Michigan Law Review

Volume 101 | Issue 6

2003

Cyberdemons: Regulating a Truly World-Wide Web

Andrew P. Lycans
University of Michigan Law School

NOTICE

Cyberdemons: Regulating a Truly World-Wide Web

*Andrew P. Lycans**

BEYOND OUR CONTROL?: CONFRONTING THE LIMITS OF OUR LEGAL SYSTEM IN THE AGE OF CYBERSPACE. By *Stuart Biegel.* Cambridge: The MIT Press. 2001. Pp. v, 452. Cloth, $34.95.

In the decade leading up to the twenty-first century, the number of Internet-related legal disputes grew exponentially. This growth continues into the new millennium, introducing old problems in a new context. For instance, in the field of copyright, Eric Eldred, the operator of a website dedicated to posting literary works already in the public domain, challenged the Copyright Term Extension Act ("CTEA").[1] The CTEA blocked his plans to post works copyrighted in 1923, works which under the previous statute would have entered the public domain in 1999.[2] Looking to trademark law, the field has become obsessed of late with providing a quick and easy way for trademark holders to regain domain names from cybersquatters without "paying them off."[3] In the First Amendment arena, the Internet continues to present challenges to the concept of a community standard of decency in obscenity jurisprudence.[4] The Ninth Circuit recently pushed the boundaries of jurisdictional law, in an interesting example of the courts keeping pace with the times, when it ruled that plaintiffs could deliver service of process by e-mail when the defendant resides outside the country, if the plaintiff obtains a court

* The author would like to thank Anna-Rose Mathieson and Roberta J. Morris for their helpful comments on an earlier draft.

1. Eldred v. Ashcroft, 123 S.Ct. 769 (2003).

2. Plaintiff's complaint, *Eldred*, 123 S.Ct. 769 (2003), *available at* http://eon.law.harvard.edu/openlaw/eldredvashcroft/cyber/complaint_orig.html. Eldred operates Eldritch press (http://eldritchpress.org) and had anticipated posting such works as *New Hampshire* by Robert Frost, *Horses and Men* by Sherwood Anderson, and *Racundra's First Cruise* by Arthur Ransome, all written in 1923 and scheduled to come off copyright in 1999.

3. *See generally* JANE C. GINSBURG ET AL., TRADEMARK AND UNFAIR COMPETITION LAW 765-829 (2001).

4. *See generally* Ashcroft v. ACLU, 535 U.S. 564 (2002) (discussing at length whether the community-standards test should apply online where distributors neither know nor could know the location of the websurfers accessing the site).

order allowing service of process by e-mail under Federal Rule of Civil Procedure 4(f)(3).[5]

Amid these decisions, Stuart Biegel[6] attempts to craft a model of when and how regulators should go about attempting to bring order to the perceived anarchy of cyberspace. Biegel begins by noting "the commonly accepted notion that no one is in charge" of the Internet (p. 3), then goes on to debunk this notion by listing a number of agencies and groups that attempt to exert some level of control over the Net and "Netizens."[7] He then compares perceptions of Internet regulation to popular notions of the law in the American Old West, demonstrating how both differ significantly from reality.[8]

Before devising a new regulatory model, Biegel asks whether the Internet presents a new entity, something distinct from what came before, and for which no elaborate and extensive bodies of law already exist (pp. 25-26). After a short review of the possibly analogous bodies of law,[9] Biegel concludes that the Internet clearly entails something different, leaving only the question of whether it "merit[s] new and different approaches to regulatory issues" (p. 31). Although Biegel answers this question sometimes yes, sometimes no, he arrives at this conclusion only after a (maybe overly) exhaustive review of previous popular and scholarly works. Given his goal of debunking some popular misconceptions, perhaps this analysis serves Biegel well in coming to a realistic answer about the need to regulate.

The belief that regulating cyberspace presents an all-or-nothing proposition represents the chief misconception Biegel dispels.[10] He emphasizes that regulators may decide to regulate some areas of cyberspace while leaving others alone, and that they may take different approaches when regulating different conduct in cyberspace. These points stand out as Biegel's main contributions in this work (p. 119). Many pioneer Netizens have a libertarian bent and believe that

---

5. *See* Rio Properties, Inc. v. Rio Int'l Interlink, 284 F.3d 1007, 1015 (2002). Fittingly, the underlying dispute involved trademark infringement, specifically the defendant's chosen domain name. *Id.* at 1012-13. Federal Rule of Civil Procedure 4(f)(3) states:

> Service Upon Individuals in a Foreign Country. Unless otherwise provided by federal law, service upon an individual from whom a waiver has not been obtained and filed, other than an infant or incompetent person, may be effected in a place not within any judicial district of the United States . . . by other means not prohibited by international agreement as may be directed by the court.

6. Professor of Education and Information Studies, Professor of Law, UCLA.

7. Pp. 4-12. Occupants of cyberspace frequently refer to themselves as Netizens, an abbreviation based on an abbreviation (Net for Internet and Netizen for Internet Citizen).

8. P. 7. Biegel does this by using the plots of Western movies. *Shane* represents the best metaphor to the Internet in his view. P. 18.

9. He considers if the Internet is analogous to a library, a phone system, a park, a television, or a newspaper. Pp. 26-27.

10. P. 51. Biegel clarifies the all or nothing terminology by saying: "Control or no control. Censorship or no censorship. Rules or no rules." P. 51.

the government should avoid *any* form of cyberspace regulation, though as Biegel points out some of these "libertarians" asked the government to step in to limit what private entities can achieve through the Internet (p. 193). Similarly, regulators may tend to view the Internet as a monolithic entity, and believe comprehensive regulation indispensable to crafting an adequate response to any cyberproblem (pp. 51-54, 119). Biegel maintains regulation in this area could very well prove more effective, and regulators could better avoid unintended consequences, if they considered particular problem areas individually (p. 54).

This Notice argues that, though following the model might help would-be regulators analyze "cyberproblems," Biegel fails to accurately apply the model in the examples he provides. Part I describes Biegel's model for categorizing cyberspace problems and for approaching regulation. Part II argues that Biegel's categories lack comprehensiveness, and that Biegel undermines his model by inaccurately applying it to difficult situations.

I. BIEGEL'S FRAMEWORK FOR ANALYZING CYBERSPACE PROBLEMS AND REGULATION

Biegel establishes a five-step framework for analyzing problematic conduct in cyberspace and for determining how to regulate it. The first step involves placing the behavior into one of four broad categories Biegel provides and then identifying representative characteristics (p. 224). Once a regulator categorizes the problem, the second step forces him to consider the potential for consensus regarding the nature and extent of the problem, and the potential for any regulatory consensus among stakeholders (p. 224). The third step involves considering whether the problem is uniquely cyber, or if an existing regulatory scheme could address it (p. 224). Subsequently, step four requires evaluation of the potential effectiveness of the three regulatory models identified by Biegel.[11] Finally, at step five the regulator must consider the impact of each regulatory model in combination with the others and predict whether any regulation could adequately address the potential problem at this time (p. 225).

