

# Who Controls the Internet? Illusions of a Borderless World

By: Jack Goldsmith and Tim Wu

**Citation:** JACK GOLDSMITH & TIM WU, WHO CONTROLS THE Internet? ILLUSIONS OF A BORDERLESS WORLD (Oxford University Press, Inc., 2006).

**Reviewed By:** Robert C. Sanfilippo<sup>1</sup>

**Relevant Legal & Academic Areas:** Internet Law, International Law, Civil Procedure, Government Regulation, Copyright Law, Privacy

**Summary:** This book is divided into an introduction and three main parts. The Introduction discusses the popular search engine Yahoo!, and its battles with the French Government regarding Nazi memorabilia posted on its auction website. Part 1 discusses the origin of the Internet, what the Internet entails and the major players involved in the belief that it should transcend territorial law. Part 2 describes government efforts to control and regulate the Internet. Part 3 provides a balance between the benefits and disadvantages of government control of the Internet and what is in store for future regulation.

**About the Authors:** **Jack Landman Goldsmith** received his B.A. from Washington and Lee University, graduating *summa cum laude* in 1984.<sup>2</sup> Mr. Goldsmith then achieved a supplementary Bachelor of Arts and a Masters of Arts degree, both from Oxford University, graduating with first class honors.<sup>3</sup> After graduating Yale Law School, Mr. Goldsmith clerked for Judge J. Harvie Wilkinson on the U.S. Court of Appeals for the Fourth Circuit, and for Justice Anthony M. Kennedy on the United States Supreme Court.<sup>4</sup> Mr. Goldsmith later began teaching at the University of Chicago Law School and subsequently at the University of Virginia

---

<sup>1</sup>J.D. Candidate, Syracuse University College of Law, 2008; Executive Editor, *Syracuse Science and Technology Law Reporter*.

<sup>2</sup> HLS: Faculty Directory, <http://www.law.harvard.edu/faculty/directory/facdir.php?id=559> (last visited Nov. 2, 2007).

<sup>3</sup> American Enterprise Institute for Public Policy Research, <http://www.aei.org/scholars/scholarID.91,filter.all/scholar.asp> (last visited Mar. 24, 2007).

<sup>4</sup> *Id.*

School of Law.<sup>5</sup> Mr. Goldsmith also formerly served in the General Counsel's office at the Pentagon and later as an Assistant Attorney General in the Office of Legal Counsel for the Department of Justice.<sup>6</sup> Presently, Mr. Goldsmith is a Professor of Law at Harvard Law School.<sup>7</sup>

**Tim Wu** graduated from McGill University in 1995 and from Harvard Law School in 1998.<sup>8</sup> Mr. Wu has also worked for the office of Legal Counsel for the Department of Justice.<sup>9</sup> After Mr. Wu's employment with the Department of Justice, he clerked for Judge Richard Posner of the Seventh Circuit Court of Appeals and later for Justice Stephen Breyer on the United States Supreme Court.<sup>10</sup> Mr. Wu was a visiting professor at the University of Virginia School of Law and is presently a Professor of Law at Columbia Law School.<sup>11</sup> Mr. Wu also has a personal website with additional articles and information available at [www.timwu.org](http://www.timwu.org).

## **Chapter 1 – Introduction – Yahoo!**

- **Chapter Summary:** Chapter 1 provides a detailed summary of the 2000 *Yahoo!* case involving Yahoo!'s auction website and the Nazi memorabilia accessible to French citizens on the website. The introduction describes the events leading up to the French court's decision and also Yahoo!'s struggles to comply with the resulting Order. The chapter ends briefly by discussing Yahoo!'s relationship with the People's Republic of China.

---

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

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

<sup>7</sup> HLS: Faculty Directory, *supra* note 2.

<sup>8</sup> Columbia Law: Full Time Faculty, [http://www.law.columbia.edu/fac/Timothy\\_Wu](http://www.law.columbia.edu/fac/Timothy_Wu) (last visited Mar. 24, 2007).

