several scholars gathered in Palo Alto to discuss how to characterize the set of social and economic relationships that has been, since the gathering, referred to as Cyberspace.<sup>1</sup> There were those who argued that Cyberspace broke all the rules and mandated completely new ones. There were others who said that nothing was different; the law always adapted to new communication technologies and the law would adapt to Cyberspace. There were even those who contended that no law, new or old, was appropriate; Cyberspace would be an open domain for freedom and the distribution, management, and production of information.

Stuart Biegel, professor of law at UCLA, has provided an excellent overview of this early debate and a thorough discussion of the legal issues surrounding Cyberspace in his recent *BEYOND OUR CONTROL?*<sup>2</sup> The book's title asks a question that Biegel answers in the negative. Cyberspace is not unregulable; in fact, Biegel would argue that to say that any set of relationships is unregulable is to misunderstand the meaning of regulation and law. The real questions are how Cyberspace is to be controlled and who governs.

Biegel's book builds on several other prominent books on the law of Cyberspace, most particularly Lawrence Lessig's *Code and Other Tales of Cyberspace*. Like Lessig, Biegel recognizes that regulation is not simply a matter of state control. Corporate control can be as intrusive as public, governmental control. In fact, corporate control and

---

<sup>1</sup> *Symposium: Surveying Law and Borders*, 48 STAN. L. REV. 1367 (May 1996).

<sup>2</sup> Stuart Biegel, *BEYOND OUR CONTROL?: CONFRONTING THE LIMITS OF OUR LEGAL SYSTEM IN THE AGE OF CYBERSPACE* (2001).

governmental control can work hand in hand to regulate relationships in cyberspace, such as through copyright law and other areas of intellectual property law. The choice is not between wholly public or wholly private systems. The control of Cyberspace occurs through a mix of private regulation and public law. Democratic principles demand such a mix of regulation to insure that neither big government nor big business controls the future and progress of the technology of the Internet and the entity that is Cyberspace.

In fact, most commentators would argue that this mix of public and private control would apply to non-Cyberspace relationships as well.<sup>3</sup> Telecommunications, electricity, airlines, security—each can be more effectively and equitably provided through a mix of private and public regulation than through either method alone. The difficult question is whether the regulation of Cyberspace requires a different body of regulation than the regulation of other activities. For example, is Cyberspace regulation simply an extension of telecommunication law since Cyberspace is a mere collection of interconnected computer servers joined by telephone lines? Or to take another example, is the regulation of obscenity in Cyberspace any different from the control of obscenity distributed through magazine racks, television, or movie theaters? The same question can be asked for intellectual property law: does Cyberspace require a revamped law of copyright and trademark? On one level, the answer seems to be yes. The medium of Cyberspace is different from that of television or magazines. And even if Cyberspace is essentially a collection of computers and telephone lines, the whole is substantively different from the parts. But despite the technological differences, many would argue that nothing is really different. What is obscene in a magazine would logically also be obscene on a web page. And theft of content, whether through VCR or through peer- to-peer sharing on the Internet, is still theft and subject to Copyright law. Even if Cyberspace is regulable, the question still remains whether the development of Cyberspace really changes anything.

Professor Biegel gives a measured response. Sometimes Cyberspace regulation mandates new laws, and sometimes the existing laws would work just fine. What Biegel provides is a method to determine whether new laws are needed and what shape this new law might take. He structures his analysis around four problems that he finds critical to the debate over regulation of Cyberspace: (1) the regulation of dangerous conduct, or what Biegel calls cyberterrorism; (2) the regulation of fraudulent conduct, such as swindles and scams; (3) the regulation

---

<sup>3</sup> Lawrence Lessig, *CODE AND OTHER TALES OF CYBERSPACE* (1999).

of unlawful anarchic conduct, by which Biegel means theft of content and sharing of online content; and (4) the regulation of inappropriate conduct, by which Biegel means hate speech. For each type of harm, Biegel assesses the need for regulation and the form of regulation if necessary. There are three basic types of regulation that Biegel plays with: (1) traditional regulation, such as existing domestic statutes and common law; (2) international models of regulation, such as treaties and international organizations; and (3) the architecture of cyberspace, such as filtering software or encryption. Biegel's book is a very thorough study of what types of regulation (if any) are appropriate to control the four problems that he sees in Cyberspace.

