Protecting Copyrights at the "Backbone" Level of the Internet

By Joseph D. Schleimer*

I. INTRODUCTION

The survival of copyright in the digital age can only be assured through the implementation of technical measures to block infringements at the backbone level of the Internet. The music industry experience since the onset of Napster makes this clear. After major court victories,[1] a few judicial setbacks,[2] some aggressive electronic counter-

* Joseph D. Schleimer is an entertainment litigator and a member of Schleimer & Freundlich LLP, in Beverly Hills, California.

[1] Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005); A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

[2] *In re* Charter Communications, Inc., Subpoena Enforcement Matter, 393 F.3d 771 (8th Cir. 2005) ; Recording Indus. Ass'n of America, Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229 (D.C.Cir. 2003); Patrick Van Eecke & Maarten Truyens, *EU P2P Trials Adrift*, J. IN-

measures,[3] and the filing of more than 25,000 lawsuits,[4] illegal music downloads now exceed 20 billion infringements annually,[5] and the number of households engaged in illegal file-sharing is still increasing.[6]

The impact on the music industry has been catastrophic. Worldwide revenue, which peaked at $45 billion in 1997, is projected to fall to $23 billion by 2009, and approximately half the people employed in the music industry a decade ago have been laid off.[7] With no end in sight for the revenue free-fall, most of those who still have jobs have polished up their resumes. The implosion of the music industry, however, is merely a harbinger for what awaits the motion picture/television industry as download speeds increase.

The Internet *should* be the most profitable distribution medium the entertainment industries have ever enjoyed. Instead, the mass shoplifting spree launched by Napster, Grokster, Aimster, Kazaa, Bit Torrent, et al., has spawned a youth culture which holds copyright law in contempt. "Music should be free" has become the mantra for an entire generation, and many young people feel foolish if they pay for recorded entertainment. Downloads of hit songs sell for 99 cents, as opposed to $1.99 or $2.99, not because 99 cents is fair market value, but rather, to compete with illegal free downloads.

The potent combination of high speed Internet access, personal computers, and devices such as the iPod, has placed the technology of mass copyright infringement at the disposal of hundreds of millions of consumers. As a result, the incentive structure of intellectual property law, developed over centuries, is in jeopardy.

The law of copyright must be enforced electronically by the Internet Service Providers ("ISPs") who operate the Internet and its backbone. Otherwise, copyright as we know it will cease to exist. The purpose of this article is to explore some of the legal and technical issues likely to arise in bringing intellectual property "law and order" to the Internet.

TERNET L., Jan. 2007, at 19; Patrick Van Eecke & Maarten Truyens, *Dutch Court of Appeal Rejects Request to Expose File Swappers Identities*, J. INTERNET L., Sept. 2006, at 19.

[3] Andrew Ross Sorkin, *Software Bullet is Sought to Kill Musical Piracy*, N.Y. TIMES, May 4, 2003, at 1; Joseph D. Schleimer, *Electronic Countermeasures Against Copyright Infringement on the Internet: Law and Technology*, J. INTERNET L., Nov. 2001, at 1.

[4] Joe Hernick, *Beware the Copyright Cops B It doesn't pay to mess with the RIAA*, INFO. WEEK, Jan. 28, 2008, at 53.

[5] STEPHEN E. SIWEK, Institute for Policy Innovation, The True Cost of Sound Recording Piracy to the U.S. Economy, Policy Report 188, 6-7 (Aug. 21, 2007)

[6] Cary Sherman, *The Rights and Wrongs in the Antipiracy Struggle*, CNET NEWS, Oct. 16, 2007

[7] ENDERS ANALYSIS, RECORDED MUSIC AND MUSIC PUBLISHING (Mar. 23, 2007)

II. CONTROLLING THE BACKBONE

It is often said that regulating the Internet is impossible because of its chaotic structure, which consists of hundreds of millions of computers connected by cables, radio transmission links, servers and routers. These computers send trillions of messages to each other every day, and the massive data flow is often referred to as a "cloud" due to its atomized structure, which involves millions of routes for information to travel in tiny packets.