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

<sup>10</sup> *Id.*

<sup>11</sup> *Id.*

- **Chapter Discussion:** Chapter 1 opens with the story of a French citizen, Marc Knobel, and his fight against neo-Nazism. After discovering Nazi memorabilia on Yahoo!’s auction website, Mr. Knobel sued Yahoo! in a French court asserting that Yahoo! had violated French law which banned the trafficking of Nazi goods in France.<sup>12</sup> Lawyers for the plaintiff argued that France “had a right to defend itself from the sale illegal merchandise from the United States” and the lawyers also asked Yahoo! to defend its position that it should be exempt from French law.<sup>13</sup>

Yahoo!’s defense, which the authors labeled an “impossibility defense,” was that the French website, [www.yahoo.fr](http://www.yahoo.fr), complied with French law, but the U.S. website, which did not have comply with French law, could still be visited by French citizens.<sup>14</sup> Because Yahoo! had no way of identifying where the location of the users were coming from, compliance with French law would require removal of all Nazi items from the U.S. website and this would deprive U.S. citizens the opportunity to purchase the memorabilia and subsequently make French law “the effective rule for the world.”<sup>15</sup>

The French court held that Yahoo! did violate French law and ordered the website to “take all necessary measures to dissuade and make impossible visits by French web surfers to the illegal Yahoo! Nazi auction sites.”<sup>16</sup> At first, Yahoo! did not comply with

---

<sup>12</sup> JACK GOLDSMITH & TIM WU, *WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD* 1 (Oxford University Press, Inc.) (2006).

<sup>13</sup> *Id.* at 3.

<sup>14</sup> *Id.* at 5.

<sup>15</sup> *Id.*

<sup>16</sup> *Id.* at 5. The authors cite to *La Ligue Contre le Racisme et L’Antisemitisme and L’Union des Etudiants Juifs de France v. Yahoo! Inc. and Yahoo! France*, Interim Court Order, The County Court of Paris 6, May 22, 2000, available at [http://www.eff.org/legal/Jurisdiction\\_and\\_sovereignty/LICRA\\_v\\_Yahoo/20001120\\_fr\\_int\\_ruling.en.pdf](http://www.eff.org/legal/Jurisdiction_and_sovereignty/LICRA_v_Yahoo/20001120_fr_int_ruling.en.pdf) (last visited Mar. 24, 2007).

the French order. However, after three court-appointed experts asserted Yahoo! could comply with the order and after warnings from the French court that it would issue fines up to \$13,000 a day, Yahoo! surrendered and took down all Nazi memorabilia from its various auction sites.

The chapter then briefly introduces Yahoo!’s relationship with the People’s Republic of China and China’s demands for Yahoo! to filter out “materials that may be harmful or threatening to Party rule.”<sup>17</sup> This topic is discussed in more detail in later chapters.

## **Part 1 – The Internet Revolution**

### **Chapter 2 – Visions of a Post Territorial Order**

- **Chapter Summary:** This chapter discusses the early explorers of the Internet, the MUD phenomenon and the notion of the Internet as self-governing: a place free from government regulation and the authority of nation-states. The chapter ends by introducing the “founders of the Internet” and their quest to preserve the values of the Internet.
- **Chapter Discussion:** Chapter 2 discusses the early users of the Internet and the stories they told of a world free from government regulation. These stories were predominantly based on the users interaction with the “interactive worlds called ‘multiple user dungeons,’ or MUDs.”<sup>18</sup> The MUD experience is explained in detail as a place where users log on from all over the world and become part of a “virtual community.”<sup>19</sup> The

---

<sup>17</sup> GOLDSMITH & WU, *supra* note 12, at 9.

<sup>18</sup> *Id.* at 14.