Biegel's book is an important one; it integrates a lot of material and talks about several current and ongoing cases. While many readers will turn to it to catch up on developments in Cyberspace law, many will also recognize that the book may well be obsolete within a year or two. What perseveres is Biegel's method for analyzing the problems of Cyberspace. There is much merit to his method. The major weakness to his approach is that it shortchanges the economic issues raised by Cyberspace. But Biegel's approach is flexible enough to incorporate economic concerns, a point I address in Section Two. What the approach begs is an answer to the key question whether cyberspace is in fact different. The problem is that Professor Biegel does not have a very useful definition of Cyberspace. It is not clear what it is that he is trying to regulate.

All of which is reminiscent of an anecdote about the method of historians and the method of economists. The joke is that historians are in search of a black cat in a dark room. Economists, however, are in search of a black cat in a dark room that the cat has just left. Writers on Cyberspace are often attempting to bell the black cat in a dark room by sitting in the room and pondering: "What's a cat?" But despite the jokes, I contend that we can better understand what is the black cat we are trying to bell as well as the dark room that we as lawyers find ourselves in when we are talking about Cyberspace by an appeal to economics and to history. Because of course Cyberspace is a little bit different and somewhat identical to what preceded it and what it coexists with, and in addressing the kinds of issues that Professor Biegel addresses, we need to be aware of the similarities and the differences.

## II. PROFESSOR BIEGEL'S METHOD

Professor Biegel concludes that Cyberspace is not beyond our control. Whether it is the government or big business, some entity will control. The difficult question, according to Biegel, is sorting out how Cyberspace should be regulated. To answer this question, Biegel offers the following approach:

- (1) First ask into which of the following four categories a particular problem falls:
  - (i) dangerous conduct
  - (ii) fraudulent conduct
  - (iii) unlawful anarchic conduct
  - (iv) inappropriate conduct;<sup>4</sup>
- (2) Then ask whether a consensus exists as to whether regulation is needed to address the problem;<sup>5</sup>
- (3) Next ask whether existing law can address the problem or whether the law needs to be adapted to the domain of Cyberspace;<sup>6</sup> and finally,
- (4) Determine what mix of traditional regulation, international law, and architecture is appropriate to address the problem.<sup>7</sup>

Using this four step method, Biegel assesses the types of regulation that are appropriate for different types of Cyberspace-based activities, such as digital downloading of music and hate speech.

Biegel's methodology is commendable for contributing order to the somewhat fractured debate over Cyberspace law. He carefully does not take a stand on whether Cyberspace is new or not. Nor does he entertain rhetoric on liberty and anarchy in Cyberspace or the death of Copyright or the resurgence of property. Instead, he applies a lawyerly, almost bureaucratic, approach, recognizing traditional legal issues and the challenges posed by new technologies. I think the approach marks an important step forward and a useful synthesis of existing case law and law review writings for classroom instruction or for the uninitiated, but interested, lay person.

The problem is that Biegel's methodology is just a bit too neat—so neat, in fact, that there is concern whether there is some substance. The four categories of harms he suggests can be quibbled with but, I would argue, are fairly accurate and thorough. More troubling is asking whether there is a consensus over the regulation, the second step of his method. By consensus, Biegel does not seek unanimity, nor is

---

<sup>4</sup> Biegel, *supra* note 2 at 224.

<sup>5</sup> *Id.*

<sup>6</sup> *Id.*

<sup>7</sup> *Id.*

he seeking majoritarian agreement. Biegel's analysis of consensus is a qualitative one; he could just as easily have used the word "compelling interest" or "urgent need." Even as a qualitative matter, it is hard to say whether his analysis of consensus is any more than a subjective interpretation of a problem. Biegel's subjectivity is uncontroversial when he concludes that there is a consensus for the need to regulate dangerous conduct and fraudulent conduct. Who would defend the need for danger or fraud? But his analysis is unhelpful in analyzing regulation of unlawful anarchic conduct and hate speech. The exact issue is whether activities like digital downloading or selling Nazi memorabilia should or should not be regulated. Placing the question of consensus at the second step, without a framework for assessing consensus, produces a large gap in the usefulness of Biegel's four step approach.

