

# TEACHING CYBERLAW

ERIC GOLDMAN\*

## ABSTRACT

Over the past dozen years, Cyberlaw courses have become a staple of the law school curriculum. This Essay explores methodological and pedagogical issues raised by these courses.

## INTRODUCTION

In 1996, Judge Frank Easterbrook questioned the utility of a “Law and Cyberspace” course, saying it was as useful as a “Law of the Horse” course.<sup>1</sup> He argued that instead of treating cyberlaw as a discrete legal discipline, lawyers would be better served mastering foundational legal principles and then applying those principles to new factual circumstances as they arise.<sup>2</sup>

Judge Easterbrook’s observations were correct in at least two ways. First, specialty courses compete with general courses for student enrollment. Students who oversubscribe to specialty courses at the expense of foundational courses may limit the long-term value of their legal education. Second, Judge Easterbrook’s reaction nicely reflects the state of cyberlaw circa 1996, when cyberlaw was almost exclusively common law, and judges were rapidly

---

\* Assistant Professor and Director, High Tech Law Institute, Santa Clara University School of Law. E-mail: [egoldman@gmail.com](mailto:egoldman@gmail.com). Website: <http://www.ericgoldman.org>. I have taught Cyberlaw continuously since 1995–1996, at three different institutions. See <http://www.ericgoldman.org/cyberlaw.html>. Many thanks to Michael Bressman, David Goldstone, Mark Lemley, David Levine, Jessica Litman, Michael Madison, and Jason Schultz for their helpful comments.

1. See Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 207–08 (1996). For a rejoinder, see Lawrence Lessig, *The Law Of The Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999). The Easterbrook-Lessig exchange stimulated significant discussion, including some discussions about cyberlaw pedagogy. See, e.g., Marci Wilson, *Is Internet Law a Discreet [sic] Practice or Just Old Wine in a New Bottle?*, OF COUNSEL, Oct. 9, 2000, at 9.

2. Easterbrook, *supra* note 1, at 208.

creating this common law by applying basic legal doctrines to new cyberspace technologies.<sup>3</sup>

Nevertheless, I think Judge Easterbrook reached the wrong conclusion. From a pedagogical standpoint, specialty courses like Cyberlaw may reinforce basic legal principles for students and provide new insights into these principles, helping students deepen their understanding of the law.

More importantly, over the past dozen years, legislators have embraced the Internet enthusiastically, enacting an extensive body of cyberspace-specific statutory regulation. These regulations do not always comport with traditional common law principles.<sup>4</sup> A lawyer who (as Judge Easterbrook advised) simply mastered well-settled legal principles would not be adequately versed in modern cyberlaw.

There are other practical reasons to study cyberlaw in a standalone course. Today, given the Internet's ubiquity, just about every lawyer encounters some cyberlaw issues regardless of practice area. Further, cyberlaw provides a good case study of legal developments in response to rapidly evolving technology and business/social practices—a process that, in our technology-driven economy, many lawyers are likely to experience in their careers.

Although many U.S. law schools offer Cyberlaw courses, as a community of Cyberlaw teachers, we have engaged in relatively few extended discussions about how to teach the course. This brief Essay seeks to advance that conversation by considering the methodology and pedagogy of cyberlaw. The Essay considers the organization of a Cyberlaw curriculum in Part I, some challenges posed by Cyberlaw courses in Part II, some tools to teach Cyberlaw courses in Part III, evaluation methods in Part IV, and teaching materials in Part V.

## I. CYBERLAW'S PLACE IN THE LAW SCHOOL CURRICULUM

It is hard to identify the first Cyberlaw course precisely. In the 1980s, some schools offered a "Computer Law" course on substantive computer law or a "Computers and the Law" course on using computers in a legal practice. Sometime in the early 1990s, schools offered courses specifically focusing on the law of networked communications. The specifics may be lost to history, but pioneering courses probably were offered in 1993–1994, with perhaps a half-dozen courses in 1994–1995, about two dozen courses in 1995–1996, and

---

3. For example, a judge reinvigorated the ancient doctrine of common law trespass to chattels for the digital age. *See CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1020–22 (S.D. Ohio 1997).