<sup>19</sup> *Id.* at 14-15.

early Internet, the authors argue, was a genuinely intimate community, a real cyberspace where “people who rarely met face-to-face got to know one another intimately.”<sup>20</sup>

In addition, the chapter discusses the commitment of the early Internet users to keep the Internet free from government regulation by establishing groups such as the Electronic Frontier Foundation, and further, by drafting documents such as the *Declaration of Cyberspace Independence*.<sup>21</sup> Chapter Two also accounts the first “great attack on cyberspace,” the Communications Decency Act (the “CDA”), and describes in detail *ACLU v. Reno*, the Supreme Court case analyzing the constitutionality of the CDA.<sup>22</sup>

In discussing the idea of a self-ruling cyberspace, the chapter introduces the “founders of the Internet,” including people such as Larry Roberts, Robert Kahn, Vint Cerf, Jon Postel and Dave Clark. The chapter continues by discussing the origin and the design of the Internet, its primary creation for the Department of Defense, and addressing the values of the Internet which were “open, minimalist, and neutral.”<sup>23</sup> The founders aimed to preserve these values by establishing such groups as the Internet Engineering Task Force (IETF), which the chapter analyzes in detail.<sup>24</sup>

---

<sup>20</sup> *Id.* at 16.

<sup>21</sup> *Id.* at 20, citing John Perry Barlow, *A Declaration of the Independence of Cyberspace*, <http://homes.eff.org/~barlow/Declaration-Final.html>.

<sup>22</sup> *ACLU v. Reno*, 521 U.S. 844 (1997); Communications Decency Act, Pub. L. No. 104-104, 110 Stat 56 (1996).

<sup>23</sup> GOLDSMITH & WU, *supra* note 12, at 22-23. The authors explain that “*open*” means the net was “willing to accept almost any kind of computer or network,” “*minimalist*”, “because it required very little of the computers that wanted to join,” and “*neutral*” between applications – e-mail, downloads and every other type of application was treated the same.”

<sup>24</sup> *Id.* at 24.

The chapter closes by examining a second view, the Internationalist view. This theory argues for a global governmental institution to work together to regulate certain aspects of the Internet, including libel, pornography, copyright and consumer protection.

### **Chapter 3 – The God of the Internet**

- **Chapter Summary:** The chapter discusses the goals and efforts by the founders of the Internet to maintain full control over the Internet. The chapter explains the eventual demise of their efforts and introduces a new age of the Internet, one which is government controlled.
- **Chapter Discussion:** Chapter 3 opens with a brief story of Jon Postel and his attempt to take control over the Internet using “root authority.”<sup>25</sup> The chapter then examines how a computer communicates using the Internet by introducing and explaining terms such as “domain names” and “Internet Address.”<sup>26</sup> Further, the chapter explains the importance of “root authority” in controlling the Internet, and touches upon the arguments presented by “the founders” and the U.S. government in the battle of who should control this “root authority.”

Chapter 3 closes by describing Postel’s last good-faith attempt to transfer “root authority” and regain control. However, the U.S. government’s threat of legal force superseded his attempt. At the end of the chapter, the authors introduce the government’s issuance of the Green Paper, “which set forth its [U.S.] initial vision of Net governance,

---

<sup>25</sup> *Id.* at 29-30. “Root authority” is “the power to issue orders respecting domain names and numbers and have those orders obeyed.”

<sup>26</sup> *Id.* at 30-32. “Internet Address” is a set of numbers, i.e. ‘128.143.28.135,’ which enable your computer to communicate on the Internet. Short hand names or “domain names” are then given to the numbers for easy access for the user.

asserting total authority over the Internet Root...” and also marked the beginning of a government controlled Internet.<sup>27</sup>

## **Part 2 – Government Strikes Back**

### **Chapter 4 – Why Geography Matters**

- **Chapter Summary:** This chapter explores the importance of geographical borders and the effects of borders on each Internet user’s experience. These experiences are based on such categories as language, culture, preferences, expectations and geographic locations.
- **Chapter Discussion:** Chapter 4 opens with a discussion of language, which the authors deem “the most immediate and important difference reflected by borders.”<sup>28</sup> The chapter discusses how English websites originally dominated the Internet, but as time progressed, the percentage of websites in English substantially decreased.