In the first step of his framework, Biegel attempts to divide all cyberproblems into four simple categories: 1) Dangerous Conduct, 2) Fraudulent Conduct, 3) Unlawful Anarchic Conduct, and 4) Inappropriate Conduct (p. 54). He defines Dangerous Conduct as "acts and behaviors that may impact physical or national security" (p. 55). Biegel includes threatening behavior such as cyberstalking (p. 55), creating and trafficking in child pornography (p. 57), unli-

11. P. 224. Discussed *infra* notes 13-18 and accompanying text.

censed online healthcare (p. 58), and cyberterrorism (p. 62) under this heading. Fraudulent Conduct encompasses hacking that leads to financial loss (p. 65); traditional fraud in an online setting (p. 70) and deceitful business practices, including noncompliance with posted privacy statements (p. 66); and the undisclosed gathering of information by recording the users Internet protocol address. Unlawful Anarchic Conduct — the least self-defining of the groups — involves conduct "which may... be illegal but may not necessarily be criminal" (p. 73). This would include copyright violations (p. 73), exposing others to pornographic content without adequate warning (p. 80), and online defamation (p. 81). One could fairly describe Inappropriate Conduct as a catchall category for other acts that many people do not like but which nevertheless remain lawful. The author gives the example of hate-related websites as typical of this category (p. 87), as well as overly aggressive business tactics (p. 91), discriminatory "hostile environment" harassment (p. 87), and inappropriate online activity in an education setting (p. 88).

Biegel believes that placing problematic behavior into one of these four categories makes it easier to identify common characteristics the "cyberproblems" share. Though he lists the potential for consensus as a separate step in his analysis (p. 225), in fact Biegel assumes that where the behavior falls in the hierarchy generally reflects the existing level of consensus.[12] Thus, activity which physically harms others such as online child pornography will likely garner a wide consensus condemning the behavior, while socially unacceptable conduct — which Biegel admits will likely engender debate even about what qualifies as unacceptable — will produce little consensus.

The third step, considering whether a problem is uniquely cyber, looks to whether current law can adequately handle the "cyberproblem" without additional regulatory activity (p. 97). The regulator must also ask if the complexity of the issues along with the multiplicity of variables would make any attempt at regulation either ineffective, or the effects unpredictable (p. 107).

Biegel also expends a significant amount of time discussing the three models of regulation he utilizes in step four of his overall approach. He believes these models capable of comprehensively regulating Internet conduct (p. 220). The first regulatory model consists of the traditional method of applying national laws to a problem and developing new laws as necessary (p. 123). The United States can often effectively employ this form of regulation as the "great majority of online users at this point in time are American[s]" (p. 125). Although the U.S. can currently handle many problems through purely national legislation, as the Internet becomes a truly *worldwide* phenomenon,

12. Pp. 223, 235. See *infra* note 41 for a discussion of the likely disagreement about behaviors falling into categories three and four.

this will become an increasingly less effective solution. As an initial matter, however, Biegel points out that this approach may fail in the short term more often than one might think. Frequently, this comes about because attempts to regulate the Internet often run into First Amendment problems, and the courts have struck down some of Congress's most high-profile attempts to regulate in this area.[13] Further, from a logistical standpoint, the sheer volume of online material inhibits effective regulation (p. 140).

The second regulatory model addresses international consensus on how to handle a problem in cyberspace (p. 157). Such consensus has the advantage of simplifying the complexity created by jurisdictional problems and a multitude of individual nations' laws (p. 158). Plus, some problems remain beyond any single nation's ability to resolve. Given the global nature of the Internet, individual nation-states cannot control all Internet behavior that has an effect within their borders.[14] The drawback of international laws, of course, comes from the need to find a consensus position each country will implement faithfully (p. 158). Despite this liability, international rules and procedures already successfully control some online transactions.[15]

The final regulatory approach considers changing the software codes that allow people to act in ways that national governments or the international community have deemed inappropriate (p. 187). Some argue that such "architectural changes" produce "immediate, final, and complete transformation[s]" (p. 188). Regulators cannot, however, ignore the fact that code changes by the "powers that be," as Biegel calls them, inevitably evoke responses by Netizens with the technological know-how to implement their own code countermeasures (p. 208). As Biegel defines the term, however, code-based solutions can also entail efforts undertaken at the individual level.[16] Thus, filtering software employed to protect children and those with delicate sensibilities also qualifies under this category (pp. 200, 204-07).

13. P. 155. One prominent example would be the Communications Decency Act, Pub. L. No. 104-104 5-502, § 110 Stat. 133 (1996). The Court struck down two highly controversial provisions, ostensibly meant to protect children, in *Reno v. ACLU*, 521 U.S. 844 (1997). P. 129. Biegel also discusses the Child Online Protection Act ("COPA"), 47 U.S.C. § 231 (1998), which the district court struck down, with the Third Circuit affirming this decision. Pp. 136-39. The Supreme Court, however, reversed, finding the COPA valid on its face. Ashcroft v. ACLU, 535 U.S. 564 (2002). Biegel also takes this discussion as an opportunity to point out the inappropriateness of individual states within the United States attempting to regulate Internet activity as some have done recently. Pp. 152-54.

14. *See, e.g.*, Mike McPhee, *Items Taken in Ft. Collins Raid Under Study*, DENVER POST, Sept. 5, 1998, at B1 (describing international cooperation in twenty-two countries to orchestrate simultaneous raids against child-pornography ring using encryption technology).

15. P. 176. In some e-commerce situations, Biegel believes that international rules and procedures control. P. 176.

16. P. 205. Biegel provides no explanation why self-help remedies qualify as part of a regulatory model.

The final step in Biegel's model synthesizes the options presented by the three regulatory models, taking into account the particular problem under consideration, to produce a coherent regulatory approach (p. 225). Thus, for something such as child pornography, Biegel's model calls for individual nations to outlaw it and for some international agreement to prevent child exploiters from taking advantage of international borders. Additionally, code-based solutions, such as removing any sites containing child pornography from the root server, also exist.[17]

II. EXAMINING THE ASSUMPTIONS UNDERLYING BIEGEL'S APPLICATION OF THE FRAMEWORK

Although the theoretical framework presented by Biegel may pique academic interest, the real value of the theory should come in its application since he designed it for real-world regulators. Unfortunately, while the framework does present some practical benefits, the model applications presented by Biegel raise problems. The following Part demonstrates that Biegel's model applications fail to faithfully implement the framework he developed. Sections II.A and II.B question the viability of the categorization step as it now stands, and suggest a slight alteration. Section II.C considers Biegel's proposal for dealing with online copying, the issue that "has become for many *the* paradigmatic cyberspace-related inquiry" (p. 74). Finally, Section II.D argues Biegel's decision to reject including private ordering in the model can cause regulators to ignore real solutions.

A. *Inconsistent Categorization: The Nuremberg Files*

Biegel's theory behind the four categories of cyberproblems[18] implies that the lower the number in his hierarchy, the easier it should be to establish a consensus on the need for action (p. 235). Thus, one can easily see why threats delivered over the Internet and child pornography would fall into the Dangerous Conduct category. Oddly though, Biegel also includes the facts of *Planned Parenthood of the Columbia/Williamette v. American Coalition of Life Activists*[19] as something that falls into the Dangerous Conduct category (p. 56). There an anti-abortion group, the American Coalition of Life

17. P. 274. Thirteen root servers containing "authoritative lists of domain names and their corresponding IP numbers" make up the root server system. Root Server A is the main computer holding the address database. P. 194. The Eastern District of Virginia has already directed a website off the Internet by suspending a defendant's domain name registration. P. 274.

18. 1) Dangerous Conduct 2) Fraudulent Conduct 3) Unlawful Anarchic Conduct, and 4) Inappropriate Conduct. P. 55.

19. 244 F.3d 1007 (9th Cir. 2001).

