Harvard Journal of Law & Technology
Volume 15, Number 2 Spring 2002

BEYOND OUR CONTROL? CONFRONTING THE LIMITS OF OUR LEGAL SYSTEM IN THE AGE OF CYBERSPACE

By Stuart Biegel
Cambridge, MA: The MIT Press
Pp. 452. $34.95 (hard). ISBN 0-262-02504-3

*David McPhie**

TABLE OF CONTENTS

A book with an interrogative title naturally prompts readers to scour its pages for an answer. Those who so search Stuart Biegel's book *Beyond Our Control?*[1] will find a study of Internet law that leaves no stone in cyberspace unturned. Blending law, technology, and history, Biegel's well-researched and carefully organized text is one of most comprehensive of its kind. Biegel provides an extensive analysis of a wide range of Internet-related cases, legislation, and treaties. In addition, he explains fundamental First Amendment, copyright, and international law doctrines for the uninitiated reader. Biegel is extremely comfortable with the fine points of the relevant Internet technologies, and his guide through the staggering array of applications, systems, and protocols is consistently straightforward and accurate. In short, the book is a self-contained, introductory course on Internet law, and Biegel proves to be a gifted teacher.

---

* J.D. 2003, Harvard Law School.

1. STUART BIEGEL, BEYOND OUR CONTROL? CONFRONTING THE LIMITS OF OUR LEGAL SYSTEM IN THE AGE OF CYBERSPACE (2001).

Biegel's principal objective in *Beyond Our Control?* is to address the question its title raises by inquiring into "the extent to which the Internet is currently under control and the extent to which [it] can or should be brought under control" (p. xiii). Is the Internet beyond our control? Biegel, lawyer-like, settles upon a classic response: "It depends." Indeed, the main theme of *Beyond Our Control?* is that, given the diversity of legal issues generated by the Internet today, no single regulatory formula can appropriately deal with all of them (p. 358). Biegel instead calls for a more nuanced and individualized study of these issues under an exhaustive and systematic approach that he develops over the course of his book.

I. BOOK SUMMARY

Biegel presents his analytic theory in three parts. Part I (pp. 3–119) lays down the basic foundation for what follows. Biegel begins by identifying a vast diversity in the body of Internet "stakeholders," drawing comparisons to the heterogeneous communities depicted in folklore of the American West. Biegel explores various conceptions of "cyberspace" and cites cases in which the rote application of real-space law to cyberspace has yielded unexpected results. He also delineates the practical limits of law in general, especially in complex contexts such as the Internet.

Chapter 3 is especially important for the development of Biegel's analysis. Here, Biegel assembles a comprehensive listing of "allegedly problematic conduct" online, sorting the conduct into four categories for analytic purposes. The first category is "dangerous conduct," which includes anything that "may impact physical or national safety" (p. 55).[2] The second is "fraudulent conduct," defined here as activity that "may impact economic safety" (p. 65).[3] The third category encompasses other "unlawful anarchic conduct," including illegal activity that does not clearly fit into the first two categories (p. 73).[4] Finally, the "inappropriate conduct" category catches what remains: lawful behavior that is nonetheless "troubling" to some (p. 85).[5]

---

2. The following problems are assigned to the first category: threats of physical injury, cyberstalking, child pornography, unlicensed online health care, and 'cyberterrorism.'" (pp. 55–65).

3. The following problems are assigned to the second category: "hacking" that poses the threat of financial loss, illegal or dishonest privacy violations, cybersquatting, and online fraud (pp. 65–73).

4. The following problems are assigned to the third category: copyright violations, pornography, and online defamation (pp. 73–84).

5. The following problems are assigned to the fourth category: discriminatory harassment online, extremist and hate-related web sites, online censorship and harassment in school settings, "spam," and other privacy violations (pp. 85–95).

In Part II (pp. 123–211), Biegel presents three basic regulatory models for controlling the Internet: "(1) legal frameworks within individual countries, (2) international cooperation, and (3) changes in the architecture [or code] of the Internet itself" (p. 124). Biegel begins with an in-depth account of U.S. attempts to regulate the Internet through legislation and the subsequent constitutional challenges to some of this legislation in the courts, including the successful overturning of key provisions of the Internet "decency" legislation of the late 1990s.[6] Turning to international law, he gives a broad overview of a few different approaches in international law and provides a summary of recent developments in this area.[7] Finally, Biegel presents a technologically savvy look at the code-based underpinnings of the Internet, and the possibilities for further control offered by new and developing technologies (such as filtering capabilities), applied at a variety of levels, from the root domain name servers to the Internet Service Providers and on down to individual users and computers.