Professor Biegel recognizes this. In his discussion of copyright law, for example, he discusses in great detail the debates over the scope of copyright control and the traditional balance within copyright law between control and access.<sup>8</sup> He points out that balance may have been upset by the expansion of Cyberspace, and that the resulting debate over Copyright has been polarized between strong property rights advocates and proponents of public access. As Biegel concludes, "Agreeing that it is essential to maintain this balance may therefore be an important additional step toward reaching the sort of consensus to move forward in this area."<sup>9</sup> But having said this, he moves on to talk about the uniqueness of Cyberspace and the need for greater appreciation within U.S. copyright law for the balance between private and public, the role of international agreements in policing both copyright infringement and copyright abuse, and the growing importance of technological safeguards to control unauthorized digital downloading. Without an assessment of the type of consensus necessary and how to achieve it, Biegel's discussion sounds more like a litany of possibilities rather than a carefully argued plan of action.

There is nothing wrong with simply listing options. The strength of Biegel's book is in describing the current state of Cyberspace and the debates over the regulation of property and of speech. But to move the debate forward, there needs to be more prescription, which in turn requires a well-structured and powerful analytical approach to assessing the legal and technical problems. I think this is lacking in the book because Professor Biegel does not pay enough attention to

---

<sup>8</sup> Biegel, *supra* note 2 at 293-302.

<sup>9</sup> *Id.* at 284.

really ferreting out and assessing the interests that are implicated by Cyberspace. On one level, this is a simple task. Since Cyberspace is a democratic medium, not in the sense that everyone has access, but that everyone could have access, the interests implicated by Cyberspace are in some ways no different from those that exist in real space: corporate versus populist, commercial versus public-interested, identity-defined versus color-blind, rich versus poor. At another level, one that we may not fully understand, Cyberspace alters conventional interests, exposing traditional fault-lines, such as those between corporate owners and artists, and creating new ones, such as those between artists and users. An interesting example is provided by Professor Jerry Kang's study of racial interactions in Cyberspace.<sup>10</sup> On the one hand, Cyberspace provides a color-blind medium, permitting people to travel anonymously and pseudonymously and hence be judged by the content of their e-mails rather than the color of their skin. In other ways, Cyberspace exacerbates racial tensions through the use of stereotyped icons, chat rooms for skinheads, and free room for racists who can spew invective anonymously and pseudonymously. Professor Kang draws from a rich literature on social psychology to demonstrate how Cyberspace can be regulated in order to control racism within its borders in a way that can spill over into real space. Biegel's approach fails because it rests on a vague search for consensus, as opposed to a clear analysis of the interests implicated and in tension in Cyberspace.

My purpose is not to dismiss Biegel's four step approach but to improve it. I contend that the approach can be improved by appeal to both history and economics. History provides a window into the successes and failures of previous attempts to regulate technology, whether the telephone or television. Economics provides a method to identify the competing interests and assess the institutional structures—whether market or non-market—needed to align and reconcile (if possible) the various interests. Despite the bad jokes about black cats and dark rooms, a more rigorous social science approach to Cyberspace can serve to identify the presence or absence of the cat and how to bell it.

How would such an approach work? In the next section, I directly address Biegel's discussion of the various policy responses to the four categories of harm he identifies. Here let me provide two illustrations.

The first concerns a topic that Biegel does not spend too much time discussing but was a subject of concern in the mid- to late Nineties: the legal status of hyperlinking. There has been no definitive ju-

---

<sup>10</sup> Jerry Kang, *Cyber-race*, 113 HARV. L. REV. 1130 (2000).

dicial ruling on hyperlinking, and most legal analysis focuses on several important settlements. Hyperlinking is an easily recognized phenomenon involving the incorporation of a web address in a web page which permits retrieving information available on the linked page. Hyperlinking can take three forms: direct linking to another page, whereby the user immediately is taken to the linked page; framing, whereby the information from the linked page is incorporated into the linking page, usually in a frame; and imaging, whereby certain graphical content from the linked page is brought to the linking page. Such a practice seems innocuous, but the practice has also created many legal disputes over confusion caused by unauthorized linking. For example, linking to newspaper web pages that have allowed users to access newspaper content has been challenged even when the content is not password protected and is freely available on the Internet. Another challenge has been to linking that allows the user to skip the first set of pages to a web page, pages usually filled with advertising. The legal conflicts simmer below the common and seemingly harmless practice.