Activists ("ACLA") maintained detailed dossiers it called the Nuremberg Files so that "Nuremberg-like war crimes trials could be conducted in 'perfectly legal courts once the tide of the nation's opinion turns against the wanton slaughter of God's children.' "[20] The ACLA shared these dossiers with Neal Horsley, including the abortion doctors' names and current addresses, which Horsley posted on his website.[21] Whenever someone killed an abortion provider, Horsley would cross off the doctor's name on the posted list.[22]

Biegel's categorization of the Nuremberg Files website in *American Coalition* creates internal inconsistencies in his categories for two reasons. First, while the district court did find for the plaintiff doctors, the Ninth Circuit overturned this decision "applying basic First Amendment principles" — to quote Biegel (p. 56). Though Biegel notes the controversy this caused, the fact that this case raised so much controversy indicates that Biegel may have miscategorized the activity under his own model.[23] The authorities can clearly proscribe the other activities he uses as examples for this category, as the public overwhelmingly supports such limits. Under current law, however, Horsley can operate his website without state interference. Thus, no strong consensus emerges that the law must do something about this site — since many would agree the First Amendment bars the state from doing anything.

The second problem follows from the fact that this site seems to fit squarely within the category of Inappropriate Conduct. When giving a sample application of the model within the Inappropriate Conduct category, Biegel goes through a long analysis on how the government could ban hate-related websites if First Amendment law changes (pp. 321-52). This chapter seems to describe exactly the kind of website at issue in *American Coalition*. Biegel might argue he could differentiate the two sites because Horsley's site referred to specific people, thus perhaps seeming more like a threat, while a generic racially based hate-related website might not mention specific people — though many likely do. Since the sites simply promote different kinds of hate, however, the same category should apply. In the end, it seems that the *American Coalition* site fits better in the Inappropriate Conduct category — many believe the site operator should not have posted the Nuremberg Files, some would deny the site First Amendment protection, but the majority of Americans believe it protected (p. 348). This

20. *Id.* at 1012-13.

21. *Id.* at 1013.

22. *Id.* He grayed out the names of the wounded. *Id.* The plaintiffs, however, did not sue Horsley. *Id.* at n1.

23. "For the problems in categories 1 and 2, consensus is not typically an issue, since the categories were organized in part by the likelihood that some degree of consensus could be reached in advance." P. 235.

fits with the low consensus Biegel envisions for Inappropriate Conduct (p. 326).

Yet no problem should fit within both the Dangerous Conduct category and the Inappropriate Conduct category as Biegel envisions them. Biegel claims that his "categories are designed to be both flexible and fluid, with certain types of generic behavior fitting under more than one category depending on specific factors that might be present . . . ." (p. 54). He then goes on, however, to define Inappropriate Conduct as "immoral or offensive acts that *do not fit under any of the other" categories.*[24] This statement just reinforces the idea that this category is a catchall, including only activities that the regulator could not place elsewhere. Of course, the problem could result from Biegel putting hate-related websites in the wrong category. One could imagine an argument that hate-related websites threaten the targeted groups physical security. Given Biegel's desperate attempts to craft a legal framework allowing the abolition of such sites (pp. 321-52), however, if he believed they qualified for the Dangerous Conduct label, he would likely have put them there.

The real problem may be the genesis of Biegel's categories. Although Biegel presents them as coming from whole cloth, they roughly correspond with: 1) criminal conduct presenting the potential for physical harm (Dangerous Conduct), 2) criminal conduct leading only to nonphysical harm (Fraudulent Conduct), 3) noncriminal conduct leading to civil liability (Unlawful Anarchic Conduct), and 4) noncriminal conduct not resulting in civil liability (Inappropriate Conduct).[25] This method of considering Biegel's model explains why he would resist putting hate-related websites in the Dangerous Conduct category — the site operators have done nothing criminal. It also explains why going from category one to four roughly tracks consensus as to the need to do something about the behavior (p. 223). As a society, we have already made these decisions.[26] Comparing the underlying categories with Biegel's categories clearly demonstrates the

24. P. 85 (emphasis added). Oddly enough, he also defines Unlawful Anarchic Conduct as mutually exclusive of the other categories. He says such behavior presents no danger to physical safety or national security, thus it cannot be Dangerous Conduct. Additionally, the fact that the behavior does not generally qualify as fraudulent or dishonest serves as a "distinguishing feature," thereby falling outside Fraudulent Conduct (the lack of fraud and dishonesty can hardly serve to distinguish category three from category two if the two categories are not mutually exclusive — and this holds true whether Biegel qualifies his statement with "generally" or not). P. 73.

25. The two categorization systems do not completely correspond. Some actions Biegel includes in Dangerous Conduct constitute crimes not resulting in physical harm for instance. But, as discussed in Section II.B *infra*, these categorizations put strain on Biegel's model.

26. Of course Biegel might argue that the political system did not adequately consider the views of all stakeholders in making the decision. This, however, criticizes our political system in general, and Biegel does not propose a more effective way of canvassing and measuring stakeholders' views.

under inclusivity of Biegel's, despite his statement that this approach "divide[s] . . . problem areas into four categories."[27] Proper categorization of the behavior comes in step one, upon which the others rely.

B. *Miscategorization: Cyberterrorism*

Even more problematic are Biegel's attempts to fit cyberterrorism within the Dangerous Conduct category. Starting from a clean slate, Biegel defines the Dangerous Conduct category as "composed of acts or behaviors that may impact physical or national security" (p. 55). Biegel uses the denial-of-service attacks of February 2000[28] as an example of the cyberterrorism that the Dangerous Conduct category would cover (pp. 229-31). He employs two gambits to include these attacks in this category. The first posits that blocking major websites, used by so many people, presents a threat to national security (p. 233). He supports this by saying that the United States government viewed such behaviors in terms of national security, seemingly oblivious to the fact that the government now appears to view everything in terms of national security.[29] Biegel's most convincing argument in this regard turns on the fact that other attacks similar in nature would in fact threaten national security.[30]

Biegel's second attempt to fit such acts into the Dangerous Conduct heading relies on the argument that denial-of-service attacks use intentional force directed at particular targets and result in injury (p. 235). In developing this argument, Biegel advocates using a very broad definition of "violent" in the online setting, which encompasses vehement or passionate speech and extreme or intense force caused

---

27. P. 54. Biegel claims that by placing a problem in one of these categories, a regulator can identify representative characteristics of the problem, and thus can better conduct the following analysis. Although it might be helpful, i.e. to take into account what has or has not worked on other problems in the category, it does not appear essential to the analysis. As such, the regulator can apply the remainder of the model without this first step.

28. These attacks involved the perpetrators planting software on nonsecure computers owned by third parties. Then, when the time came for an attack, the "cyberterrorists" marshaled these computers to send an extreme volume of requests to the targeted websites, with the intent of denying others access to the sites. The websites targeted included Yahoo, Amazon.com, eBay, CNN, eTrade, ZDNet, and Datek. Pp. 229-30.

29. P. 233. For examples of the growth of the national-security argument's influence see, for examples, Robert Schlesinger, *Citing Oil Need, Bush Pushes Energy Bill Senate Seeks Block on Arctic Drilling*, BOSTON GLOBE, Oct. 12, 2001, at A6 (discussing national security interest in oil as a reason for drilling in wildlife preserves), and T. Shawn Taylor, *In the Name of Homeland Security*, CHI. TRIB., Mar. 9, 2003, § 5, at 5 (discussing governmental use of national security concerns to fight federal-employee unions and worries about sexual harassment claims). In fairness to Biegel, he completed this book before September 11th. Merely parroting the government line about this being a national security issue, however, does not prove anything.

30. P. 234. Cyberterrorists previously attempted to disable communication systems. P. 234.

by unexpected or unnatural sources.[31] This allows him to place cyberterrorism in a category in which it does not belong.