4. See, for example, 47 U.S.C. § 230 (2000), a paradigmatic example of cyberspace exceptionalism.

rapid expansion thereafter.<sup>5</sup> Today, between one-half and two-thirds of U.S. law schools regularly offer at least one Cyberlaw course.<sup>6</sup> Other academic departments, including business and computer science/information science schools, offer Cyberlaw as well.<sup>7</sup>

An accurate course census is hindered by diversity in course titles and substantive coverage. The course lacks a single universally adopted course title; instead, popular Cyberlaw course titles include:

- “Cyberlaw”/“Cyberspace Law”/“Law of Cyberspace”
- “Internet Law”/“Law of the Internet”
- “Information Technology Law”/“IT Law”
- “E-commerce Law”

Historically, I have titled my course “Cyberspace Law” or “Cyberlaw” because the term covers the full range of electronic networks, such as Bulletin Board Systems (BBSs) not connected to the Internet. However, the term “cyberspace” may be slightly dated;<sup>8</sup> the term was more commonly used in the 1990s when other networks still competed with the Internet. Today, I suspect students would better understand the title “Internet Law,” and that may make it a more logical choice.<sup>9</sup>

Substantively, Cyberlaw courses often reflect one of the following approaches (clearly, this list is not exhaustive):

- *Survey courses* cover multiple disparate doctrines—such as jurisdiction, contracts, trespass to chattels, intellectual property, defamation, privacy, pornography, the First Amendment, tax, gambling, spam, spyware, etc.—typically emphasizing breadth over depth. Survey courses work well in either a lecture or seminar format, and both formats are popular. In some courses, student-organized reading assignments or student presentations comprise an integral part of the course’s content.

---

5. See Roberta Rosenthal Kwall, *The Intellectual Property Curriculum: Findings of Professor and Practitioner Surveys*, 49 J. LEGAL EDUC. 203, 204, 207 (1999) (in 1999, 34 of 69 schools responding to a survey offered a Cyberlaw course of some sort).

6. See Kenneth L. Port, *Essay on Intellectual Property Curricula in the United States*, 46 IDEA 165, 170 (2005) (in 2004–2005, 106 school websites listed some type of Internet law course).

7. Compilations of Cyberlaw course URLs can be found at JURIST, [http://www.jurist.law.pitt.edu/cour\\_pgs.htm#Cyberspace](http://www.jurist.law.pitt.edu/cour_pgs.htm#Cyberspace) (last visited Jan. 8, 2008), Prof. Jessica Litman’s website, <http://www-personal.umich.edu/~jdlitman/classes/cyber/courses.html> (last visited Jan. 8, 2008), and elsewhere.

8. See Posting of Robert Vamosi to CNET News.com Blog, *William Gibson: “Cyber” is Going Away*, [http://www.news.com/8301-10784\\_3-9756972-7.html](http://www.news.com/8301-10784_3-9756972-7.html) (Aug. 8, 2007, 1:42 PDT).

9. See Posting to Institute for Information Law & Policy Blog, *Cyberlaw Has Been Renamed “Internet Law” Starting Fall 2007*, [http://cairns.typepad.com/iilp/2007/03/cyberlaw\\_has\\_be.html](http://cairns.typepad.com/iilp/2007/03/cyberlaw_has_be.html) (Mar. 17, 2007).

- *Free speech-focused courses* focus on the Internet as a speech medium and the role of the First Amendment.
- *IP-focused courses* focus on IP and the Internet.
- *E-commerce courses* focus on doing business on the Internet. Architecturally, these courses often resemble survey courses, but they may emphasize different issues. For example, an e-commerce course may be an advanced commercial law course, emphasizing topics such as online authentication, the Uniform Computer Information Transactions Act (UCITA), and electronic currency. Alternatively, an e-commerce course may use a hypothetical e-commerce website as a case study.
- *Computer crimes courses* focus on the Computer Fraud & Abuse Act, the Electronic Communications Privacy Act, the Fourth Amendment and other topics.
- *Computer law courses* focus on the computer hardware and software industry. While some computer law topics do not obviously relate to cyberlaw (e.g., maskwork protections), computer law courses routinely cover many topics in other Cyberlaw courses.<sup>10</sup>
- *Cyberlaw clinics* provide supervised opportunities for students to work on cyberlaw-related litigation or other real-life projects.
- *Technology-in-practice courses* consider the role of technology in the legal practice.<sup>11</sup> Example courses include e-discovery and advanced legal research courses based on Internet research.