In Part III, Biegel builds on the foundation laid in Parts I and II and presents his analytic framework to be used in developing a regulatory response to "problematic conduct" on the Internet. The framework is "comprised of four interrelated parts" (357):

> [W]e first identify the category of allegedly problematic conduct from the list of four broad areas documented in chapter 3 . . . . Next, we explore the potential for consensus [of opinion] among the various stakeholders regarding both the nature and the extent of the problem and the prospects for any sort of regulatory solution. Then we examine just how uniquely cyber this problem might be, and analyze the extent to which such a determination might help answer the question of how we might regulate the problem area. [We finish] by exploring in detail the

6. This legislation included the Communications Decency Act of 1996 (CDA), Pub. L. No. 104-104, 110 Stat. 56, 133–43 (1996), and the Child Online Protection Act of 1998 (COPA), Pub. L. No. 105-277, 112 Stat. 2681–736, 2681–736 to 2681–742 (1998) (codified at 47 U.S.C. § 231 (2002)). Portions of these acts were held to be unconstitutional in Reno v. ACLU, 521 U.S. 844 (1997) [hereinafter *Reno I*] and ACLU v. Reno, 217 F.3d 162 (3d Cir. 2000), *cert. granted*, 532 U.S. 1037 (2001) [hereinafter *Reno II*], respectively.

7. These developments include the adoption of the World Intellectual Property Organization Copyright Treaty, Dec. 20, 1996, S. Treaty Doc. No. 105-17, by the United States and the passage by the World Trade Organization of the Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, LEGAL INSTRUMENTS—RESULTS OF THE URUGUAY ROUND vol. 31, 33 I.L.M. 81 (1994), both of which provide for baseline standards of intellectual property protection on an international scale.

> potential applicability of each of the three basic regulatory models identified in part 2 . . . pointing whenever possible toward a combination of realistic approaches . . . (pp. 224–25).[8]

The remainder of Part III then applies this framework to "four major representative problem areas," with one major problem taken from each of the four Chapter 3 categories. For example, Chapter 9 takes up the problem of cyberterrorism, and Chapter 10 focuses on consumer fraud online in general.

Biegel acknowledges that the final two representative problem areas he addresses — private personal copying and online hate speech — are quite a bit more controversial than the first two, and are, accordingly, more difficult to regulate. He nevertheless dutifully applies his framework to each subject and arrives at some possible solutions.

In the private personal copying context, Biegel ultimately calls for amendments to the copyright statute that would clearly distinguish between uploading and downloading, and would specifically provide an exemption for "de minimis private personal downloading and forwarding of protected works in a networked environment for noncommercial purposes" (p. 306). With regard to hate speech online, Biegel examines and rejects the viability of using existing free speech exemptions under First Amendment law (fighting words, defamation, obscenity, etc.) to put an end to hate speech. He then proposes that hate speech, which is "no less obscene than prurient sexual activity," should be given its own exemption from the First Amendment, similar to that currently existing for obscenity (p. 346).

Biegel concludes his book by noting that because "regulation" can be defined extremely broadly, it is in a certain sense inevitable that the Internet be regulated in some way — indeed, it always has been. The question then becomes one of how we want to regulate, and the answer to that question must necessarily be determined on a case-by-case basis, through a framework like the one he has suggested. Biegel ends with a summary of "twenty regulatory principles [that] can serve as important guidelines for the resolution of Internet-related problems in the coming decade" (p. 359).

Beyond Our Control? provides an excellent and comprehensive summary of the current state of cyberlaw. It is apparent, however, that Biegel's larger aim is not merely to restate the law, but to prescribe a

---

8. In his discussions, Biegel sometimes splits the fourth part of the framework into two distinct steps: (1) analysis of the regulatory models and (2) "synthesis" of solutions found (p. 225). For this reason, he sometimes refers to his analytical method as a "five-step framework" (p. 224). In his application of the framework and book summary, he generally combines the two steps.

process through which legal problems of cyberspace should be addressed in the future. It is therefore instructive to take a closer look at Biegel's four-part framework for analysis, one part at a time.