When reading this portion of the book, many will find the similarities to the civil-rights sit-ins in the South striking.[32] There the protesters caused a denial of service by taking up places at lunch counters and other public accommodations that would not serve them. By sheer numbers, they could effectively disrupt service by taking up all the available space until the proprietors relented. The resulting racial strife certainly had greater national security implications than not being able to access Yahoo for three hours.[33] What the "cyberterrorists" do mirrors the civil rights protests, only in an online setting.[34] In fact, Biegel himself describes the Electronic Disturbance Theater's ("EDT") attempted denial-of-service attack on the Pentagon's website as an act of cyber civil disobedience.[35] EDT calls its actions a virtual sit-in.[36] Various groups have used electronic civil disobedience to protest war, the treatment of minorities, and even terrorism itself.[37] The only difference between the nonviolent civil rights protests of the 1960s and these cyber protests originates from Biegel's decision to define violence as including directing your cyber presence toward a particular location as an act of force.[38] While civil disobedience does often result in arrest in the real world, Biegel states that cyberterrorism — which in his view includes cyber sit-ins — "should arguably

31. Pp. 231-32. This argument assumes something cyberterrorists do in directing their attack qualifies as force.

32. An obvious difference between the two exists of course. Civil rights protesters risked beatings and arrest to make their point while many "cyberterrorists" want to remain anonymous. Additionally, some cyberterrorists utilize the property of innocent third parties without their consent. P. 229. This is not true, however, of EDT. EDT protesters use Floodnet, a Java applet, that automatically reloads the targeted webpage every three seconds, but they do not use third-party property. Jeanne Carstensen, *Hey Ho, We Won't Go: Civil Disobedience Comes to the Web*, *available at* http://amsterdam.nettime.org/Lists-Archives/nettime-l-9806/msg00012.html (last visited May 2, 2003).

33. *See* MARY DUDZIAK, COLD WAR CIVIL RIGHTS: RACE AND THE IMAGE OF AMERICAN DEMOCRACY (2000) (suggesting the civil rights movement created a national security issue for America in the fight against communism).

34. Biegel uses the loaded term "cyberterrorists" very liberally. Those who practice electronic civil disobedience claim their activism follows in the footsteps of Henry David Thoreau and Gandhi. *See* Stefan Wray, *On Electronic Civil Disobedience* (1998), *available at* http://www.thing.net/~rdom/ecd/oecd.html. Clearly they do not view themselves as terrorists anymore than the civil rights protesters of the 1960s considered themselves to be terrorists.

35. P. 241. The Pentagon responded with a counteroffensive, flooding the browsers launching the attack with graphics and messages, causing them to crash. P. 241.

36. *See* Paul Van Slambrouck, *Newest Tool for Social Protest: The Internet*, CHRISTIAN SCI. MONITOR, June 18, 1999, USA 3.

37. *See* John Lasker, *Hactivists Wage War*, BUFF. NEWS, May 14, 2002, at E1.

38. Biegel would declare the equivalent of walking in the door of the diner and sitting down to be an act of force.

have the same level of punishment . . . [as] offline penalties for terrorism."[39]

It seems quite odd that Biegel himself would have to strain to fit anything into the different categories. After all, he created them only a few pages earlier, and one would think he could have finessed the categories rather than warping the definitions of the conduct involved to obtain the desired result. This may flow from the fact that the stakeholders would likely agree that the government should do something about such attacks[40] — meaning in Biegel's framework the behavior should fit into category one or two[41] — but the actual acts committed do not nicely fit into either Dangerous Conduct or Fraudulent Conduct without manipulation. The fact that this behavior does not seem to fit well within the framework prescribed leads to additional questions about the comprehensiveness of the categories. Perhaps more categories would solve the problem — but of course with additional categories the attractive simplicity of the system declines.

C. *Ignoring the Model: Giving in to the Copyright Anarchists*

In marked contrast to his recommendations concerning denial-of-service attacks, where Biegel would treat cyber activists in the same way as real-world terrorists, he professes his willingness to abandon the current copyright regime as being unrealistic in the online world. Since copyright infringement constitutes one of the most contentious Internet-related problems (p. 280), Biegel does not feel the need to fit copyright violators into the Dangerous Conduct category — despite his argument that extreme economic harm can have national security implications.[42] Here the fact that many online users are violating the current copyright provisions on an almost daily basis persuades him of the wisdom of this action.[43] He proposes to scrap the current copyright

39. P. 239. This does not mean cyber activists should not be punished for the crimes they commit. It merely aims to make clear the extent of the punishment Biegel proposes, and the activities to which he would attach those punishments. The situation requires a more nuanced approach than Biegel advocates.

40. P. 235. For discussion of the role of consensus in Biegel's model, see *supra* notes 12, 23-24 and accompanying text, and *infra* notes 41, 43 and accompanying text.

41. Biegel contends that someone applying his method can place all problematic behavior into one of his categories. He then specifically notes that low consensus will typify category four and sets up category three in terms of large numbers of people on both sides of the debate. He expects high consensus in categories one and two. P. 235.

42. P. 281. The sale of copyrighted materials accounts for six percent of the United States' gross national product. Laurie A. Santelli, *New Battles Between Freelance Authors and Publishers in the Aftermath of* Tasini v. New York Times, 7 J.L. & POL'Y 253, 269 (1998).

43. P. 280. Biegel never clarifies why radical proposals to change the substantive law enter into the analysis. His model does allow for changes in the law in steps three through five when the stakeholders come to agreement. This proposal does not result from an appli-

provisions in exchange for a simpler system that online users will understand.[44]

His analysis raises several potential problems. Biegel claims an emerging pattern in the case law allows for private personal copying under the fair-use defense.[45] Yet for all of Biegel's attention to the fair-use doctrine in relation to private personal copying, he ignores

---

cation of this process. Biegel makes much of the fact that stakeholders cannot come to agreement in this field. In apparent response to this, Biegel makes a proposal that does not resolve this inability to agree (one side will certainly reject it and the other might or might not support it). Simply because Biegel believes his proposal well-reasoned and fair does not mean the stakeholders will agree to it, but Biegel makes no effort to deal with this lack of consensus.

44. P. 303. The belief that simplicity holds the key to copyright compliance undergirds Biegel's proposed reforms. P. 303. This is a fundamentally flawed vision of the law. Biegel argues that since no lay person could understand this area of the law, society cannot expect Netizens to follow copyright law. Biegel's argument here rests on an unacknowledged — and highly dubious — assumption. Namely, Biegel assumes that Netizens know about the fair-use doctrine, want to comply with it, but simply cannot figure out how to do so. P. 303. He seems to envision Netizens combing through Westlaw searching futilely for clear conduct rules. Many areas of the law that society expects people to obey, however, display a similar complexity. For instance, when discussing the countermeasures various entities have taken against cyberterrorism, Biegel provides an extensive analysis of when the occupant of a building may inflict physical injury in defense of habitation. Pp. 242-44. The answer entails a complex analysis that turns on a number of variables. Pp. 242-44. Yet we expect people to conform their behavior to this standard despite the fact that they most likely have no clue that it exists.

In fact, Meir Dan-Cohen maintains that overbreadth and vagueness, the antithesis of clear conduct rules, can become virtues in some areas of the law such as necessity and duress. *See, e.g.*, Meir Dan-Cohen, *Decision Rules and Conduct Rules: On Acoustic Separation in Criminal Law*, 97 HARV. L. REV. 625, 639 (1984). In such situations, society benefits when conduct rules (directed at the general populace) and decision rules (directed at those imposing punishment for crimes) differ so as to preserve the deterrence effect of the law. *Id.* The two need not fully overlap. *Id.* at 649. Dan-Cohen goes on to suggest that overbroad and vague laws that exhibit simplicity, when combined with fair decisional rules, can result in good law. *Id.* at 639. This, however, would not satisfy Biegel, or the purpose of the fair-use doctrine. Dan-Cohen's method covers more than society intends to punish to provide adequate deterrence. Fair use does not seek to over deter, but encourages uses that qualify as fair.