There is merit in each type of course, but I would like to offer two points in support of teaching Cyberlaw as a survey course. First, a survey of disparate legal doctrines can encourage students to think about client problems “horizontally” rather than in doctrinal silos. Horizontal cross-doctrinal issue-spotting is an essential skill for lawyers, but law school courses often do not practice that skill. By teaching students a critical way of thinking, a survey-style Cyberlaw course can significantly contribute to the law school curriculum.

Further, a survey-style Cyberlaw course can fill in doctrinal coverage gaps in the curriculum. For example, some first year professors omit topics like UCC Article 2 from contracts, or defamation from torts, deferring those topics to upper-division electives that students may or may not take. A Cyberlaw survey course may expose those students to otherwise-excluded concepts—a beneficial development for students who do not take the other contemplated

---

10. For that reason, computer law casebooks now incorporate cyberlaw materials. See, e.g., MARK A. LEMLEY ET AL., *SOFTWARE AND INTERNET LAW* (3d ed. 2006); PETER B. MAGGS ET AL., *INTERNET AND COMPUTER LAW CASES—COMMENTS—QUESTIONS* (2d ed. 2005).

11. See generally Bernard Hibbitts, *Innovative Instruction: Law School Courses Focus on the Technology of Law*, NAT’L L.J., Sept. 16, 2002, at C4 (giving examples of different courses in this category).

upper-division electives. Alternatively, when students have been exposed to doctrinal material before, a survey course may refresh and reinforce the material for students.<sup>12</sup>

#### A. *Cyberlaw and Curricular Overlaps*

Inevitably, Cyberlaw courses overlap to some degree with other courses in the curriculum. As cyberlaw becomes mainstream, “non-tech” courses are addressing cyberlaw topics and materials.<sup>13</sup> For example, contracts courses may discuss online contract formation<sup>14</sup> or the statute of frauds applied to electronic records,<sup>15</sup> and torts courses may discuss online trespass to chattels.<sup>16</sup> Overlap also can occur because of

- *Technological Convergence.* Technological convergence has caused some courses with disparate doctrinal antecedents to morph into Cyberlaw courses. Examples include Privacy Law, Communications Law, and Media Law, all of which now inevitably spend significant time discussing the Internet.
- *Incomplete Curricular Gatekeeping.* Curricular gatekeepers (such as the Academic Dean or a Curriculum Committee) may not recognize course overlap due to titling diversity (e.g., “Cyberlaw” sounds distinguishable from “IT Law”) or because a course’s substantive content is unclear.
- *Style Differentiation.* Professors sometimes encourage curricular gatekeepers to ignore possible overlaps because the professors have different teaching styles (e.g., lecture vs. seminar) or the courses are organized differently (e.g., one course is a survey and the other emphasizes free speech considerations).

Curricular overlap is not always bad, and repetition has some pedagogical value, but overlaps can confuse students and make it hard to select courses. Thus, with respect to the Cyberlaw curriculum, curricular gatekeeping is both a constant challenge and a vital function. In some cases, rather than proliferating new and overlapping courses, it may be better to offer another section of the same course (if student demand can support multiple sections).

---

12. For this reason, I encourage third year law students to consider Cyberlaw as a bar exam preparation tool.

13. See Katherine S. Mangan, *Law Schools Can't Meet the Demand for Courses on Internet Issues*, CHRON. HIGHER EDUC., Sept. 29, 2000 at A12, A13.

14. Contracts casebooks may include cases such as *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996) and *Specht v. Netscape Commc'ns Corp.*, 306 F.3d 17 (2d Cir. 2002). See, e.g., JOHN D. CALAMARI, ET AL., *CASES AND PROBLEMS ON CONTRACTS* 127–33, 186–95 (5th ed. 2007).

15. Contracts casebooks often discuss the Uniform Electronic Transactions Act (UETA) and the Electronic Signatures in Global and National Commerce Act (E-SIGN). See, e.g., JOHN E. MURRAY, JR., *CONTRACTS: CASES AND MATERIALS* 10 (6th ed. 2006).