II. THE FRAMEWORK'S FOUR PARTS

A. Categorization of the Problem

Biegel's persistent promotion of his four categories of "allegedly problematic conduct" is the most puzzling aspect of the framework. First, it is not clear what exactly the four categories are meant to represent. Biegel explains that the categories are situated along a "sliding scale" that indicates, for a given activity, the harm it causes and the consensus that exists regarding the proper way to regulate that activity (p. 223). Each category on that scale, therefore, is meant to signify a grouping of activities with similar harm/consensus values.

Yet, there is a discrepancy between what the categories are meant to signify and how they are in fact defined. When it comes to drawing the actual bounds of each category, Biegel does not directly use harm or consensus, but rather distinguishes according to other factors, such as physical versus economic injury and lawful versus unlawful behavior. In other words, he uses these other factors as proxies for harm and consensus.

Of course, there tend to be strong correlations between these two sets of factors, so it is by no means senseless to match them up in this fashion. For example, the physical-economic distinction closely tracks the harmfulness factor (physical bodily injury is generally considered to be more harmful than economic injury). And where a law has been passed making a particular activity illegal, it is probably because there is at least some sort of minimal consensus among the voting public on the issue (namely, the behavior should be regulated somehow and passing a law is an appropriate method of regulation).

But this correlation is far from exact, and so the four-way sorting at times yields incongruous results. For example, would the widespread distribution of bootleg copies of Windows XP (a category three activity) inflict lesser harm on Microsoft than a "cyberterrorist" attack disabling the official Windows XP sales web site for a day (category one)? Is there a greater consensus regarding how online health care should be regulated (category one) as opposed to something like online fraud (category two) or defamation (category three)? Indeed, the categorizations may be correct, but the book makes no attempt to prove actual consensus or quantify harm, leaving the work instead to the presumptions behind its categories.

Part of the problem here may simply be that in the process of sorting, Biegel is not exactly true to his own categories, loosely defined as

they are. For example, Biegel cites the massive hacking attacks against Yahoo, Amazon, eBay, and others in February 2000 as the "representative case" of cyberterrorism that would fall under category one ("physical harm"). He explains his reasoning through an extensive proof-by-dictionary: the definition of terrorism includes "the systematic use of violence." Violence may be defined as "proceeding from extreme or intense force." The directing of a gigabtye of data every second to a single web site amounts to the "systematic use" of "extreme or intense force." The hacking attacks of February 2000 therefore constitute terrorism. And since "terrorism" obviously implicates physical and national security, the attacks are correctly placed in category one (pp. 231–32).

To be sure, Biegel points out earlier that a cyberterrorist attack could conceivably be used to incapacitate power plants and emergency telephone systems instead of online auctions and bookstores. So is it potential for physical harm (as opposed to actual physical harm) that puts an activity into category one? Apparently not — defamation, for instance, is relegated to measly category three status, despite the fact that Biegel describes in detail a case in which the defamed victim was inundated with death threats and might have gotten physically hurt (p. 134).[9] Defamation would have been included in category one if potential for harm were the defining characteristic for this category.

Behind the classification confusion looms a much larger question: why categorize at all? Ideally, each category of problems would have a corresponding category of similar solutions. Thus, by solving any particular problem in a given category, one would be better equipped to tackle similarly situated problems.

Biegel seems to have this idea in mind when he devotes the latter part of the book to applying the four-part framework to "representative problem[s]" in each of the four categories. For example, Biegel explains that by grouping the activities of category three together,[10] we find a general solution for that category: "[I]t is likely that for each of the [activities in this category] some creative combination of all three regulatory models might work best" (p. 359). This prescription, however, sounds suspiciously similar to the one given a page later in his twenty regulatory principles: "In cyberspace, it is reasonable to assume that a creative combination of approaches will be more effective than any single regulatory strategy" (p. 360). In other words, the category-specific solution is no more specialized than the solution urged for problems in all categories.

---

9. *See* Zeran v. AOL, 129 F.3d 327 (4th Cir. 1997).

10. In the book's conclusion, for example, Biegel refers to the "many useful parallels between personal copying, obscenity, and online defamation [in category three]" (p. 359).