Despite its unruly nature, there are interconnection points where the Internet bit stream can be monitored, and copyright infringements can be detected, filtered, and blocked.[8] Professor Jonathan Zittrain of Oxford University has studied and catalogued these technological gateways, which he calls the "Internet Points of Control."[9] Steven J. Murdoch and Ross Anderson of the University of Cambridge refer to them as "choke points," where surveillance and filtering mechanisms can be positioned.[10]

The implementation of backbone-level technology to block copyright infringement would undoubtedly face legal challenges under the First and Fourth Amendments to the U.S. Constitution, privacy laws and anti-wiretapping statutes. Complex issues are also likely to arise under the immunity provisions of the Digital Millennium Copyright Act[11] ("DMCA") and the member-state implementation acts stemming from the European Community Directives on Copyright and Electronic Commerce.[12]

Precedent for the imposition of filtering technology on particular web sites has already been set by American courts, including the U.S. Supreme Court.[13] There is also at least one foreign precedent for imposing the electronic filtering of copyright infringements on an ISP through court action.[14]

---

[8] Jonathan Zittrain, *A History of Online Gatekeeping*, 19 HARV. J.L. & TECH. 253, 256 (2006).

[9] Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653 (2003)

[10] Steven J. Murdoch & Ross Anderson, *Tools and Technology of Internet Filtering, in* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 57, 65 (2008).

[11] 17 U.S.C. § 512 (2000).

[12] Council Directive 2001/29/EC on Copyright of 22 May 2001, art. 5(1); Council Directive 2000/31/EC on Electronic Commerce of 8 June, 2000, arts. 12B15.

[13] United States v. American Library Ass'n, Inc., 539 U.S. 194 (2003); A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002); Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 454 F. Supp. 2d 966 (C.D. Cal. 2006).

[14] Sabam v. S.A. Tiscali (Scarlet), District Court of Brussels No. 04/8975/A (2007), English translation published at 25 CARDOZO ARTS & ENT. L. J. 1279 (2008).

III. Private Sector Enforcement of Copyrights

The initiative to use technology to protect copyrights online should come from the private sector, for several reasons.

First, the Internet backbone is owned, controlled and operated by private, semi-private, and multi-national companies, who coordinate their systems through compacts and a web of cooperative arrangements and have a record of efficiency and innovation. By contrast, political control over the Internet is fragmented among hundreds of overlapping jurisdictions, and none of the scores of governments involved with the Internet have the ability to control the entire system, a condition which has been described as "cyberanarchy."[15] As a result, the most practical means to organize technological copyright protection at the backbone level is to do so through the private sector.

Second, any effort to protect copyrights online will fail without the active support of the major technology companies. They alone possess the necessary hardware and know-how to make such protection work, so their support is essential to success. These companies will provide the services their customers demand, and their customers are the ISPs.

Third, the only precedent for imposing any kind of global governance on the Internet was achieved through privatization, when the Clinton administration delegated "root authority" to the Internet Corporation for Assigned Names and Numbers ("ICANN"), a non-profit corporation. ICANN is the prototype, and could even serve as the nucleus, for a private, world-wide authority for the protection of copyrights online through the use of technical means.

Fourth, a system of private, Online Dispute Resolution ("ODR") will be essential for Internet blocking to conform to law. ICANN has already created an ODR system to adjudicate domain name disputes,[16] and it functions with great success. Since ICANN arbitration awards are enforced by technical measures, a similar system should be employed to resolve Internet copyright issues related to blocking and unblocking.

Fifth, from a logistical standpoint, the private sector has already established world-wide global cooperatives to combat computer viruses, and those organizations employ the same kind of fingerprinting, filtering and blocking technology which would be used to protect copyrights.

---

[15] Jack L. Goldsmith, *Against Cyberanarchy*, in Who Rules the Net? Internet Governance and Jurisdiction 31 (2003).

[16] ICANN Uniform Domain Name Dispute Resolution Policy, http://icann.org/dndr/udrp/policy.htm (updated Feb. 17, 2002).

At the forefront in this field is Cisco Systems, headquartered in San Jose, California, which owns and operates the Ironport Threat Operations Center, collecting computer virus intelligence from 100,000 contributing organizations around the world. Through Ironport, Cisco already has a "view" into 25% of global e-mail traffic, and uses that intelligence to offer dynamic virus filtering systems which can quickly respond to emerging threats on a global scale.[17]

Symantec, Inc., of Cupertino, California, has its own Global Intelligence Network, which gathers information from more than 120,000,000 client, server and gateway systems. It has more than 40,000 sensors operating in 180 countries, and the agility to respond rapidly, and globally, to new virus threats.[18] These are exactly the kinds of world-wide operational capabilities which would be needed to protect copyrights online.