16. See, e.g., *Intel Corp. v. Hamidi*, 71 P.3d 296 (Cal. 2003).

### B. *Credit Hours*

Typically, Cyberlaw is taught as a two- or three-unit course in a single semester. A two-unit survey course tends to feel fairly rushed to students, and it requires professors to make some difficult coverage decisions. As a result, many professors choose to teach Cyberlaw as a three-unit course. A one-unit Cyberlaw survey course would pose significant coverage challenges, but a specialized cyberlaw topic (e.g., Jurisdiction in Cyberspace) might lend itself very well to a short course format. At schools with a large student demand for Cyberlaw courses, Cyberlaw could be organized into a two-semester six-unit sequence of basic and advanced courses.

## II. PEDAGOGICAL CHALLENGES

This Part discusses some pedagogical challenges commonly encountered when teaching Cyberlaw.

### A. *Topic Organization*

Cyberlaw can be difficult to organize because many legal doctrines are conceptually linked to each other, providing no single ideal place to start. For example, the trespass to chattels (TTC) doctrine is an important legal doctrine with respect to both spam<sup>17</sup> and factual databases,<sup>18</sup> and it also arises in any discussion about regulatory differences between physical and virtual property. So, where is the best place to introduce the doctrine? Currently, I discuss contracts, then TTC (comparing and contrasting *Hamidi* and *Register.com*), and then copyright, after which I discuss how contracts, copyright, and TTC are all tools that can be used to protect factual databases. At the semester's end, I cover spam as a capstone topic. This approach works passably, but it means TTC is referenced in three different places in the course.

Similar organizational challenges also arise with the coverage of search engines, blogs, virtual worlds, social networking sites (such as MySpace and Facebook), adware/spyware, and other technological applications. These technologies often implicate multiple cyberlaw doctrines, making them perfect semester-end capstone topics. However, these technologies inevitably arise during the semester, so where is the best place to introduce them? Inevitably, there will be some redundancies and divided coverage.

Finally, cyberlaw simultaneously involves the substantive legal doctrines of cyberspace and the regulatory processes used to develop those doctrines. Both topics warrant careful exploration, and most cyberlaw professors end up

---

17. See, e.g., *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015 (S.D. Ohio 1997); *Hamidi*, 71 P.3d 296.

18. See, e.g., *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 404–05 (2d Cir. 2004); *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1069–72 (N.D. Cal. 2000).

addressing both. However, this creates some tension in allocating scarce class time between substantive doctrines and jurisprudential processes. As a result, the allocation ratio between the two discussions, and their placement in the semester, may vary widely among professors.

### B. *Evolving Law*

Cyberlaw changes constantly. For example, during the 1990s, I routinely replaced one-third to one-half of my teaching materials *every year*; and I no longer teach *any* materials from my Spring 1996 course reader.<sup>19</sup> While the rate of legal change may be slowing,<sup>20</sup> cyberlaw still evolves much faster than most other legal doctrines. This puts significant pressure on casebook authors and publishers to keep casebooks up-to-date.<sup>21</sup> As a result, cyberlaw professors often feel like they need to keep up with new developments personally, perhaps more so than in other doctrinal areas.<sup>22</sup>

Cyberlaw also has many doctrinal holes and ambiguities where the rules are still developing. Further, cyberlaw lacks the time-tested classic teaching materials found in more established doctrines, and some cyberlaw doctrines lack good teaching materials at all.<sup>23</sup> As a result, students can easily leave the course confused about the applicable legal rules, and professors have to work hard to avoid this outcome.

---

19. See Posting of Eric Goldman to Technology & Marketing Law Blog, *Fall 2005 Cyberlaw Syllabus*, [http://blog.ericgoldman.org/archives/2005/08/new\\_cyberlaw\\_sy.htm](http://blog.ericgoldman.org/archives/2005/08/new_cyberlaw_sy.htm) (Aug. 14, 2005, 13:20).

20. See Posting of Eric Goldman to Technology & Marketing Law Blog, *Fall 2006 Cyberlaw Syllabus*, [http://blog.ericgoldman.org/archives/2006/08/fall\\_2006\\_cyber.htm](http://blog.ericgoldman.org/archives/2006/08/fall_2006_cyber.htm) (Aug. 13, 2006, 08:34).