B. Existence of a Consensus

The second part of the framework involves an inquiry into "consensus" — that is, the degree to which there exists a consensus among Internet "stakeholders" as to how a particular cyberspace activity should be regulated, if at all.[11] This idea of consensus is, of course, one of the characteristics that the four categories of part one are supposed to quantify. Thus, the placement of an activity into a category in the first part of the framework helps to resolve the inquiry of the second part; it may, in fact, render that second inquiry wholly unnecessary.[12]

Apparently, the main function of the consensus inquiry is not to promote generation of a solution, but to provide an estimation of the chances that the framework will generate a viable solution. The theory, not surprisingly, is that if there is no consensus in favor of regulation, then "the particular problem area is likely to remain beyond our control" (p. 53).[13] More specifically, Biegel implies that where there is no consensus, regulation via any of the three basic regulatory models (or a combination thereof) will probably fail, and so any solutions generated by the framework must wait for the winds of public opinion to change, if those solutions are to be successfully implemented.[14]

---

11. At a few points in the book, Biegel also incorporates an activity's harmfulness into this concept of consensus: "[P]roblems in cyberspace are most easily and effectively resolved when there is a consensus among the relevant stakeholders regarding both the severity of the harm and the appropriateness of the regulatory approach" (p. 221). Harm and consensus are the two factors measured by the sliding scale of categories in part one of the framework; folding the notion of harm into the concept of consensus would simplify the scale conceptually. Measure of harm would be calculated subjectively by the stakeholders, as opposed to the notion of harm described elsewhere in the book, in which the assumption appears to be that harm from an activity can be more or less objectively determined.

12. Although the four categories are supposed to represent different levels of consensus, activities are not explicitly placed into categories according to consensus level. If consensus were one of the factors used to determine in which category a particular activity should go, then the inquiry of the second step would essentially be performed before the first, and not after.

13. Biegel points out that regulation in the absence of consensus is difficult both at the rule-generating stage and at the enforcement stage (p. 53). Rule-generating is obviously difficult without consensus precisely because rule-generating bodies tend to rely on consensus (verified, e.g., through vote) as part of the procedure through which new rules are enacted. And effective enforcement is impossible without public consensus, Biegel argues, since enforcement agents quickly become overwhelmed as a practical matter if enough of the population simply has no desire to abide by a given law. He cites as examples the dual failures of national alcohol prohibition in the past, and today's ban on marijuana use (pp. 102–05).

14. See, for example, Biegel's discussion of consensus on the hate speech issue (p. 326). Note that Biegel assumes that there is enough give in the First Amendment to provide for a hate speech ban, should the public express widespread demand for such a ban (p. 348) (implying that the reason the ban is unlikely is that "Americans . . . love

This theory is largely accurate when it comes to national and international law. However, the third of Biegel's three regulatory models — code-based regulation — is, by contrast, distinctively impervious to consensus. That is, if the entire world believes that making unauthorized copies of DVDs is acceptable, but DVD manufacturers invent technologies that make DVDs sufficiently difficult to copy, then, ultimately, the public consensus, however strong, will not prevail.[15] This is precisely the beauty of code (or the curse, depending on one's proclivity for bootleg copying).

C. Uniqueness

The question whether or not a particular problem in cyberspace has a suitably similar real-space analog is a very useful one. It is, in fact, exactly the sort of question that lawyers and judges turn to as a matter of course, in the typical examination of precedent.

Biegel infuses the uniqueness inquiry with added formality by painstakingly delineating another set of three categories, each with a corresponding analytic approach. Where there is a very similar real-world problem, then "traditional approaches and existing laws are likely to work best" (p. 223). Where there exists a real-world problem that is similar in some aspects and not in others, then "traditional approaches and existing laws would only constitute part of the regulatory approach" (p. 223). Finally, where there is no analogous real-world problem, then "no one formula is appropriate"; hence, the inquiry should search for possible "unique" solutions under the three regulatory models, or outside those models.[16]

In practice, Biegel properly avoids applying these categories too rigidly. For example, in Biegel's discussion regarding file-sharing online (e.g., the Napster controversy), he begins by noting that the

---

their free speech rights"). The extent to which constitutional principles can and should defer to public opinion is a debatable question, to say the least. *See* R.A.V. v. City of St. Paul, 505 U.S. 377, 391 (1992) ("The First Amendment does not permit [government] to impose special prohibitions on those speakers who express views on disfavored subjects").