Further, Chapter 3 addresses additional reasons an Internet user would want a unique experience from other users, such as different “culture, currency, climate and consumers norms.”<sup>29</sup> During the discussion of user preferences, the chapter shifts to a discussion on the benefits of information filtering. The authors conclude that geography is the most efficient way to match products and services to each Internet user, and illustrate their conclusion with an Amazon.com example.<sup>30</sup>

In addition, chapter 4 presents a discussion on the importance of “place.” Here, the authors introduce the term “bandwidth” and explain that a greater “bandwidth” will

---

<sup>27</sup> *Id.* at 46.

<sup>28</sup> GOLDSMITH & WU, *supra* note 12, at 50.

<sup>29</sup> *Id.* at 51.

<sup>30</sup> *Id.* at 52-53.

result in faster communication on the Internet.<sup>31</sup> The authors contend that the effectiveness of the Internet's communication is conditioned upon the real-space location of the data, the hardware through which the data will travel, and the geographic distribution of that hardware.<sup>32</sup> This is illustrated through an example describing a computer user in Boston, who could type a query into Yahoo!'s search engine, but it would be costly and time-consuming for the request to travel from California, where Yahoo!'s servers are, to the user's computer in Boston.<sup>33</sup>

The chapter states the final reason for the importance of "real-space geography" by presenting the early problems with Amazon.com.<sup>34</sup> Amazon originally took orders only from Seattle, as they had no retail stores, very little inventory and no "physical presence outside Seattle."<sup>35</sup> Problems arose when out of state customers wanted to return items or when customers ordered more than one book. The limited availability of the books delayed orders. Amazon was forced to build warehouses scattered across the world closer to their customers in order to address these problems.

Chapter 4 closes with an examination of Net Geo-Identification, what it is, and the benefits and consequences of using it.

---

<sup>31</sup> *Id.* at 54. The authors describe bandwidth as "the amount of data that can be sent through an Internet connection in a particular time."

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

<sup>33</sup> GOLDSMITH & WU, *supra* note 12, at 55.

<sup>34</sup> *Id.* at 57.

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

## Chapter 5 – How Governments Rule the Net

- **Chapter Summary:** This chapter focuses on how national governments control the Internet through the use of coercion within their country as opposed to controlling sources outside the borders.
- **Chapter Discussion:** Chapter 5 opens with a description of the Principality of Sealand and HavenCo's (Sealand's company that equipped the principality with servers) promise to clients of servers that were "physically secure from any legal action."<sup>36</sup> The chapter continues with a discussion of "intermediaries" and how controlling local Internet intermediaries can affect the flow of the Internet within the particular government's borders.<sup>37</sup>

The authors illustrate how a government can control the Internet by using a metaphor pertaining to a transaction of illegal acts. The metaphor divides the transaction of illegal acts into three parties: source, intermediary, and target; and illustrates the parties with a hypothetical involving counterfeit Gucci bags arriving from Thailand which are then sold on the streets of the United States.<sup>38</sup> The authors argue that "effective control over any of the three elements of the transaction permits the government to control conduct within its borders."<sup>39</sup> The chapter then presents different models, strategies, and theories, each with the government regulating one of the three

---

<sup>36</sup> *Id.* at 65.

<sup>37</sup> *Id.* at 68. The authors define local intermediaries as "the people, equipment, and services within national borders that enable local Internet users to consume the offending communication." The authors illustrate government control of Internet intermediaries through other examples of government control such as Bartender's responsibility to prevent drunk driving of their patrons and Pharmacists and Doctors preventing certain kinds of drug abuse.

<sup>38</sup> GOLDSMITH & WU, *supra* note 12, at 69. In the Gucci Hypothetical, the source is the manufacturer, the intermediary is Chinatown, and the target is the purchasers.