21. See Part V, *infra*.

22. Fortunately, many blogs and news services cover cyberlaw. Two tools used by many cyberlaw professors are:

- The Cyberprof e-mail list, maintained by Professor Mark Lemley of Stanford Law School. To subscribe, contact Professor Lemley personally.
- BNA's Internet Law News e-mail newsletter, maintained by Professor Michael Geist of University of Ottawa, Faculty of Law. To subscribe, see *BNA's Internet Law News*, <http://ecommercecenter.bna.com> (last visited Jan. 15, 2008).

23. An example might be online jurisdiction, where the seminal *Zippo* case is often cited but rarely followed. Compare *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997), with *Toys "R" Us, Inc., v. Step Two, S.A.* 318 F.3d 446, 452–54 (3d Cir. 2003) (citing *Zippo* but adopting a different test), and *ALS Scan, Inc. v. Digital Serv. Consultants, Inc.*, 293 F.3d 707, 714 (4th Cir. 2002) (same).

### C. *Heterogeneous Technical Backgrounds*

Cyberlaw students typically have widely heterogeneous levels of technological sophistication. Classes typically attract some highly motivated software engineers, and some courses are cross-listed with other departments (like Engineering) whose students bring significant technical expertise into the classroom. However, the course may also attract casual Internet users who are intimidated by the course's technological issues and their more technical peers. This mix of students can lead to excellent cross-fertilization of ideas, but it can be challenging to design a course that satisfies both audiences.

To deal with student heterogeneity, I typically spend the first two weeks of the semester defining terms and explaining basic Internet technologies. Occasionally the Netheads find this module "slow," but the foundational discussion helps minimize confusion later in the semester. This may also minimize grading disparities at exam time.

### D. *Sensitive Content*

Cyberlaw courses inevitably cover sensitive topics—e.g., pornography,<sup>24</sup> racist content,<sup>25</sup> misogynistic content,<sup>26</sup> and other types of generally offensive content.<sup>27</sup> As with any other curricular area with sensitive topics, professors should understand that students will be uncomfortable and proceed gently.

## III. PEDAGOGICAL OPTIONS

This Part discusses some pedagogical options available to cyberlaw professors.

---

24. For example, I have taught at least one *Playboy* case every year for the past thirteen years, and I expect to continue doing so for the foreseeable future. See Posting of Eric Goldman to Technology & Marketing Law Blog, *Fall 2005 Cyberlaw Syllabus*, [http://blog.ericgoldman.org/archives/2005/08/new\\_cyberlaw\\_sy.htm](http://blog.ericgoldman.org/archives/2005/08/new_cyberlaw_sy.htm) (Aug. 14, 2005 13:20). However, *Perfect 10* may supplant *Playboy*'s role as an Internet law mainstay; I included three *Perfect 10* cases in my 2007 course. See Eric Goldman, *2007 Cyberspace Law Syllabus*, <http://www.ericgoldman.org/Courses/cyberlaw/2007cyberlawsyllabus.pdf> (last visited Jan. 9, 2008).

25. See *Noah v. AOL Time Warner, Inc.*, 261 F. Supp. 2d 532, 535 (E.D. Va. 2003) (AOL allegedly discriminated against Muslims; the opinion quotes some racist and offensive statements made by other AOL users).

26. See *U.S. v. Alkhabaz*, 104 F.3d 1492, 1497–98 n.1 (6th Cir. 1997) (containing the text of a disturbing and offensive rape-murder "fantasy" story).

27. See *Zeran v. America Online, Inc.*, 958 F. Supp. 1124, 1127 nn.3 & 5 (E.D. Va. 1997) (referencing some of the offensive T-shirts offered by an anonymous prankster with messages that were highly insensitive to 1996 Oklahoma City bombing victims).