15. Biegel acknowledges the distinction Lawrence Lessig makes between "perfect control" and "effective control" (p. 210) (citing LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 57 (1999)). Biegel nevertheless concludes that even "if the architectural changes succeed in locking the digital door. . . . lock-picking tools [may] become easily available to a widespread population" (p. 211). In contrast, Lessig's argument is that, so long as it is enough of a hassle to go to the trouble to pick the lock in the first place, the lock will effectively discourage resistance to regulation. Perhaps Biegel thinks that no code-based lock could ever be tricky enough to provide an effective amount of hassle; Lessig, however, provides the promising counterexample of digital certification using "public key" encryption. *See* LESSIG, *supra*, at 30–42, 54–57.

16. Biegel actually qualifies his categorization by noting that "a given problem may not fall cleanly under any one of these three alternatives" (p. 224).

"proliferation of free and unfettered digital copying" has generated legal issues that go "far beyond" photocopying or videotaping, even "beyond anything that has been seen before" (p. 290). The implication seems to be that the file-sharing issue is a third-category, "totally different," problem, and that we should not waste time tinkering with existing law. As Biegel states when discussing current regulatory solutions, the "national law model not only has not worked, but may in fact be more appropriately characterized a part of the problem than part of the solution" (p. 290).

It later becomes clear, however, that Biegel advocates clarification, not overhaul, of the copyright statute.[17] He admits that "the potential applicability of the national law model must still be considered," despite its limitations (p. 291). The implication is that, although the ability to make perfect copies distinguishes digital copying from analog copying in a highly significant way, there are enough similarities between the two to warn against abandoning the whole of copyright law when crafting a solution. This more moderate approach makes sense. If a specific provision of a copyright statute does not appear to make sense in light of the novelties of digital copying, there is no reason why lawmakers cannot turn to more general legal principles to elucidate a solution, traveling upward through a hierarchy of law in a search for guiding principles.[18]

In fact, on a general level, it is hard to imagine that there exists any problem in cyberspace that it is so utterly different that cannot be informed by existing law and doctrine.[19] Cyber-claims tend to be based ultimately on real-world injuries, for which the law already provides a range of remedies in most cases.[20] This suggests that Biegel's third uniqueness category may, in fact, be an empty set.

We are left, then, with the bulk of "problematic conduct" on the Internet likely falling into the second intermediate category and the corresponding admonition that "traditional approaches and existing laws [should] only constitute part of the regulatory approach" (p.

---

17. Biegel states that "[a] pragmatic approach under traditional national law would begin with clear rules . . . ." (p. 305).

18. This hierarchy may extend all the way to the Constitution. *See* U.S. CONST. art. I, §8, cl. 8 (granting Congress power to promote the "useful Arts, by securing for limited Time to Authors . . . the exclusive Right to their . . . Writings . . . .").

19. *Cf.* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 207 ("[T]he best way to learn the law applicable to specialized endeavors is to study general rules."). Also, compare Biegel's prediction: "[Someday] there will be no such thing as cyberspace law because the online world will be virtually indistinguishable from the offline world. There will be no separate Internet specialization in law . . . because every member of the legal profession will be an Internet lawyer . . . ." (p. 364).

20. Ostensibly the damage that music companies and the Recording Industry Association of America are complaining about — economic loss due to lost sales — is familiar enough.

224). This inquiry might be extended advantageously by looking beyond the degree to which the problem is different from its offline counterpart and examining exactly how the problem is different. This information would provide some direction as to the specific changes or additions that would need to be made to existing law in order to accommodate the new problem.

D. Regulatory Models

Biegel's set of regulatory models might likewise be clarified and expanded. He explicitly catalogues three basic regulatory models in his list: national law, international law, and code. The first two models principally represent actors (national governments and international alliances) that effectuate regulation. In contrast, the third model is a means through which regulation may be effected. For example, a regulator on a national or international level could mandate or regulate the code used by others.[21] To be precise in our analysis, then, it is worthwhile to distinguish between the question of who should regulate and the question of how to regulate.[22] Biegel suggests law and code as the two principal means through which regulation should occur[23] and two principal sets of actors, national and international.[24]

The most conspicuous omission from this second list of actors is the private party. Admittedly, Biegel does discuss the "private ordering" regime, describing it as a sort of "default position" that controls in the absence of other types of regulation (p. 221). However, by explicitly adding it to the analysis of the framework's fourth step, we can create a more comprehensive menu of regulatory options.