Biegel's method is unhelpful in addressing the problems posed by hyperlinking. First, it is difficult to categorize within the four types of harms he describes. Hyperlinking is not dangerous or fraudulent conduct. The practice is different from digital downloading and therefore does not immediately fit into the category of unlawful anarchic conduct. Perhaps, given the ambiguity posed by hyperlinking (does the linker have to get permission or not?), the category of inappropriate conduct is correct, suggesting that Biegel's fourth category is a catch-all, designed to capture all phenomena that fail to fit the other three categories. Even if we could find the correct category, the second question poses a real quandary. Is there a consensus about hyperlinking? The practice is ubiquitous, so seemingly it is accepted as norm for Cyberspace interactions. But there are large interests, such as newspaper publishers, that are concerned with the practice, as evidenced by the disputes. Biegel's second question would have to be answered no.

But pursuing the inquiry along these lines seems to miss the point. The initial reaction that someone may have when posed with the issue of hyperlinking is what is the problem. Hyperlinking seems to benefit everyone, with minimal harm. It is no different from passing on information to a colleague or a friend. More crucially, the information is already public since it is posted on the Internet. Hyperlinking simply makes retrieval and access easier. Comparison could be made with practice outside Cyberspace, such as the use of citation and reference to direct readers to other sources of informa-

tion. A more careful analysis would proceed to look at how hyperlinking occurs and what types of information are shared by and with whom. This consideration would also focus on the economic interests at stake in hyperlinking: why is it that owners of linked web sites sue creators of hyperlinks? For example, in some cases, parties complain that the linking creates a false association with the web site containing a link. In other cases, the concern is that hyperlinking may distort the content of the linked page by either putting the content in a distorting frame or by allowing the user to skip pages that contain valuable advertising and other information. In many ways, what I suggest here is consistent with Biegel's inquiry into consensus. But I am suggesting that this inquiry requires a detailed understanding of social practice, both current and historical, and economics.

Furthermore, the question of what regulation is most appropriate is also more difficult than Biegel suggests. While his three categories of regulation capture well the available options, the categories are at some level too general to be of much value. A more fruitful inquiry might be to ask whether the available legal theories, whether grounded in state common law or federal statute, are appropriate to address the identified harms. In the context of hyperlinking, for example, are the harms of creating a false association, distorting content, or skipping content best dealt with under theories of tort law, property law, or unfair competition law? This inquiry is in part doctrinal to be developed by analogy with existing case law, but in part it is developed by recognizing the need to expand existing case law and statutes. I would argue that this part of the inquiry is in large part an economic one, entailing an inquiry into how legal rights should be assigned and how violations of legal rights should be redressed in order to facilitate and control the practice to be regulated. For hyperlinking, the economic inquiry boils down to one of whether the linker has the right to link or the linked has the right to say no. The question of how to assign the right rests on how we would predict each rule would affect transactions in Cyberspace by raising costs and creating benefits. Once the right is assigned, the next question is how to structure the remedy if the right is violated. In working through these various issues, attention should be paid to institutional details, such as the ability of the courts to enforce certain rights and remedies.

The analysis I describe is a familiar law and economics approach. I would contend that it offers a more structured and systematic means of understanding the issues of consensus and regulatory structure than? Biegel proposes. Although the law and economics approach is fairly bare bones and basic in many ways, it permits broaching more difficult questions, such as what transactions in Cyberspace should or



should not be permitted or whether the paradigm for Cyberspace should be one of monetary transactions or one of gift exchange. The value of what I suggest is to add even more structure to Biegel's four-step inquiry by more rigorously focusing on what interests are at stake and what legal doctrines are appropriate in satisfying these interests.

The application of hyperlinking was described in very fundamental terms. The focus of the inquiry as I framed it was whether hyperlinking should or should not be regulated. But my approach is applicable to even more specific questions, such as whether hyperlinking constitutes copyright infringement. Here the inquiry would focus on applying traditional copyright categories of property rights (reproduction rights, derivative-work rights, distribution rights, display rights) versus limitation on these rights (such as fair use or categories of protected use). The law and economics approach would serve as a guideline for interpreting the copyright statute to see what categories various rights or defenses would apply and how. For example, a fair use analysis of hyperlinking grounded in law and economics would center on giving the linker a right to establish the hyperlink and its attendant transactional costs and benefits. The approach I propose would allow for consideration of a wider range of regulatory means than Biegel proposes and a deeper consideration of the details of how such regulation would affect transactions in Cyberspace.