Sixth, a number of ISPs and technology companies are providing services to national governments which censor the Internet. As a result, they have experience and technology which could be adapted to protect copyrights.

The most tightly controlled censorship regime is operated by the People's Republic of China, which blocks Internet materials the Chinese government considers seditious or harmful. China contracted with Cisco Systems, Nortel Networks, Sun Microsystems and 3COM for what has been nicknamed the "Great Firewall of China," a massive filter system operating at the backbone level of the Chinese Internet.[19]

The technology companies insist that all they do is sell hardware and software and comply with Chinese law, and deny any moral responsibility for the manner in which the Chinese government uses their wares.[20] However, Cisco and its competitors also provide support services, so it is implausible that they have not played an active role in (and gained invaluable experience from) the use of their technology for

---

[17] CISCO/IRONPORT, 2008 INTERNET SECURITY TRENDS: A REPORT ON EMERGING ATTACK PLATFORMS FOR SPAM, VIRUSES AND MALWARE (2008); *see also* linked support materials on *Ironport Virus Outbreak Filters*, www.ironport.com.

[18] SYMANTEC, INTERNET SECURITY THREAT REPORT, TRENDS FOR JANUARY-JUNE 2007 (Sept. 2007).

[19] OPEN NET INITIATIVE (ONI), INTERNET FILTERING IN CHINA 2004B2005: A COUNTRY STUDY, 3, 6-8 (Apr. 14, 2005). The Open Net Initiative is a collaboration of the Citizen Lab at the Munk Centre for International Studies, University of Toronto; the Berkman Center for Internet & Society at Harvard Law School; and the Advanced Network Research Group at the Cambridge Security Programme (Centre for International Studies) at the University of Cambridge. The Report was a team effort, led by principal investigators Jonathan L. Zittrain and John G. Palfrey, Jr. *See also,* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET: ILLUSIONS OF A BORDERLESS WORLD 93 (2006).

[20] Rebecca MacKinnon, *China's Internet: Let a Thousand Filters Bloom*, YALEGLOBAL, June 28, 2005.

censorship of the Chinese Internet. Irrespective of whether Cisco and the other companies have turned a blind eye to the misuse of their technology, the fact remains that these companies possess the technical capability and know-how to adapt their censorship technology for use in protecting copyrights.[21]

For "carrot and stick" reasons, certain private sector entities have already begun implementing online filtering. On the "stick" side of the equation, under the spur of Viacom's multi-billion dollar infringement lawsuit, Google has announced implementation of "digital fingerprinting" software, to filter out copyright infringements on its YouTube subsidiary.[22]

On the "carrot" side, AT&T, a major backbone and consumer ISP, has a business plan to distribute copyrighted works to its customer base, and has been investigating and publicly advocating the voluntary implementation of filtering to block copyright infringements.[23] As discussed below, this business approach is likely to spread to the other major ISPs, all of whom, for competitive reasons, must begin licensing and distributing entertainment content, or risk being trampled by the competition.

Comcast, another major backbone ISP, implemented technical measures to reduce the undue consumption of bandwidth caused by peer-to-peer transfers of video files.[24] The traffic-management justification for throttling peer-to-peer users was strongly supported by a German survey, which estimated that file-sharing constitutes 50% to 90% of total Internet traffic.[25] The ISPs and the backbone providers are just now waking up to the realization that this massive bandwidth,

---

[21] Cisco has supplied China with highly sophisticated backbone routers which are capable of bi-directional packet inspection, with the ability to apply 750,000 "filtering rules." ONI, *supra* note 19, at 7.

[22] Miguel Helft, *Google Tries System to Halt Video Pirating*, INT'L HERALD TRIBUNE, Oct. 17, 2007.

[23] Rob Preston, *Amid All the Talk of Big Brother, A Bigger Mistake*, INFO. WEEK, Jan. 28, 2008, at 64; Tim Barker, *AT&T's Idea to Monitor Net Creates a Web of Suspicion*, ST. LOUIS POST-DISPATCH, Feb. 14, 2008, at A1; Laura M. Holson, *Hollywood, Silicon Valley and AT&T? It's a Deal*, N.Y.TIMES, Mar. 3, 2008, at C1; Brad Stone, *AT&T Considers Filtering Internet*, N.Y. TIMES, Jan. 14, 2008, at C6.