<sup>39</sup> *Id.*

specific elements, and the outcome of that particular regulation. As the chapter continues, the authors present what they consider the “primary intermediaries of government control over the Internet,” and discuss how countries such as Germany, France and Britain enacted laws that require intermediaries (primarily Internet Service Providers) to effectively block material from being viewed by their citizens.<sup>40</sup>

The chapter lists examples of control through the use of intermediaries previously described including: government threats to a popular search engine to remove copyrighted documents from the web by threats to that search engine, the crippling of online cigarettes purchases because of government coercion to the major credit card companies, shutting down voting websites by seizing domain names, and finally the direct physical control of the individual.

The chapter closes by describing the issues of “small nations, intermediary minimization, and mixing,” and how the government controls fares in these three areas of avoidance.<sup>41</sup> Finally, the authors present an Epilogue of the demise of Haven Co.

## **Chapter 6 - China**

- **Chapter Summary:** This chapter examines the Chinese Government’s increasing control over the Internet.
- **Chapter Discussion:** Chapter 6 opens by describing three accounts of Internet regulation by the Chinese Government involving citizens who criticized the

---

<sup>40</sup> *Id.* at 73. The authors describe ISPs as “the most important and most obvious gatekeepers to the Internet.”

<sup>41</sup> *Id.* at 81-84. The chapter describes how intermediary control is less effective in small nation areas such as Fiji and Ghana. Further, the chapter discusses the intermediary control of Internet gambling in Antigua and the mixing of protected speech and Internet pornography.

government.<sup>42</sup> China has a sophisticated firewall system, built predominantly by Cisco, which allows the government to block websites outside of its borders, which the government feels should be censored. The Chinese filtering system is described in detail, including what information is blocked and what appears on the blocked site when Chinese citizens attempt to access the site.<sup>43</sup>

The chapter states that American companies play a large role in the censorship of information on the Chinese servers. The particular companies and their methods involved in the censorship are discussed, and an attempt by an independent group to breach the regulation is examined by the authors. The chapter also describes other methods used by the Chinese government to help with the censorship of information.<sup>44</sup>

The chapter closes by reminding readers that one of China's goals is to have the "fastest and most sophisticated Internet network in the world," while maintaining complete control over information.<sup>45</sup> However, not all of China's methods of regulation are accepted by the rest of the world.<sup>46</sup>

---

<sup>42</sup> *Id.* at 87-89. Such accounts include a list describing 44 reasons that Chinese politicians are worse than prostitutes, an essay entitled "How a national security apparatus can hurt national security" which appeared on numerous Internet sites, and a citizen registering under the "China Democratic Party" during a visit by President Clinton.

<sup>43</sup> GOLDSMITH & WU, *supra* note 12, at 95. The authors state that common blocked sites include information pertaining to Tibetan independence groups, human rights sites, religious or spiritual sites, new age churches, and all information related to the banned Falun Gong religious movement.

<sup>44</sup> *Id.* at 97-98. Such methods include requiring bloggers to register with the Chinese government, camera surveillance in Internet cafes, and Internet Commentators in chat rooms.

<sup>45</sup> *Id.* at 100.

<sup>46</sup> *Id.* at 104. China implemented wireless Internet servers, but required registration with a "centralized authentication point" before logging on to the server. This was eventually suspended due to pressure from the U.S. and the World Trade Organization.