This combination of three actors and two methods gives us six distinct regulatory models to examine, as compared to Biegel's original three: (1) national government passes law, (2) national government mandates code, (3) international alliance ratifies treaty, (4) international alliance mandates code, (5) private parties make agree-

---

21. Lessig makes this same point: that government may regulate a subject indirectly by regulating the code that constrains that subject. *See* LESSIG, *supra* note 15, at 91. One example Lessig uses is the Americans with Disabilities Act, which forces builders, under penalty of law, to change the physical architecture of buildings to make them wheelchair-accessible. *Id.*

22. Biegel also expresses an awareness of this distinction at one point (p. 315).

23. As the example above shows, these two means may work in conjunction. *See supra* text accompanying note 21. Of course, we could add to this list of regulatory means; Lessig mentions at least two others, social norms and market forces. LESSIG, *supra* note 15, at 87.

24. These two actors might be considered together in a more general "government actor" category. Biegel admits that the two as regulators are similar: "[T]he same limitations of the law that were discussed on a national level are equally applicable in . . . an international [context]" (p. 176).

ments enforced by law (contract), and (6) private parties implement code.[25]

III. THE FRAMEWORK AS A WHOLE

As a procedural tool for deconstructing the great problems of the Internet, Biegel's four-part framework does not go as far as it might. To begin with, there is nothing about that framework that makes it particularly suited to solving problems in the Internet context, as a simple paraphrase of the four parts makes evident:

(1) Decide how bad the problem is.
(2) See if everyone agrees on a solution to the problem.
(3) Consider similar problems that have been previously solved.
(4) Explore all options and generate a solution.

Many of the sets of categories developed over the course of the book could be applied with equal efficacy to other bodies of law. (We could organize criminal law, for example, according to physical crimes, economic crimes, all other crimes, and legal behavior that some people think should be crimes.) Even the concept of using code to solve legal problems is not limited to the Internet context.[26] Thus, although Biegel's framework successfully arrays the great problems of cyberlaw into a structure, in some cases, we are not any better equipped to tackle them than we were when they were free-floating legal issues.

Even as a general theory of legal analysis to be applied to any area of law, the framework is overly broad. This fact becomes most apparent at the end of the book when Biegel derives from the framework his "list of [twenty] relevant principles that can help guide the regulatory process across the board" (pp. 359–64). These principles include: "review the academic journal databases" for ideas (number 5); "continue to respect the autonomy of individuals" (number 3); "consider the entire range of regulatory approaches" (number 2); "[b]eware of all-or-nothing arguments" (number 4); and "[remember that] there is no . . . quick fix," that "regulatory approaches must be realistic," and that "any attempt [to regulate] must proceed slowly and with great caution" (numbers 19, 16, and 20, respectively).

The greatest concern regarding the framework is that it may actually hinder useful analysis in some contexts. In other words, by dismissing more traditional analytic approaches, some potentially valu-

25. Biegel, in fact, hints at the distinction between (5) and (6) in the fourteenth of his twenty principles, where he compares "private rule-making" and "private architectural adjustment" (p. 362).

26. *See, e.g.*, *supra* note 21.

able critical methods may be lost.[27] This is what happens, for example, in Biegel's application of his framework to the hate speech issue. In applying part four of the framework, Biegel explores the possibilities for regulation at the national level by reviewing the current state of free speech law under the First Amendment.[28] In an excellent summary, he reviews a wide range of recognized free speech exceptions and explains how hate speech cannot fall within any of those exceptions. Yet he ultimately concludes that a new exception for hate speech on the Internet could be carved out of the First Amendment, modeled after the established and "workable" obscenity exception of *Miller* (p. 346).[29]

Biegel does not elaborate upon the details of a hate-speech analog to the *Miller* test. But recollection of his discussion seven chapters earlier regarding the decency provisions of U.S. pornography legislation immediately raises serious questions about the effectiveness of such a test for the Internet. In the course of that earlier discussion, Biegel quotes the Third Circuit's explanation of the inapplicability of the *Miller* test in an online context.[30] Since "the Web is not geographically constrained," the court argues, sending pictures over the Internet is "unlike the voluntary physical mailing of material from one geographic location to another, as in Miller" (p. 394).[31]

Geography matters here because one fundamental aspect of the *Miller* test is that the prurient nature of the transmitted matter is to be judged according to "contemporary community standards."[32] And since "[c]urrent technology prevents Web publishers from . . . limiting their site's content 'from entering any [specific] geographic community,'"[33] a web publisher is forced to adapt published content to satisfy the most restrictive community standard existing in the United States.