Professor Biegel offers a systematic approach to analyzing the legal issues raised by Cyberspace regulation. The approach, however, simplifies the interest analysis and provides too general a set of regulatory tools. In this section, I have tried to add greater structure [Two sentences from now, you say that his method is "so structured," which makes this comment sound odd. Maybe it's something else you added?] to Biegel's approach by appealing to traditional law and economics methodology. In the next section, I discuss Biegel's discussion of four specific problems in Cyberspace law and show how an enriched approach can aid us in structuring the legal institutions that govern Cyberspace.

### III.

#### NATIONAL, INTERNATIONAL AND ARCHITECTURAL REGULATIONS

Professor Biegel's conclusions, constituting the last four chapters of the book, can be succinctly summarized in Table One. The rows of the table describe the four types of harms Biegel identifies; the columns, the three regulatory tools. Each cell of the table summarizes Biegel's prescription for large reform.

TABLE ONE	TRADITIONAL REGULATION	INTERNATIONAL MODEL	ARCHITECTURE
DAINGEROUS CONDUCT	CFAA State law self-defense	Coordination International agency	Filtering Shielding hardware Rerouting
FRAUDULENT CONDUCT	FTC actions	Information sharing	Not pertinent
UNLAWFUL ANARCHIC CONDUCT	Copyright law	TRIPS	Technical protection services
INAPPROPRIATE CONDUCT	First Amendment	Global baseline for hate speech?	Not pertinent

For example, with respect to dangerous conduct, Biegel identifies several federal and state statutes in the United States that would serve as a basis for regulating dangerous conduct.<sup>11</sup> He also find several international mechanisms, such as coordination and the creation of an international agency to deal with dangerous conduct.<sup>12</sup> Finally, he identifies several technical solutions that would change the Internet architecture to control dangerous conduct in Cyberspace.<sup>13</sup> It is important to point out that Biegel limits dangerous conduct in the later chapters of the book to cyberterrorism, or the hacking into and destruction of computer software and hardware, such as through the transmission of a computer virus. As a result, his discussion is uncontroversial. Traditional regulation, consisting of federal law under the Computer Fraud and Abuse Act (CFAA) and state law (such as causes of action under common law tort or state statute for conversion, trespass, or trespass to chattels), already exists to deal with such problems. Similarly, international coordination among nation states in combating the transmission of computer worms and viruses is also well-developed. Finally, the use of firewalls and filtering softwares that can detect for viruses is also well-known. Professor Biegel brings together much of the current state of knowledge on the topic of cyberterrorism, a well-recognized problem with readily understood solutions.

The problem is that the regulatory issues are far from clear. While no one (except for the most rabid of anarchists) would argue against the legal regulation and criminalization of cyberterrorism, the debates are in the form of regulation. While Professor Biegel does an exquisite job in detailing the role of traditional regulation, interna-

<sup>11</sup> Biegel, *supra* note 2 at 236-8.

<sup>12</sup> *Id.* at 247-50.

<sup>13</sup> *Id.* at 250-1.

tional enforcement, and architecture in combating cyberterrorism, he ignores some important fault lines. For example, does the existence of technological safeguards negate the need for a legal cause of action in tort or under state law? Phrasing the question more technically, does the availability of architecture-based solutions serve as a defense to a tort of cyberterrorism (brought, for example, under a trespass theory)? If appropriate technological safeguards exist, such as scanning for viruses, can failure to use such safeguards constitute consent or assumption of risk, depending upon the tort theory? No court has directly addressed this issue, but the co-existence of technological safeguards and traditional regulation may produce a redundancy unless private self-help and private law complement each other in combatting cyberterrorism. Biegel flirts with this issue when he discusses the defense of self-defense in the case of traditional regulation.<sup>14</sup> His point is that private retaliation may be justified when some entity is the victim of cyberterrorism, if the response is reasonable and proportional. The bigger question of the relationship between private law and self-help in Cyberspace is ignored.

Much of my discussion applies equally to Biegel's discussion of fraudulent conduct in Cyberspace. But Biegel's conclusions with respect to fraudulent conduct rest on firmer foundations. Once again there is a consensus that fraud should be regulated. I would go further and say that Cyberspace provides another venue for traditional fraud without really changing the legal or social harms in any way. Cyberspace multiplies the number of instances and types of fraud that can now occur. Consequently, Biegel correctly focuses his discussion on the role of the Federal Trade Commission in policing on-line fraud and the importance of global coordination through information sharing in order to combat fraud on the international level. His conclusion that technological safeguards are less pertinent is also hard to dispute.