### A. *Digital Artifacts*

Cyberlaw is rich with digital artifacts, such as screenshots of websites that led to litigation. Unfortunately, by the time a case reaches the classroom, usually the subject website has changed or is offline altogether. Fortunately, the Wayback Machine<sup>28</sup> can help resurrect websites. Through the Wayback Machine, I have found the websites of (among others) Ken Hamidi,<sup>29</sup> Terri Welles,<sup>30</sup> Christopher Lamparello,<sup>31</sup> Equitrac,<sup>32</sup> and others. These digital artifacts can make the topic clearer to students (“a picture is worth a thousand words”) and perhaps reveal interesting and fun facts not discussed in the court’s opinion.<sup>33</sup>

### B. *Online Interactivity*

Given the students they attract and their subject matter, Cyberlaw courses naturally lend themselves to experimentation with online interactive components.<sup>34</sup> Some options to consider are

- *E-mail Lists/Message Boards/Blogs.* A class e-mail list, message board, or blog can allow the professor to broadcast content to students between class sessions or allow students to interact with each other online, thereby extending the course discussion outside the classroom’s time and space. These tools also can be configured to allow students to self-publish content to the world.
- *Wikis.* Wikis can help groups jointly develop and edit documents. Wikis also can enable student self-publication.
- *Virtual Worlds.* Virtual worlds can provide an online environment for student-professor or student-student interactions, including chats and group collaboration. Virtual worlds also may provide an interesting laboratory for students to experiment with course principles.

---

28. <http://www.archive.org> (last visited Jan. 9, 2008). For more recently changed web pages, Google’s “Cache” feature may provide better artifacts than the Wayback Machine. Also, Professor Rebecca Tushnet at Georgetown University Law Center maintains the Georgetown IP Teaching Resources Database, another source for digital artifacts. For access, contact Professor Tushnet directly.

29. See *Intel Corp. v. Hamidi*, 71 P.3d 296 (Cal. 2003).

30. See *Playboy Enters., Inc. v. Welles*, 279 F.3d 796 (9th Cir. 2002).

31. See *Lamparello v. Falwell*, 420 F.3d 309 (4th Cir. 2005).

32. See *Promatek Indus., Ltd. v. Equitrac, Corp.*, 300 F.3d 808 (7th Cir. 2002). The pre-injunction website shows the keyword metatags that sparked the litigation.

33. See generally Rebecca Tushnet, *Sight, Sound, and Meaning: Teaching Intellectual Property with Audiovisual Materials*, 52 ST. LOUIS U. L.J. 891 (2008) (discussing the use of artifacts in intellectual property courses).

34. Because these components have utility in all courses (not just Cyberlaw), there is a rich literature on the subject. See, e.g., Pearl Goldman, *Legal Education and Technology: An Annotated Bibliography*, 93 LAW LIBR. J. 423 (2001).

### C. *Integration with Transactional Drafting*

Cyberlaw offers a good platform to integrate transactional drafting lessons. For example, in an online contracts module, students can draft a user agreement; and when discussing online privacy, students can draft a privacy policy. Transactional drafting is time-consuming to teach, so it competes with doctrinal material for scarce class time, but this type of cross-training can yield good pedagogical payoffs.<sup>35</sup>

### D. *Integration with Ethics Discussions*

Cyberlaw presents a great opportunity to teach ethics pervasively.<sup>36</sup> Cyberlaw is filled with morally ambiguous situations and actors, so I raise ethical considerations in connection with almost every cyberlaw case I teach. For example, some ethical issues I raise from *Intel v. Hamidi* are

- *Property Rights*. Did Hamidi need Intel's permission to use its computer network? Even if a network owner acquiesces to certain public uses by connecting to the Internet, was it ethical for Hamidi to continue sending e-mails to Intel when he knew that Intel was trying to block his messages?
- *Illicit Data*. Was it ethical for Hamidi to knowingly use an illicit list of Intel employee e-mail addresses?
- *Spam*. Is it ethical to send spam, and how is Hamidi's situation similar/different?
- *Censorship*. Is it ethical for a company to squelch e-mails to its employees because it does not like the substance of the e-mails?
- *Pro Se Litigants*. Did Intel or the judicial system owe any extra duties to Hamidi as a pro se litigant?
- *Setting a Trap*. The dissent suggests that system owners might reduce their investments in their networks to set legal traps for people like Hamidi. Would it be ethical to do so?

While *Intel v. Hamidi* is particularly rich in ethical issues, ethics topics arise in just about every cyberlaw doctrine, and students often find it stimulating to explore them.