Complexity often results from an attempt to introduce fairness into the law because society expects conduct rules and decision rules to fully overlap. For instance, "thou shal[t] not kill," *Exodus* 20:13 (King James), is a simple law, but many would prefer the current criminal law, which allows for killing in self-defense, even if the law allows only a narrow and technical exception. The simplicity rationale is further undercut by the fact that people do not always obey simple laws despite the fact that they can determine compliance with little effort — the speed limit representing an excellent example. *See* Margaret Raymond, *Penumbral Crimes*, 39 AM. CRIM. L. REV. 1395, 1397-99 (stating most Americans speed and estimating the percentage at somewhere between sixty-seven and ninety).

45. P. 305. The fair-use defense resulted from judicial activism, a decision that fulfilling the purpose of the Copyright Act necessitated an exception to copyright owners' rights. *See* Joseph P. Liu, *Copyright and Time: A Proposal*, 101 MICH. L. REV. 409, 453 (2002). Eventually, Congress codified the fair-use defense, requiring the courts to look at four factors: 1) the purpose and character of the use, 2) the nature of the copyrighted work, 3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole, and 4) the effect of the use upon the potential market for or value of the copyrighted work. 17 U.S.C. § 107 (2003). Congress also left the courts free to consider additional factors that they may find relevant. *See* H.R. Rep. No. 94-1476, at 66 (1976).

one of the major theories in the field — that fair use constitutes a form of market failure.[46] In the past, high transaction costs made low-value transactions unprofitable.[47] The Internet actually presented a possible way to reduce these transaction costs and thus would diminish the need to employ the fair-use doctrine.[48]

Further, Biegel's de minimis proposal,[49] which would allow people to download set portions of larger works and small works in their entirety — for private noncommercial use only — then forward them on to a limited number of people (p. 306), advances a much more radical theory than he admits. He does, in fact, acknowledge that Congress would have to amend the Copyright Act to implement his proposal (p. 306), but still attempts to justify it using fair-use concerns. Thus, in evaluating Biegel's suggested amendment, the four fair-use factors prove useful.[50]

Biegel, without mentioning them specifically, seeks to justify his proposal on two of the fair-use grounds. He, in essence, wants to collapse the third factor, the amount and substantiality of the portion used in relation to the work as a whole, into a *per se* rule, allowing "downloading . . . documents of less than ten pages . . ." and limited numbers of music files — presumably meaning entire songs.[51] Here,

---

46. *See* Wendy J. Gordon, *Fair Use As Market Failure: A Structural and Economic Analysis of the* Betamax *Case and Its Predecessors*, 82 COLUM. L. REV. 1600, 1614-15 (1982). Gordon points out in a later piece, however, that just because no market failure remains does not automatically mean fair use should not apply. *See* Wendy J. Gordon, *Market Failure and Intellectual Property: A Response to Professor Lunney*, 82 B.U. L. REV. 1031, 1031-32 (2002). The law and economics articles which cite to Gordon largely disagree, or at least fail to acknowledge this point.

47. *See* Abraham Bell & Gideon Parchomovsky, *Pliability Rules*, 101 MICH. L. REV. 1, 51 (2002).

48. The founding of the Copyright Clearance Center in 1977 presented another option — and a reason for cutting back on the fair-use defense in certain instances. *See* American Geophysical Union v. Texaco Inc., 60 F.3d 913, 929 (2d Cir. 1994). The major problem to date on the Internet revolves around an economical way to charge for these low-value transactions.

49. One must realize that Biegel adopts an unnecessarily confusing name for his proposal. As he notes, copyright law already has a de minimis allowance, much more limited than what he suggests. The de minimis doctrine allows for "trivial instances of copying," On Davis v. Gap, Inc., 246 F.3d 152, 173 (2d Cir. 2001), because trivial copying is not an infringement.

50. He explicitly notes that the third fair-use factor addresses traditional de minimis issues. P. 306.

51. P. 307. One can see where Biegel's desire for a simple law begins to betray him here. If he sticks to the simple rule, it leads to anomalous results. If someone wishes to download a work with only one line on the eleventh page would his proposal bar this? If it does not, Biegel finds himself back in the case-by-case line drawing business, which he designed his simple rule to avoid. If it does, this raises another worry. Namely, inflexible laws often lead to nonsensical results. Biegel does not explain why the public should prefer a simple law that leads to nonsensical results over a hard-to-interpret, complex rule striving for sensible outcomes. One also wonders if Congress must provide a standard font, type size, and margins to guarantee compliance with this "simple" rule. Plus, Biegel's proposal seems incomplete.

Biegel commits the cardinal sin of conflating de minimis with small. Neither society nor copyright law judges a work by its length, and this proposal would alter the third factor to consider only the amount taken. As the Supreme Court noted in *Harper & Row v. National Enterprises*,[52] however, the heart of a work can reside in a small percentage of the larger work, creating a need to consider substantiality.[53] While Biegel would prevent people from taking books and long articles in their entirety, he ignores the fact that the value of many works lies only in a small portion of a work.[54] No doubt Biegel does not address the concerns raised by the fourth fair-use factor, the effect his proposal would have upon the potential market for, or value of, the copyrighted work, for just this reason. Allowing everyone to download the work for personal use would destroy the market for many copyrighted works. Simply put, people use whole genres of copyrighted works only — or predominantly — for private personal and noncommercial purposes. Indeed, Biegel's proposal may present a takings issue. His amendment to the Copyright Act would take small works from their owners and put them in the public domain because no work under ten pages would receive protection in noncommercial settings and online users could download the most valuable parts of other works (p. 307). Biegel attempts to counter this by insisting that the purpose and nature of the use be noncommercial (p. 306) — the first fair-use factor. He fails to acknowledge, however, that the first factor is not the entire test because even noncommercial private uses can destroy the value of some works.[55]

As for the second factor, the nature of the copyrighted work, Biegel apparently finds this unimportant, though he concerns himself mainly with works at the core of copyright law. Thus, Biegel plucks out the concerns underlying two of the fair-use factors while failing to comprehend why Congress — taking its cue from the courts — included the other two factors in the test.[56] The term de minimis comes from the longer Latin phrase *de minimis non curat lex*, which Biegel

---

Much online infringement involves visual works, which the proposal fails to address. In fact, to meet Biegel's goal would require more of a civil law code than a short, simple law.

52. 471 U.S. 539 (1985).

53. *Id.* at 564-66, 579 (finding that taking three-hundred words from a 200,000-word book to be substantial).

54. President Ford's autobiography, at issue in *Harper & Row*, provides a good example. Everyone generally agrees that his reasons for pardoning President Nixon — contained in a small portion of the overall book — provided the material of most interest to a vast majority of the potential audience. *See id.* at 565, 568.

55. Plus, it focuses on the noncommercial purpose of the use ignoring completely the nontransformative character of the use. *See* Kelly v. Arriba Software Corp., 280 F.3d 934, 940-42 (9th Cir. 2001) (discussing the importance of transformative character).