---

27. Biegel rejects the "common approach[es]" of categorizing problems under "traditional areas of the law," or under sub-categories such as "freedom of expression, intellectual property, and privacy" (p. 53). He explains that "these organizational frameworks may prove either too broad or too narrow for our purposes" (p. 54).

28. It is difficult to distinguish this sort of analysis from the uniqueness inquiry that presumably takes place in the framework's second part.

29. *See* Miller v. California, 413 U.S. 15, 24 (1973). Biegel quotes verbatim the three prongs of the *Miller* test earlier in this chapter, during his summary of the obscenity standard (p. 330).

30. *See Reno II*, *supra* note 6, at 175. The Third Circuit was evaluating a provision of the COPA that had incorporated a variant of the *Miller* standard.

31. *Id.*

32. *Miller*, 413 U.S. at 24; *see also id.* at 32 ("[I]t is neither realistic nor constitutionally sound to read the First Amendment as requiring that the people of Maine or Mississippi accept public depiction of conduct found tolerable in Las Vegas, or New York City. [People] in different States vary in their tastes and attitudes and this diversity is not to be strangled by the absolutism of imposed uniformity.").

33. *See Reno II*, *supra* note 6, at 175 (quoting ACLU v. Reno, 31 F. Supp. 2d 473, 484 (E.D. Pa. 1999) (alteration in original)).

The Third Circuit found this an impermissible burden on speech and declared explicitly that *Miller* "has no applicability to the Internet."[34]

Given this ruling, Biegel's choice of *Miller* as a model for an online hate speech ban seems somewhat injudicious.[35] However, the question at this point is not whether it would be possible to devise a *Miller* variant that would achieve Biegel's purpose (though that is an interesting problem). The critical issue to consider here is why Biegel rejects the compatibility of *Miller* with the Internet in the obscenity context, while embracing that very compatibility in the context of hate speech. It is admittedly a subtle inconsistency, but its origin may well be the fact that the discussions of obscenity and hate speech are in entirely different sections of the book. Had the two issues been addressed in conjunction, for instance, under a chapter on free speech and the Internet, perhaps the tension would have more clearly manifested itself.

The point here is a simple one, but it merits emphasis. Structure, in and of itself, is not what adds rigor to analysis. On the contrary, to apply structure for its own sake is the very elevation of form over substance, and the result is obfuscation, not enlightenment.

IV. CONCLUSION

Does Biegel successfully answer the question his book title asks? It depends. As a self-described "recent history of the Internet" and a "snapshot in time" (p. 359), *Beyond Our Control?* provides a thorough, insightful, and accessible account of "the extent to which the Internet is currently under control" (p. xiii).

In response to the companion question of "the extent to which [the Internet] . . . should be brought under control" (p. xiii), Biegel only goes so far as to tell us what the answer is not, rejecting both universal regulation and no regulation at all. The questions have thus only multiplied, and this is by design. Biegel's aim is to provoke us to think about these matters deeply, to evaluate objectively the com-

---

34. *See id.* at 180.

35. Biegel appears to agree with the reasoning of the Third Circuit in *Reno II*, drawing general principles from its outcome ("[A]ny legal restrictions [online] . . . that are explicitly geared to a traditional 'contemporary community standards' approach will inevitably run into [a] problem . . . .") (p. 140). But the Third Circuit could, of course, be wrong. Indeed, it is curious to note that the "contemporary community standards" problem never arose in *Reno I*, wherein the Supreme Court majority agreed that the CDA provision prohibiting obscene material online actually survived their ruling, under *Miller*. *Reno I*, *supra* note 6, at 883. In fact, the ACLU conceded this point up front. *See id.* Similarly, the district court considering the COPA challenge stated that, since "plaintiffs are not challenging the provision of COPA that pertains to speech that is obscene," that portion of COPA would remain unaffected. ACLU v. Reno, 31 F. Supp. 2d 473, 479 (E.D. Pa. 1999). It is therefore unclear what the ultimate ramifications are of the Third Circuit's rejection of Miller in the online context.

plexities they raise, and ultimately to imagine solutions to issues that have yet to even fully emerge. Biegel leaves us prepared to tackle these larger questions, and this is the real legacy and lasting contribution of his book.