---

35. See Eric Goldman, *Integrating Contract Drafting Skills and Doctrine*, 12 J. LEGAL WRITING INST. 209 (2007).

36. See Deborah L. Rhode, *Ethics by the Pervasive Method*, 42 J. LEG. EDUC. 31 (1992).

#### IV. EVALUATION METHODS

##### A. Exams

I typically test on real-life situations rather than manufactured facts. Often, I ask students to critique a live website, and I allow and encourage them to review the website while writing their answer. This approach can be risky; public critique of a live website in a sample answer can be defamatory or constitute legal advice. On the plus side, real-life situations routinely are more interesting than anything I could hypothesize, and students find it helpful (or, at least, comforting) to explore the website while preparing their answers.<sup>37</sup>

##### B. Papers

Cyberlaw is a rich area for student papers. Cyberlaw has lots of underexplored areas, and promising new topics are being generated daily. Furthermore, numerous writing competitions will accept student papers on cyberlaw topics,<sup>38</sup> and cyberlaw papers are very publishable (especially given the proliferation of technology-focused specialty journals).

Unfortunately, student papers rarely achieve this potential, instead often gravitating to uninspired topics such as: descriptive topics that summarize a case or the current law without offering any analytical discussion; current event topics on an imbroglio du jour, or a pending case or statute that will be forgotten, mooted, or preempted when the student completes the paper; or overgrazed topics where a student has very little chance of adding value to a thoroughly discussed topic.<sup>39</sup> As professors, we can help students avoid these pitfalls by carefully guiding their topic selection process.<sup>40</sup>

#### V. READING MATERIALS

Finding good cyberlaw teaching materials can be challenging. There are many excellent casebooks on the market,<sup>41</sup> but no cyberlaw casebook is perfect. First, because cyberlaw is rapidly evolving, published cyberlaw

---

37. In case the website is off-line during the exam period, the exam describes the website and includes screenshots so students can identify the key points even if they cannot inspect the website.

38. In my biased opinion, the most comprehensive source of writing competitions is my mom's book, which most law school libraries now have in their collections. See the most current version of GAIL ANN SCHLACHTER & R. DAVID WEBER, *HOW TO PAY FOR YOUR LAW DEGREE*.

39. For example, I emphatically discourage students from writing about online music distribution or *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005).

40. Among other things, I require students to read Professor Volokh's *Academic Legal Writing* before the semester. See EUGENE VOLOKH, *ACADEMIC LEGAL WRITING: LAW REVIEW ARTICLES, STUDENT NOTES, SEMINAR PAPERS, AND GETTING ON LAW REVIEW* (3d ed. 2007).

41. See APPENDIX 1, *infra*.

casebooks have a short shelf life and are often effectively out-of-date upon publication.<sup>42</sup> Second, given the topical linkages discussed above, many professors have their own unique preferences for organizing topics, and casebooks may not match that organization.

Instead of using a published casebook, a substantial number of cyberlaw professors compile their own reader. Back in the 1990s, when the casebook market had not yet developed, this was a necessity. Even now, with good casebooks on the market, a self-prepared reader offers several benefits:

- The professor can pick exactly what materials he or she wants to cover (meaning no wasted or unused material) and can edit and organize the material to his or her preferences.
- The material can be up-to-date. Indeed, some professors feel that if they must prepare a supplement anyway, preparing an entire reader is not much extra incremental work.
- A reader typically costs students less than a casebook.
- The materials can be published to the Internet, allowing students to access and read them online if they choose.<sup>43</sup>

For these reasons, I believe that preparing my own reader produces better results than using a published casebook. However, self-prepared readers require extra time to prepare and edit,<sup>44</sup> so many professors may reach the opposite conclusion.

### CONCLUSION

Even if we disagree with Judge Easterbrook's assessment of the merits of teaching Cyberlaw as a standalone course,<sup>45</sup> it does not inherently follow that the course's *pedagogy* raises unique issues. Indeed, many issues discussed in this Essay are not unique to Cyberlaw, but arise (sometimes regularly) in other aspects of the legal curriculum.

---

42. Mark Lemley related a story to me highlighting this challenge. He and his co-authors submitted the first edition of the *Software and Internet Law* casebook in October 1999, with a scheduled publication date of March 2000. Due to changes during that period (such as enactment of ICANN's Uniform Dispute Resolution Policy (UDRP) and the Anti-Cybersquatting Consumer Protection Act), a website providing updates for the casebook was launched *before* the book was published.