It is in the last two chapters of the book, when Biegel turns to copyright infringement and hate speech, that the fractures in Biegel's approach become most apparent. Once again, the chapters are thorough and well researched. The materials serve as a fairly up-to-date source on contemporary issues (contemporary meaning the date when Biegel finished his manuscript, given the rapid clip at which Cyberspace law gets made). But Biegel does not do justice in cracking the complications. To be fair, no one person could realistically address all the issues raised by Copyright law and by hate speech regulation. But Biegel's analyses of Copyright and hate speech, suggest that, at least with respect to these two categories of harms, Cyberspace is beyond

---

<sup>14</sup> *Id.* at 242-6.

our control. That is too negative, and supplementing Biegel's discussion with a careful consideration of interest group analysis might justify a more positive conclusion.

Biegel admits that the issue of copyright infringement is a knotty problem for Cyberspace regulation. Focusing on the practice of digital downloading of music (which is quickly expanding to include downloading of video, text, and other works), Biegel recognizes that there is no consensus whether such activity should be regulated.<sup>15</sup> A majority of copyright owners urge that digital downloads are copyright infringement pure and simple. A coalition of users and owners argue that digital downloads either do not constitute copyright infringement or are justified under the fair use doctrine. At the heart of the dispute are differing conceptions of the benefits and costs of digital downloading. Copyright defenders assert the rights of copyright owners to control and profit from every possible distribution and use of their works; the opponents contend that there is very little harm from digital downloading, with substantial benefits to users and to less established artists trying to establish a foothold in the marketplace. As Biegel points out, these tensions reflect the broader and historically recurring issues in Copyright law between owners and users.<sup>16</sup> Lack of a clear consensus should not be seen as a basis for failing to pursue regulation and maintaining the status quo. In the realm of copyright, the status quo is one of contention.

The question for Biegel is whether situating the terms of copyright debates in Cyberspace reformulates the debate in any way. With respect to that question, the answer really does turn out to be no, at least in the terms of Biegel's method. Biegel's treatment of the Copyright controversies is a solid discussion of the salient issues in United States Copyright law (well-laid-out in a trilogy of cases, *Diamond Rio*,<sup>17</sup> *MP3.com*,<sup>18</sup> and *Napster*<sup>19</sup>) and a brief overview of the TRIPS agreement, which imposes some minimum standards that each member state must meet in designing its copyright law.<sup>20</sup> Biegel concludes that the primary difficulty in creating effective traditional or international regulation is in establishing a baseline on fair use. Biegel proposes that the appropriate baseline is one of permitting *de minimis*

---

<sup>15</sup> *Id.* at 282-4.

<sup>16</sup> *Id.* at 297-301.

<sup>17</sup> *Recording Indus. Ass'n of America v. Diamond Multimedia Sys., Inc.*, 180 F.3d 1072 (9th Cir. 1999).

<sup>18</sup> *UMG Recordings, Inc. v. MP3.com, Inc.*, 92 F. Supp. 2d 349 (S.D.N.Y. 2000).

<sup>19</sup> *A&M Records Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001).

<sup>20</sup> Biegel, *supra* note 2 at 310-3.

private non-commercial copying.<sup>21</sup> I would tend to agree that this baseline is appropriate (although far from simple to enforce), but I am hesitant in accepting the position that absent such a baseline regulation is not possible. Biegel concludes that technical safeguards always exist to protect the copyright holder, such as password-protected sites or encrypted content.<sup>22</sup> Professor Biegel almost suggests that regulation would move in this direction even if the appropriate baseline for domestic and international regulation were not established. But such technical safeguards will not resolve the Copyright issues. As the recent Second Circuit decision in the Corley case illustrates, the relationship between fair use and the violation of technical safeguards is an open question (although the future does not appear to be bright for fair use).<sup>23</sup>