## **Chapter 7 – The Filesharing Movement**

- **Chapter Summary:** Chapter 7 analyzes the file-sharing movement, from its origins of free illegal music downloading software such as Kazaa, Napster, and Grokster to the emergence of legal, pay-per-use downloading software such as Steve Jobs' iTunes phenomenon. The chapter also examines the record companies' response to the early software and chronicles the *Metro-Goldwyn-Mayer Studios v. Grokster, Ltd.* litigation.<sup>47</sup> The chapter closes by illustrating how law and government can maintain control of the Internet despite technological change.
- **Chapter Discussion:** Chapter 7 opens by introducing Niklas Zennstrom, the creator of one of the first file-sharing software programs, Kazaa. The chapter describes the recording industry's vulnerability to music copying and distribution and the chapter eventually transitions into a brief description of the Napster program, how filesharing works, and the copyright infringement lawsuit that followed. After Napster's shutdown, another filesharing program, Kazaa, emerged as the "super-peer system," being downloaded close to 319 million times.<sup>48</sup>

Kazaa's and Napster's software are compared and contrasted, and the chapter explains how the popularity of Kazaa led to the Recording Industry Association of America (RIAA) striking back against Kazaa and its cousin, Grokster, by initiating lawsuits. The RIAA's arguments are discussed, as are Kazaa's defenses, and the

---

47. See *MGM Studios, Inc. v. Grokster, Ltd.*, 259 F. Supp. 2d 1029 (C.D. Cal. 2003); *MGM Studios Inc., v. Grokster, Ltd.*, 380 F.3d 1154 (9th Cir. 2004); *MGM Studios Inc., v. Grokster, Ltd.*, 545 U.S. 913 (2005).

<sup>48</sup> *Id.* at 109.

discussion ends with the RIAA losing not only at the lower courts, but also on appeal to the federal appellate court in California.<sup>49</sup>

After analyzing the outcome of the lower court's decision, the chapter proceeds with a discussion regarding Congress's interest in protecting the record industry, and talks about the RIAA's appeal to the Supreme Court of the United States.<sup>50</sup> Before discussing the Court's decision, the chapter describes Kazaa's eventual downfall due to "adware" problems, "sleeper software," and the posting of fake files, all of which led customers to eventually stop using the software.<sup>51</sup>

The chapter ends with the emergence of the iTunes software, describes it, and compares it with Kazaa. The chapter closes by analyzing the Supreme Court's decision in *Grokster* and briefly discusses the emergence of underground and new filesharing technology, such as Bittorent, and an Epilogue about Mr. Zennstrom's fate and future.<sup>52</sup>

### **Part 3 – Vices, Virtues, The Future**

#### **Chapter 8 – Virtues and Vices of Government Control**

- **Chapter Summary:** The chapter explains how government regulation can be beneficial to the Internet and its users, and this point is illustrated through a discussion of the auction website, eBay.com.

---

<sup>49</sup> GOLDSMITH & WU, *supra* note 12, at 109-12. See *MGM Studios, Inc.*, 259 F. Supp. 2d 1029; *MGM Studios Inc.*, 380 F.3d 1154.

<sup>50</sup> See *MGM Studios Inc.*, 545 U.S. 913.

<sup>51</sup> GOLDSMITH & WU, *supra* note 12, at 116-17. The authors describe "adware" as "parasite-like programs that install on users' computer to grab user information or to display ads at the right time." "Sleeper software" was part of idea that a "computer would run in the background on millions of machines, and Kazaa would then sell the computer's time to interested clients."

<sup>52</sup> *Id.* at 121-25.

- **Chapter Discussion:** Chapter 8 opens with a history of eBay.com and a biography of its creator, Pierre Omidyar. After introducing and describing the online auction site, the chapter unfolds with discussions about the early problems eBay faced, such as consumer dissatisfaction, and the preventive measures the website took to help alleviate the conflicts.<sup>53</sup> As the company grew, so did the problems, such as the “Furby Fraud of 1998,” the user who “sold his soul” on eBay and the Rolex scam of 1999.<sup>54</sup> User fraud eventually led to a class action lawsuit five years after eBay landed itself on the web.<sup>55</sup>

With all the problems facing eBay, the company eventually hired two law enforcement officials, and later partnered with an online mediation company to help police the eBay community and to find and prosecute fraudulent users. As the chapter points out, fraud was not the only problem facing eBay. eBay also faced breach of contract problems, as each transaction made on eBay involves a legally binding contract. In addition, eBay has a release from liability agreement that each purchaser must agree to before conducting business on the site. As the chapter states, “by upholding eBay’s release and preventing eBay from being destroyed by lawsuits, government helps make eBay a viable and cost effective service.”<sup>56</sup>

The chapter continues by discussing the necessity of a government where public goods are provided to the community and explains additional benefits government regulation can provide for private groups like eBay. The chapter closes by discussing

---

<sup>53</sup> *Id.* at 131-32. In the early stages of eBay, a user known as “Uncle Griff” would play the role of a mediator to help resolve conflicts between other users.