43. To increase the odds that students will actually read the materials, I compile my reader into a printed volume, but I also post a hyperlinked syllabus for students who want to read the unedited materials.

44. I typically spend ten to twenty hours a year preparing and editing my reader, but I also make two time-saving choices: (1) I do not include any materials that require me to obtain copyright permissions, and (2) I include a much smaller number of items than a typical casebook would contain.

45. See Easterbrook, *supra* note 1.

Nevertheless, this Essay discusses many thorny issues that, collectively, test our skills as teachers. Cyberlaw is a tremendously fun, interesting—and challenging—course to teach. We all benefit by identifying and acknowledging these challenges, by constantly innovating our teaching methods, and by sharing our tips with each other. This Essay is just one limited and early step towards that goal. I look forward to continuing this discussion.

## APPENDIX 1. BIBLIOGRAPHY OF CYBERLAW TEACHING MATERIALS

*Cyberlaw Casebooks*

- PATRICIA L. BELLIA ET AL., *CYBERLAW: PROBLEMS OF POLICY AND JURISPRUDENCE IN THE INFORMATION AGE* (3d ed. 2006)
- RAYMOND S.R. KU & JACQUELINE D. LIPTON, *CYBERSPACE LAW: CASES AND MATERIALS* (2d ed. 2006)
- MARK A. LEMLEY ET AL., *SOFTWARE AND INTERNET LAW* (3d ed. 2006)
- PETER B. MAGGS ET AL., *INTERNET AND COMPUTER LAW: CASES—COMMENTS—QUESTIONS* (2d ed. 2005)
- RONALD J. MANN & JANE K. WINN, *ELECTRONIC COMMERCE* (2d ed. 2004)
- MARGARET JANE RADIN ET AL., *INTERNET COMMERCE: THE EMERGING LEGAL FRAMEWORK* (2d ed. 2006)
- MARGARET JANE RADIN ET AL., *INTELLECTUAL PROPERTY AND THE INTERNET: CASES AND MATERIALS* (2004)
- MADELEINE SCHACHTER, *LAW OF INTERNET SPEECH* (2d ed. 2002)
- RICHARD WARNER ET AL., *E-COMMERCE, THE INTERNET AND THE LAW, CASES AND MATERIALS* (2006)
- JONATHAN L. ZITTRAIN, *INTERNET LAW* (forthcoming 2008)
- JONATHAN L. ZITTRAIN, *INTERNET LAW JURISDICTION* (2005)
- JONATHAN L. ZITTRAIN, *INTERNET LAW TECHNOLOGICAL COMPLEMENTS TO COPYRIGHT* (2005)

*Computer Crime Casebooks*

- ORIN S. KERR, *COMPUTER CRIME LAW* (2006)
- DAVID J. LOUNDY, *COMPUTER CRIME, INFORMATION WARFARE & ECONOMIC ESPIONAGE* (2003)

*Some Widely Read Cyberlaw-Related Books*<sup>46</sup>

- ORSON SCOTT CARD, *ENDER'S GAME* (1985)
- WILLIAM GIBSON, *NEUROMANCER* (1984)
- LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* (1999)
- BRUCE STERLING, *THE HACKER CRACKDOWN: LAW AND DISORDER ON THE ELECTRONIC FRONTIER* (1992)
- CLIFFORD STOLL, *THE CUCKOO'S EGG: TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE* (1989)

*Some Cyberlaw History*

- EDWARD A. CAVAZOS & GAVINO MORIN, *CYBERSPACE AND THE LAW: YOUR RIGHTS AND DUTIES IN THE ON-LINE WORLD* (1994)
- MIKE GODWIN, *CYBER RIGHTS: DEFENDING FREE SPEECH IN THE DIGITAL AGE* (1998)
- LANCE ROSE, *NETLAW: YOUR RIGHTS IN THE ONLINE WORLD* (1995)
- LANCE ROSE & JONATHAN WALLACE, *SYSLAW* (2d ed. 1992)

---

46. By definition, a selected list like this is woefully underinclusive; my goal here is to encourage you to explore a few books that are well known among cyberlaw professors.