56. Indeed, his proposal only takes half of the concerns behind each factor he does consider into account.

loosely translates as "the law does not take notice of, or concern itself, with very small or trifling matters" (p. 306). The complete destruction of a work's value hardly qualifies as trifling. For just this reason, de minimis, as the courts now use the term, refers only to truly trivial uses.[57]

Biegel also attempts to use the *Sony Corporation of America v. Universal City Studios Inc.*[58] case to support a growing trend towards allowing private personal copying; however, this rings hollow (p. 299). In *Sony*, Universal Studios and Disney brought suit against Sony because of Sony's production of the Betamax.[59] The Betamax functioned like a VCR,[60] enabling the user to time shift "to record a program he cannot view as it is being televised and then watch it once at a later time."[61] Content producers feared this would lead to people watching less television and attending fewer movies.[62] The holding of the *Sony* decision allowed private personal copying in the context of free, over-the-air broadcast as a fair use.[63] In part, this flowed from the Court's belief that the time-shifting would actually produce more profit than televised shows and movies alone.[64]

This argument overlooks several key differences, however, between *Sony* and Biegel's favorite topic, songs downloaded and stored in the MP3 format. Justice Stevens — presciently according to Biegel — predicted that revenues would actually increase due to time-shifting — and they have (p. 309). Downloading songs off the Internet is not, however, time-shifting — it does not record broadcast music as presented free over the air by its creators for one time use later.[65] The Court only authorized time-shifting, and downplayed the likelihood people would try to build videotape libraries rather than watching the content once and recording over the program.[66] Biegel notes the Court avoided deciding if building personal libraries of copyrighted works without payment constitutes a fair use (p. 299). MP3s, however, squarely present the issue because people do try to put together music

57. On Davis v. Gap, Inc., 246 F.3d 152, 173 (2d Cir. 2001).

58. 464 U.S. 417 (1984).

59. *Id.* at 420.

60. *Id.* at 422.

61. *Id.* at 421.

62. *Id.* at 452-53.

63. *Id.* at 425.

64. P. 300 (referring to *Sony*, 464 U.S. at 443, 446-47, 452-53). Given the current prerecorded videotape and DVD market, this prediction proved true.

65. The Court expressly declined to address the transfer of private copyrighted material among individuals that Biegel advocates in his de minimis proposal. *Sony*, 464 U.S. at 425.

66. *Id.* at 421, 424 n.3, 451.

libraries on their computers by downloading songs off the Internet.[67] While increasing the number of people who see television shows does benefit the content producers in terms of advertising rates, increased audience without a corresponding increase in record sales provides little benefit.[68]

Attempting to counter this observation, Biegel writes "[f]rom the time that audiotaping technology first developed, industry officials have raised the specter of alleged lost profits . . . [y]et the record companies continue to make large sums of money, and music industry profitability overall has shown no concrete signs of abating" (p. 308). While this might have seemed true at the beginning of 2001, it is no longer so.[69] The profitability of the music industry dropped dramatically over the last several years, and industry executives blame this in large part on the practices that Biegel wants to hold harmless.[70] Biegel suggests that the music industry should find a way to profit from this downloading — but tellingly does not offer any suggestions as to how to do so (pp. 300-01, 309).

---

67. *See* Hiawatha Bray, *Recording Industry Shows Some Cunning*, ST. PETERSBURG TIMES, Jan. 27, 2003, at C4 (discussing use of the Internet to build music collections); *Wherehouse Music Retailer Seeks Bankruptcy Protection*, HOUSTON CHRON., Jan. 22, 2003, at 10B (same).

68. *See* Jane C. Ginsburg, *How Copyright Got a Bad Name for Itself*, 26 COLUM. J.L. & ARTS 61, 64 (2002) ("[T]he cumulative . . . impact of private copies, particularly if the copying becomes widespread and systematic, may be quite deleterious and should be prevented"). Concert attendance generally does not provide a benefit to the record studio that produces an album. *See* Adam Sherwin, *Rock Artists Sign Up to Live Bootleg CDs*, THE TIMES (LONDON), Feb. 17, 2003, at Home News 5 (reporting the first contract with a leading artist, Robbie Williams, where the studio will get a cut of the gate). Traditionally, concert tours were meant to promote record sales, but this has changed for some of the most high profile acts. *See* Rodney Ho, *The Long Goodbye: On Her Latest 'Farewell' Tour, Singer Cher Illustrates How Hard It Can Be for Those in the Limelight to Leave It for Good*, ALA. J. & CONST., Apr. 25, 2003, at 1E (discussing how some acts now make more off of ticket sales than album sales). This does not solve the problem for less well-known acts that cannot charge exorbitant prices for tickets. Nor do groups who can charge such prices need the additional exposure, and fans willing to spend so much for tickets would likely have bought the album if they could not download it for free.

69. Jeff Leeds, *After a Rocky Year, Time to Face the Music*, L.A. TIMES, Dec. 29, 2002, at C1. Biegel does say "concrete signs," thereby indicating that the downward trend was already apparent then. P. 308. Biegel also claims the music industry cannot base loss estimates on the number of MP3 files downloaded because such activity differs from CD piracy. P. 309. As Biegel himself continually points out elsewhere, however, effective does not mean perfect. With an adequate statistical analysis the industry can establish roughly how much loss MP3 downloading produces — though no doubt what they release publicly may skew towards the high end of an honest analysis. His baseline reliance on CD piracy also fails — all those willing to pay the price a pirate charges may not be willing to pay the authorized price, but we do not say that the industry can establish no estimate of the loss in this situation. Additionally, Biegel says, somewhat misleadingly, that "sampling" a song by downloading it could lead to album sales — but conveniently ignores the fact that it could also rob "one-hit wonders" of any significant revenue. P. 309.

70. Patrick MacDonald, *Music-Industry Meltdown*, SEATTLE TIMES, Feb. 23, 2003, at K1. Others blame it on the low quality of the product, *id.*, but this does not explain the vast numbers of people downloading the recordings now.

Biegel also seems to have an unrealistic view of the fair-use defense overall. He refers to the rights of online users in the context of fair use (p. 295), but fair use is a shield, not a sword.[71] Infringers can protect themselves from liability in an infringement action if they qualify for the defense, but cannot force the intellectual property holder to grant them access to the material. The Copyright Act only grants copyright owners rights. Additionally, his proposal does not actually provide a solution. His proposal will exist along side current fair-use law (pp. 306-07), displacing only a portion of it, thus undercutting his simplicity rationale.

At a more fundamental level, one can disagree with Biegel on the extent of Netizens' disdain for the copyright law as it now stands. Biegel states that "Netizens [have] demonstrat[ed] a disrespect for the [copyright] law that has arguably not been seen since the days of prohibition."[72] Although the prevailing social norms in cyberspace do reflect a belief that copyright laws somehow do not apply there (pp. 74-76), this does not mean that society should abandon copyright law on the web as it now stands because of these social norms.[73] In the past, appeals by the creators of intellectual property have proven successful at persuading people to respect the originators enough to not steal their work.[74] Plus, apparent disdain for copyright law might not run so deep as one might suppose on the Internet.[75]

---

71. *See, e.g.*, Robert A. Kreiss, *Accessibility and Commercialization in Copyright Theory*, 43 UCLA L. REV. 1, 47 (1995). The name itself indicates a defense, not an affirmative right.

72. P. 290. This analogy enthralls Biegel, and he uses it repeatedly in regard to the social contract breaking down in regard to copyright. The analogy, however, is weak. Prohibition created criminal laws, while copyright involves mainly civil violations. Ignoring criminal laws indicates a greater breakdown in the social contract. *See* Raymond, *supra* note 44, at 1424 (discussing how rarely enforced criminal laws, which do not induce social opprobrium and shame for violation, undercut the criminal law). In discussing the importance of the social contract, Biegel fails to distinguish between civil and criminal liability. People can incur civil liability without believing the law that forces payment illegitimate. One need look no further than efficient breach of contract to confirm this. *See* Richard A. Posner, *The Strangest Attack Yet on Law and Economics*, 20 HOFSTRA L. REV. 933, 935-37 (1992).