<sup>54</sup> *Id.* at 133.

<sup>55</sup> *Gentry v. eBay, Inc.*, 121 Cal.Rptr.2d 703 (2002).

<sup>56</sup> GOLDSMITH & WU, *supra* note 12, at 138.

different governments and the laws eBay has faced when dealing in overseas transactions with nations such as the United Kingdom, Germany, and India.<sup>57</sup>

## **Chapter 9 – Consequences of Borders**

- **Chapter Summary:** This chapter explores the concept of the “bordered Internet” and discusses various cases involving communications on the Internet and how they collide with sensitive local public policies.
- **Chapter Discussion:** Chapter 9 begins by describing a defamation case involving Dow Jones & Company, Inc. and Joseph Gutnick, an Australian billionaire.<sup>58</sup> Dow Jones was sued in an Australian court, which did not apply the United States First Amendment. The court found that “the place where the person downloads the material will be the place where the tort is committed.”<sup>59</sup> The case eventually settled, proving that each nation’s laws apply differently to communication on the Internet.

The chapter then describes three reasons that the global Internet is “becoming a collection of nation-state networks.”<sup>60</sup> The authors point to (1) different languages, (2) technological developments, as was seen in China, and finally, (3) the enforcement of national laws, as seen from the above case. A single rule for six billion people using the Internet cannot survive because of these differences, and the world would be, as the

---

<sup>57</sup> *Id.* at 144. The authors describe legal problems such as defamation suits in the United Kingdom when dealing with consumer negative feedback, Nazi paraphernalia in Germany, financial challenges and child pornography problems eBay faced in India when it bought the popular Indian auction site, Baazee.com.

<sup>58</sup> Dow Jones & Company Inc. v. Gutnick, (2002) HCA 56 (10 December 2002), *available at* <http://www.austlii.edu.au/au/cases/cth/HCA/2002/56.html>.

<sup>59</sup> *Id.* at 61.

<sup>60</sup> GOLDSMITH & WU, *supra* note 12, at 149.

authors describe, “divided and discontented.”<sup>61</sup> With a decentralized governance of the Internet, the authors argue, each nation can adapt the Internet to each nation’s own cultures and values.

In addition, the authors point out that a nation will always take the necessary steps to prevent harm within its territory and this does not change if the harm is caused by Internet communication. The authors argue that because companies like Dow Jones purposely avail themselves in nations like Australia, the above result is not unfair to Dow Jones. In fact, “it is the cost of doing business in Australia...Australians need not forgo redressing this harm to one of its citizens in Australia out of deference to the U.S. Constitution.”<sup>62</sup> The authors also argue that Dow Jones can “leave Australia altogether, eliminating its presence and assets there and with them any fear of Australian libel law.”<sup>63</sup>

The chapter closes by discussing the implications of the *Gutnick* decision and reviewing the author’s arguments for a decentralized approach to Internet control.

## **Chapter 10 – Global Laws**

- **Chapter Summary:** The chapter discusses two themes: first, techniques used by nations within their borders to control conduct outside of the borders and second, how problems with the Internet, such as online gambling, domain name governance and privacy laws, can affect international relations with other countries.

---

<sup>61</sup> *Id.* at 152.

<sup>62</sup> *Id.* at 157-58.

<sup>63</sup> *Id.* at 160.