Biegel is equally pessimistic about our ability to control hate speech in Cyberspace.<sup>24</sup> The primary difficulty is that United States law is so different from the rest of the world in the regulation of hate speech, while much of the speech that nation states find regulable as hate speech can be traced to United States Internet Service Providers and United States web site owners. The regulation of hate speech is extremely limited by the First Amendment protections for speech. Except for obscene speech and fighting words (the latter almost a nullity), regulation of hate speech is forbidden as a viewpoint-based restriction on speech. The rest of world accepts a wider set of speech regulations, including the banning of certain materials such as Nazi literature (and other paraphernalia). As Biegel accurately points out, the United States is not going to move on this issue.<sup>25</sup> Nor will the rest of the world. Since Cyberspace is not constrained by territorial boundaries, providing a soapbox that effectively reaches the entire planet (or at least those portions of the planet appropriately wired), the lack of an international consensus on the regulation of speech undermines the possibility of regulating speech that many citizens find hateful or offensive. Biegel points out that technological means of regulation are non-existent in controlling hate speech.<sup>26</sup> In some ways, he overstates this point, because in theory one can filter out certain types of offensive information. But these filters will often be quite coarse and ineffective. Interestingly, Biegel points out that technological means may aid in ferreting out hate speech by allowing anti-

---

<sup>21</sup> *Id.* at 320.

<sup>22</sup> *Id.* at 317-9.

<sup>23</sup> *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2nd Cir. 2001).

<sup>24</sup> Biegel, *supra* note 2 at 351-2.

<sup>25</sup> *Id.* at 325-6.

<sup>26</sup> *Id.* at 349.

hate-speech groups to monitor the distributors and creators of hate speech.<sup>27</sup> But this use of technology presumes the free and open marketplace of ideas that is the basis for United States First Amendment law.

Biegel completed his manuscript before the recent decision by a district court in the Yahoo! case.<sup>28</sup> In that decision, the district court ruled that a judgment by a French tribunal against Yahoo!-USA for allowing the sale of Nazi memorabilia in France through its United States auction site could not be enforced in a United States court because of conflict with the First Amendment. The result was a correct one, but the reasoning was far from clear. The court seemed to be saying that the order by the French tribunal requiring Yahoo!-USA to establish certain filters to ensure that French citizens could not purchase or otherwise have access to Nazi memorabilia could not be issued by a United States court without violating the First Amendment.<sup>29</sup> Consequently, a United States court could not enforce the judgment of a foreign court that the United States court itself could not issue.<sup>30</sup> It is far from clear whether the court was undertaking a vagueness, an overbreadth, or a prior restraint analysis of the foreign judgment (and, more importantly, whether any of these types of analyses was appropriate). If the issue were one of vagueness or overbreadth, then the court's concern was that the order would chill protected speech as well as unprotected speech and have harmful First Amendment effects. If this were the court's reasoning, then perhaps foreign judgments that were more narrowly tailored or were limited to money damages would pass constitutional muster. If the court's reasoning were based on prior restraint, then the compelling question becomes one of whose First Amendment rights are violated: Yahoo!-USA's? United States users of Yahoo!-USA? Those United States users seeking to distribute Nazi paraphernalia? The question of whose rights is important in light of the relevant question of the status of computer code as speech, a subject I end this section with. The district court's decision in the Yahoo!-USA case most clearly can be seen as a case of an evolving customary international law of free speech, although the court's failure to use the word custom perhaps indicates a tacit recognition that free speech is far from the norm in the international arena.

---

<sup>27</sup> *Id.* at 351-2.

<sup>28</sup> Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 169 F. Supp. 2d 1181 (N.D. Cal. 2001).

<sup>29</sup> *Id.* at 1189.

<sup>30</sup> *Id.*

The problems Professor Biegel sees with the regulation of unlawful anarchic conduct and inappropriate conduct in Cyberspace—the issues of copyright infringement and hate speech—seem insurmountable. But insurmountable does not necessarily mean unregulable. Regulation in these two areas is difficult and tricky. Biegel does a thorough job in presenting the legal issues, but there needs to be more work on discerning the structural problems posed by copyright and hate speech. Once the structure is understood, we can move closer, I hope, to understanding the shape of appropriate regulation.