73. In the context of First Amendment social norms, Biegel advocates fighting these norms, p. 326, even after acknowledging that change might prove impossible.

74. This observation finds support in Jane Ginsburg's latest work. *See* Ginsburg, *supra* note 68. Ginsburg believes "[c]opyright owners [are] generally perceived to be large, impersonal and unlovable corporations (the human creators . . . tend to vanish from the polemic view)." *Id.* at 61-62. Ginsburg specifically criticizes the view that any law "that gets in the way of what people can do with their own equipment in their own homes" is an illegitimate law, and labels this consumer greed. *Id.*

This view also finds support in J.R.R. Tolkien's experience with American copyright law. In 1965, Ace Books published an unauthorized edition of each book in *The Lord of the Rings* trilogy on the belief that the American copyright was no longer valid. William A. Davis, *Hobbit Forming*, BOSTON GLOBE, Dec. 29, 1991 (Magazine), at 13. J.R.R. Tolkien, in response, included the following on the back cover of each authorized book in the trilogy published for the American market: "A STATEMENT FROM THE AUTHOR ABOUT THIS AMERICAN EDITION: 'This paperback edition, and no other, has been published with my consent and co-operation. Those who approve of courtesy (at least) to living authors will

More importantly for Biegel's proposal, he seems to ignore the fact that several of the regulatory models he uses in step four, namely code solutions and traditional national law, could implement current law (pp. 290-91). If problems in earlier steps counsel regulators to ignore real solutions, then the proposal is of little use. For instance, a national law based solution to the seemingly intractable problem of Netizens refusing to pay sales tax on Internet purchases indicates regulators might continue working with national law solutions to good effect without radical changes.[76] As for traditional national law in the copy-

---

purchase it, and no other.' " J.R.R. TOLKIEN, THE FELLOWSHIP OF THE RING back cover (Ballatine Books 1972) (1965); J.R.R. TOLKIEN, THE TWO TOWERS back cover (Ballatine Books 1972) (1965); J.R.R. TOLKIEN, THE RETURN OF THE KING back cover (Ballatine Books 1972) (1965). Later, in 1992, a district court held that distributing a large number of foreign published copies of the work without copyright notice — a violation of § 9 of the 1909 copyright act — does not cause invalidation. Eisen, Durwood & Co., Inc. v. Tolkien, 794 F. Supp. 85 (S.D.N.Y. 1992). As far as Ace was concerned, however, this ruling was irrelevant. Even though the publishing houses believed Tolkien had no copyright protection in America, his tactic was so effective that Ace discontinued further publications and paid Tolkien royalties. It claimed it had not paid the royalties earlier because it did not have Tolkien's address. Ace's own authors then simultaneously mailed their publisher the address in a campaign coordinated by Ballatine, Tolkien's American publisher. Philip Marchand, *Ballatine and Tolkien Made Sci-Fi Go Sky High*, TORONTO STAR, May 9, 1991, at E8. The cover statement became so famous that when Signet Books published a parody of *The Lord of the Rings*, the authors included a parody of the statement as well. *See* HENRY N. BEARD & DOUGLAS C. KENNEDY, BORED OF THE RINGS back cover (Signet Books 1969) ("A STATEMENT FROM THE AUTHORS OF THIS *LAMPOON* EDITION: This paperback edition, and no other, has been published for the purpose of making a few fast bucks. Those who approve of courtesy to a certain other living author will not touch this gobbler with a ten-foot battle-lance.") The music industry recently began a similar campaign with some of its biggest stars. *See* MacDonald, *supra* note 70.

75. On a recent visit to a discussion board, someone posted "caps" — an abbreviation of "screen captures," frozen stills taken from moving pictures — from a television show. Another board visitor immediately responded that he had originally produced those caps and posted them on a different discussion board and the second poster should not have reposted them. This led to a lively discussion with the general consensus being that the proper "netiquette" was for the original capper to "sign" his work so he could receive credit for it, but that once he posted it others could repost it. This suggests a respect for the author of a work, albeit one that differs substantially from what copyright law would prescribe — both posters were clearly violating copyright law. Posting copyrighted material on the Internet infringes on the copyright holder's 17 U.S.C. 1(g) § 106(5) right of public display. *See* Kelly v. Arriba Software Corp., 280 F.3d 934, 944-45 (9th Cir. 2001); Video Pipeline, Inc. v. Buena Vista Home Entm't, Inc., 192 F. Supp. 2d 321, 332 (D.N.J. 2002). It also violates the exclusive right of reproduction. *See Kelly*, 280 F.3d at 940. Intellectual property holders might conceivably direct such attributive impulses into a greater respect for existing copyright law or some reasonable variant.

76. *See* David Colker, *Will Smoke Cloud States' Tax Vision?*, L.A. TIMES, Mar. 1, 2003, at C1. Netizens have ignored this tax just as they have ignored copyright law, yet a solution appears on the horizon and the states did not have to scrap their sales-tax laws to do it. The reader should also note that this law gained no more respect or compliance among Netizens due to its simplicity. This, despite the increasing difficulty of claiming ignorance of the law — the telephonic tax filing system employed by many states insists on explaining the tax and making the taxpayers swear under penalty of perjury that they have paid all applicable taxes. Yet the feeling remains widespread among Netizens that only suckers pay this tax. Admittedly, the states must make small adjustments to reconcile certain aspects of their tax codes but this is just the sort of "national law" solution Biegel expects.

right arena, several options remain untried, at least in regard to certain areas. In regard to MP3s, for example, an Audio Home Recording Act approach, which would force the collection and payment of royalties by MP3 manufacturers to copyright holders, might prove effective,[77] as might other smaller adjustments of the current law, without a wholesale overhaul. With respect to code-based solutions, in the very chapter dealing with copyright infringement, Biegel himself notes a possible solution — the Clever Content Server, which allows people to view an image but disallows screen captures and disables the "save as" feature on the browser (p. 319). Biegel describes this product as leading to a "potentially dystopian scenario" (p. 318-19) — where apparently everyone would have to obey the law whether they wanted to or not.[78]

Biegel leaves the reader with the overall impression that he takes a dim view of the current copyright law, and therefore manipulates his regulatory model to advocate for change in deference to realism. In light of Biegel's views of online-hate sites, this attitude betrays an agenda-based application of the model on Biegel's part regarding the role of consensus. In the context of online hate sites, Biegel wants to challenge well-entrenched social norms — a.k.a. consensus — embodied in constitutional interpretation (p. 323) — rather than "facing reality" as he would with online copyright social norms.

D. *Corrupting the Model: Regulating Online Hate*

In some ways, subjecting Biegel's analysis of online hate sites to an overly searching scrutiny seems unfair because he essentially admits that in devising a method of regulation for this area, he is getting his ice skates ready in case hell freezes over (p. 326). Biegel advocates nothing less than discriminatory regulation of speech based on content (pp. 326, 328), which a vast majority of the American people, both on the left[79] and the right, oppose.[80] Admirably, Biegel acknowledges

77. *See* 17 U.S.C. § 1001-1010 (2003). When someone buys an MP3 player the law could require him or her to pay a royalty to copyright holders. Admittedly, this may well depress the sales of MP3 players, but these devices do contribute to a significant amount of copyright infringement.