- **Chapter Discussion:** Chapter 10 opens by describing the events leading up to the apprehension of Russian hacker, Alexey Vladimirovich Ivanov, on U.S. soil. The authors detail how important it is to get custody of a “cyber criminal” because without getting custody, the authors argue, “there can be no punishment and no deterrence of future crimes.”<sup>64</sup>

The chapter describes many types of cybercrimes that can occur and the problems that come with trying to prevent them. However, some preventative measures occur globally, such as the Council of Europe’s Cybercrime Convention, which was a treaty that attempted to “outlaw cybercrimes world wide and establish standards for international cooperation in preventing and prosecuting such crimes.”<sup>65</sup> The chapter discusses the treaty, including the reasons for its ratification and its ultimate failure.

The chapter then discusses the Domain Name System’s (DNS) relationship to global law, and provides an in-depth discussion of the present “root authority” naming system, the Internet Corporation for Assigned Names and Numbers (ICANN).<sup>66</sup> The chapter continues its discussion of ICANN by describing the relationship of ICANN with the United States and various efforts to shift the domain name system back under U.S. control.

The chapter closes by examining online gambling and the effects it had on international relations between Antigua and the United States. The authors also provide a discussion regarding privacy laws in the European Union, related predominately to

---

<sup>64</sup> *Id.* A “cyber criminal” is one who commits cybercrimes. A cyber crime is defined by the authors as “occurring when computers on the Internet illegally access or harm files and programs on other computers.”

<sup>65</sup> GOLDSMITH & WU, *supra* note 12, at 166.

<sup>66</sup> *Id.* at 168-70.

Microsoft's "dot-NET Passport," and how the influence of these laws on the Internet "will in many cases be the dominant rule, worldwide."<sup>67</sup>

### **Chapter 11 – Conclusion: Globalization meets Governmental Coercion**

- **Chapter Summary:** The final chapter discusses the effects of government coercion and its influence over the Internet by briefly summarizing the vices and virtues of coercion through examples discussed in previous chapters.
- **Chapter Discussion:** Chapter 11 presents the reader with two specific ideas on globalization: (1) "a recognition that we live in an era where technology has made it easier than ever before to move capital, goods, and services across national borders and around the world," and (2) "that a belief that globalization diminishes the relevance of borders...and thereby undermines the territorial nation-states' roles as a central institution for governing human affairs."<sup>68</sup>

The authors recall previously discussed events of government coercion, including the *Yahoo!* case, the Chinese government's extreme control, "the founders" attempt to regain control from the government, and the rise and fall of illegal file sharing. The authors use these examples to state the overall argument that lives are dominated by social norms and morality, and that these rules and governance cannot "function apart from an underlying system of territorial government and physical coercion."<sup>69</sup> The authors also argue that the Internet was supposed to be a test for community self-

---

<sup>67</sup> *Id.* at 175-76.

<sup>68</sup> *Id.*, at 179.

<sup>69</sup> *Id.* at 181.

governance systems, free from outside governmental regulation, but online communities like eBay.com produced opposite results.<sup>70</sup>

The authors close by articulating how different nations can shape the architecture of the Internet, which in turn influences the future of the Internet in that particular nation. By using coercive powers, each nation, its geography, and the attitudes of the people within the geography can establish different versions of the Internet. The authors conclude that “these factors will do much to determine how life on the bordered Internet is lived.”<sup>71</sup>

**DISCLAIMER: This book review is not intended to infringe on the copyright of any individual or entity. Any copyrighted material appearing in this review, or in connection with the *Syracuse Science & Technology Law Reporter* with regard to this review, is disclosed and complies with the fair or acceptable use principles established in the United States and international copyright law for the purposes of review, study, criticism, or news reporting. The views and opinions expressed in the reviewed book do not represent the views or opinions the *Syracuse Science & Technology Law Reporter* or the book reviewer.**

---

<sup>70</sup> GOLDSMITH & WU, *supra* note 12, at 181-82.

<sup>71</sup> *Id.* at 184.