The point that is missing from Professor Biegel's analysis of digital downloading and hate speech is the conception of computer code as speech. In the *Yahoo!-USA* case, the court is unclear as to whose free speech interests are violated; the court asserts that a U.S. court would be restricted in issuing an order equivalent to the French court's order without violating the First Amendment. But it should make a difference whether it is the purveyors of the Nazi materials, potential U.S. purchasers of the materials, or *Yahoo!-USA* whose First Amendment rights are violated. If it is the first two, then perhaps the order could be rectified by the payment of a fine by *Yahoo!-USA* or by *Yahoo!-USA*'s providing each French citizen the appropriate filtering software to block Nazi related materials. If it is *Yahoo!-USA*'s rights, then deeper questions are raised. What type of right is this, a pure speech right or a commercial speech right? A more difficult question is one of consistency. If *Yahoo!-USA*'s free speech rights were being violated by an order requiring it to implement the filtering software, then why were *Napster*'s rights not similarly violated when it was ordered to filter copyrighted work from uncopyrighted works that were being shared through its peer-to-peer system? To say that the answer rests on the fact that *Napster* was engaged in the distribution of copyright-protected materials and that the First Amendment does not protect illegal speech seemingly begs the question, since the main question we are interested in is the role of the First Amendment in trumping copyright infringement, just as the First Amendment trumps the regulation of hate speech.

The tension between the First Amendment and Copyright law is a long-lived one, with periods of detente giving way to short episodes of glaring conflict. The most recent conflict arose with the publication of *The Wind Done Gone*, a parody of *Gone With The Wind*.<sup>31</sup> Publication was enjoined by the district court in Georgia, which found that there would be irreparable injury from publication to the holder of the copyright in *Gone With The Wind*. The Eleventh Circuit very soon

---

<sup>31</sup> *Sun Trust Bank v. Houghton Mifflin Co.*, 268 F.3d 1257 (11th Cir. 2001).

after reversed the district court's decision, holding that while there may have been copyright infringement, the injunction against publication violated the First Amendment rights of the author of *The Wind Done Gone*, and that the injury could be repaired by an award of monetary damages.<sup>32</sup> The First Amendment, however, was a casualty in the Second Circuit's decision in the Corley case, having to do with the publication of DECSS, a decryption computer program that allowed hackers to break through the encryption code that scrambled the content of CD's and DVD's.<sup>33</sup> The Second Circuit ruled that Corley's First Amendment rights were not violated, because his computer code was functional speech, something that facilitated or was instrumental to the creation of speech, and hence in a different category from that of core, protected speech. In light of these two decisions, the key question not answered in the Yahoo!-USA case becomes more salient. What was the protected speech interest: the interest in creators and users of Nazi books in having access, or the interest in Yahoo!-USA and other ISP's in writing their code?

I discuss these recent cases to illustrate how compelling and difficult the issues raised by Professor Biegel are and will continue to be. Biegel's recommended solution is to structure rights around two new baselines, the first permitting *de minimis* private non-commercial copying and the second allowing the government to regulate hateful speech.<sup>34</sup> The movement towards the new baselines requires a rejection of an absolutist Copyright law and an absolutist First Amendment. The difficulty is in reconciling Copyright law and the First Amendment. Copyrighted works and infringing works are both forms of expression, potentially subject to First Amendment protection. Allowing Copyright law to serve as a basis to enjoin infringing expression potentially runs into the restrictions of the First Amendment. In the context of Cyberspace, this tension has been sidestepped by categorizing software as a functional speech, an unprotected category of First Amendment speech. The Yahoo!-USA case, currently on appeal, casts some doubt on whether this manouever is consistent with First Amendment law and the trends of international law.

#### IV. TAKING CONTROL

Professor Biegel's book is an important contribution, if for no other reason than its compiling ten years of academic discussion and

---

<sup>32</sup> *Id.* at 1261.

<sup>33</sup> *See* Corley, 273 F.3d 429.

<sup>34</sup> *See* Biegel, *supra* note 2 at 320, 352.



litigation over Cyberspace law. At the core of his book is the recognition that regulation does not rest on a distinction between public and private actors and that private design and architectural choices can be as important and viable a form of regulation as governmentally imposed ones. But the book fails in providing a helpful and thorough perspective of the conflicting interests affected by the regulation of Cyberspace. The focus on consensus in his analytical method is one source of the difficulty. The other is in the author's statement, made at the end of his book, that he is using the term regulation in a neutral way.<sup>35</sup> I am not sure that is possible. Any regulation will affect some groups more than others. Regulation is never neutral in its effects. Recognizing the ranges of interests that are shaped and affected by the various possible Cyberspace laws from which we must choose is necessary in creating the most desirable and appropriate Cyberspace law we can. Professor Biegel's book is helpful in casting some light into a dark room. Will the cat get away?

---

<sup>35</sup> *Id.* at 355.