78. The apparent downside being that the Clever Content Server is not clever enough to distinguish between pages containing copyrighted material and those that do not and turning the relevant features off and on as necessary — though this may come about someday with advancing technology. This would not prevent all copyright infringement on the web, but it would cut down on it without radical change.

79. At least as traditionally personified by the ACLU, though certain groups on the left disagree. *See* Philip Gailey, *ACLU Weakens Its Commitment to Free Speech*, ST. PETERSBURG TIMES, Apr. 11, 1993, at 2D (discussing traditional ACLU approach and its disagreement with some groups on the left over this approach).

80. P. 323. Of course to say that most Americans oppose content discrimination vastly oversimplifies First Amendment law. The Court carves a number of things out from First Amendment protection such as fighting words, Chaplinsky v. New Hampshire, 315 U.S. 568,

this and moves on to applying his model in the event of a First Amendment sea change.[81] He chooses obscenity as his model for crafting speech regulations (p. 346).

Why Biegel chooses obscenity as a model is a mystery. By hypothesis, he assumes a change in First Amendment law, and, logically, regulators would shove online hate into the obscenity exception only if the more likely First Amendment exceptions, such as incitement, defamation, or harassment were unavailable.[82] Part of this willingness to use obscenity as a model may result from Biegel's generosity in stating that the Supreme Court has a workable definition of obscenity that avoids vagueness and overbreadth problems (p. 346). A quick review of the Court's obscenity jurisprudence calls this into question,[83] especially in the online context, as Biegel acknowledges elsewhere (pp. 41-42). Also, a First Amendment exception allowing only for the "regulation of certain narrowly defined categories of online hate" would seem to be unique in First Amendment law.[84]

571-72 (1942), expression directed to inciting imminent lawless action, Brandenbug v. Ohio, 395 U.S. 444, 447 (1969), obscenity, Miller v. California, 413 U.S. 15 (1973), and libel, New York Times Co. v. Sullivan, 376 U.S. 254 (1964). When evaluating if speech falls into one of these unprotected areas, a court must consider the content. An alternative view maintains that the Constitution allows content restrictions but bars viewpoint discrimination — a government approved view. Am. Booksellers Assn. v. Hudnut, 771 F.2d 323 (7th Cir. 1985). Jurists, however, cannot follow this view blindly either — situations exist where the government does have an "approved view" and it restricts speech on this basis. *See, e.g.*, Leach v. Carlile, 258 U.S. 138 (1922) (government and manufacturer opinions diverged on the effectiveness of a drug, with the government preventing the manufacturer from disseminating its viewpoint through the mails). Suffice to say, for our purposes, a widely acknowledged concept exists, often labeled discrimination based on content, barring the government from doing exactly what Biegel proposes. *See* Police Dep't v. Mosley, 408 U.S. 92 (1972).

81. Biegel thinks such a change possible because America lies far outside the international mainstream on this issue. *See, e.g.*, Yahoo! Inc. v. La Ligue Contre Le Racisme & L'Antisemitisme, 145 F. Supp. 2d 1168, 1171-72 (N.D. Cal. 2001) (discussing French law banning the sale of Nazi-related items); Tania Branigan, *Threat of War: The Strange Journey of a Salvation Army Boy Who Converted to a Campaign of Hate*, THE GUARDIAN, Feb. 25, 2003, at 3 (discussing conviction of Muslim preacher for using threatening or abusive language to stir up racial hatred), *available at* www.Lexis.com/universe; Jon Sawyer, *U.S. Money in Egypt Obtains Mixed Results*, ST. LOUIS DISPATCH, Sept. 15, 2002, at B1 (noting conviction of professor for defaming the state). He also acknowledges, however, that if the international community reaches an agreement, the U.S. view may prevail because of the United States' domination over the equipment of the Internet. P. 352.

82. Biegel makes clear that case law currently bars these options. Pp. 328-38.

83. Paris Adult Theatre I v. Slaton, 413 U.S. 49 (1973) (Brennan, J., dissenting) ("we are manifestly unable to describe [obscenity] in advance except by concepts so elusive that they fail to distinguish clearly between protected and unprotected speech").

84. P. 347. Presumably Biegel chooses this approach under the assumption that the international community forced this First Amendment exception upon an unwilling America who would want to comply with an international treaty calling for such an exception and no more. At the least, this narrow approach conflicts with his reasons for analogizing obscenity and online hate. One might expect this, as it flies in the face of Justice Scalia's majority opinion in *R.A.V. v. City of St. Paul*, 505 U.S. 377 (1992). There the Court announced that simply because the government could proscribe the expression entirely does not mean it can discriminate based on the content within the proscribable area. *Id.* at 382-85. The First

Returning to the regulatory aspects, the question arises as to why Biegel opposes including private ordering[85] as a model of regulation (p. 220). His stated reason that private ordering does not satisfy the requirement "that a regulatory model must be all encompassing, with the potential to address almost every controversy in cyberspace" (p. 220) makes little sense.[86] Biegel does acknowledge the benefits of simply having the webhosting site cease to offer hate-related sites space (p. 328). Namely, such private actors do not trigger the state action requirement, and hence can act where the government could not in the face of First Amendment challenges (p. 328). While Biegel does not believe this would suffice, webhosting requires a significant capital outlay and adequate community pressure could convince these services of both the immorality and the unprofitability of continuing to provide service to such sites.[87] Proposing a regulatory scheme that has no chance of implementation while paying only lip service to a practical solution demonstrates an overcommitment to an academic idea, and a weakness in Biegel's model.

CONCLUSION

One can take issue with the particulars of Biegel's framework for evaluating and implementing regulatory changes. His categories are not comprehensive, and the credibility of his model suffers when he tries to force everything into one of them. At times, he appears willing to manipulate his model to achieve substantive goals. At other points, he seems willing to ignore real solutions to preserve the integrity of his model. The framework itself, however, does offer several important contributions. Namely, it forces the regulator to acknowledge that

---

Amendment does not, however, "prohibit[] *all* forms of content-based discrimination within a proscribable area of speech . . . a particular type of . . . content discrimination does not violate the First Amendment when the basis for it consists entirely of the very reason its entire class of speech is proscribable." Virginia v. Black, 123 S.Ct. 1535, 1540 (2003) (O'Connor, J.) (allowing content discrimination in a cross-burning case as a true threat, the form of intimidation most likely to inspire fear of bodily harm).

85. Private ordering involves self-regulation by Internet service providers. As private actors, the First Amendment does not constrain them. P. 220.

86. Biegel's problem here originates with his all encompassing definition of code-based solutions. By including such noncomprehensive solutions as content filters on individual computers under the code-based solution model, pp. 204-07, he can include individually noncomprehensive solutions in his regulatory model. This approach gives the impression that labeling drives this analysis more than content. With such a broad definition of code-based solutions, Biegel could have included Internet service provider self-regulation under this heading. *See* p. 200 (including filter access provided by Internet service providers as a code-based solution).

87. *See* Gary Williams, *"Don't Try to Adjust Your Television — I'm Black" Ruminations on the Recurrent Controversy over the Whiteness of TV*, 4 J. GENDER RACE & JUST. 99, 129-31 (2000) (discussing the use of boycotts to effect social change, including racial justice); *cf.* NAACP v. Claiborne Hardware, 458 U.S. 886 (1982) (discussing a store's unsuccessful suit against such a social-justice boycott that hurt its business).

control of the Internet is not an all or nothing proposition. It also provides a step-by-step analysis requiring the regulator to think about the best way to achieve his or her goal. In the end, perhaps the most valuable contribution comes from this methodical approach, forcing regulators into a reasoned analysis. The question is will actual regulators, unlike Biegel, be willing to go where the model leads them.