[24] Peter Svensson, *Traffic Control: Internet Undergoes Changes As Service Providers Struggle With Demands of Web Video*, PITT. POST-GAZETTE, Feb. 16, 2008, at A7; Dan Mitchell, *Sharing is Never Easy*, N.Y. TIMES, Oct. 27, 2007, at C5 ("[A]n anonymous Comcast executive admitted that in some cases peer-to-peer file-sharing traffic like that generated by BitTorrent, is delayed, though not blocked.")

[25] Peter Svensson, *Study: Comcast Actively Hinders Subscribers= File-Sharing Traffic*, SAN MATEO COUNTY TIMES, October 22, 2007.

instead of being used for copyright thievery, should be generating huge distribution fees for the ISPs and backbone providers.[26]

In the past, the technology companies have lined up against the protection of copyrights online because they had a strong incentive to adopt that position. The explosive growth of the Internet, and with it, the ISPs, has been fueled by file sharing and the wide availability of free content on the peer-to-peer services. The massive free-for-all touched off by Napster, and carried forward by its successors, has been a bonanza for the computer industries, which have made record profits selling hardware and Internet access. How many iPods have been purchased to listen to songs illegally downloaded from file sharing services? How much broadband service has been subscribed to for the same reason?

That era, however, is coming to a close, as the *sine qua non* for continued success on the world wide web is now content. To use the aphorism commonly ascribed to Viacom Chairman Sumner Redstone, "content is king." This was underscored by a recent deal between AT&T and Hollywood's largest talent agency, the William Morris Agency, described by the New York Times as "an indication of how quickly online and mobile entertainment are transforming. . .[and] a recognition. . .that a failure to act now could leave the partners vulnerable to interlopers who seek to upend their traditional businesses."[27] This trend was also observed by Sun Microsystems Chairman Scott McNealy, who recently stated, "I have explained to every telco that either you become a destination site, or the destination site will become a telco. . . "[28]

What determines the success of a destination site is content, and the most attractive content is copyrighted. As Internet access becomes available from competing providers, the marketplace is evolving into a competition for eyeballs. As a competitive matter, the ISPs must start licensing entertainment content or risk a loss of their customer base to competitors who do provide entertainment.

Once the ISPs cross the threshold and become content distributors, they will be transformed into copyright stakeholders, and will have to enforce copyrights or have their licensed assets undercut by piracy. Why pay to license episodes of *Seinfeld*, if the same episodes are availa-

[26] Under pressure from the FCC, Comcast has since formed an alliance with Bit Torrent and plans to implement a "protocol agnostic" system of traffic management. Deborah Yao, *Comcast Will Treat BitTorrent Traffic Equally*, Associated Press, Mar. 27, 2008.

[27] Holson, *supra* note 23.

[28] Agam Shah, *McNealy: Telcos Falling Behind in Internet Race*, INFOWORLD, Feb. 28, 2008.

ble on YouTube? No ISP is going to want to allow the use of its "fat pipes" to transmit copyright infringements, when it is paying license fees (or sharing advertising revenue) to deliver copyrighted materials to its customers.

The ISPs have thus far allowed mass infringements to pass through their systems under the cover of immunity conferred on them by the DMCA and the European Community Directives.[29] However, that immunity requires the ISPs to maintain their pure virgin status as mere conduits, a posture they cannot maintain and at the same time operate web sites which deliver massive quantities of illegal content.

Viacom, Inc. v. YouTube, Inc., filed in 2007 in the Southern District of New York, should put to the test the question whether "mere conduit" status will be available as a defense for web sites which host mass copyright infringements. Before filing the lawsuit, Viacom served 150,000 "take down" notices under the DMCA, covering tens of thousands of infringements which had been posted on YouTube by the public.[30]

Notices under the DMCA force the web site host to "expeditiously" cull noticed infringements, or lose statutory immunity. 17 U.S.C. § 512(c). The volume of notices served by Viacom reflects the fact that contumacious members of the public would simply re-post the deleted videos. In response, Viacom hired BayTSP, Inc., of Los Gatos, California, to send webcrawlers onto the YouTube web site, generating a massive quantity of take-down notices in the months before the lawsuit was filed.[31]

When robotically-generated take down notices arrive by the tens of thousands, the web site operator must either automate the takedown, or use manual compliance methods and risk loss of immunity under the DMCA, which requires the takedown to be expeditious.[32] Looked at another way, the Viacom case demonstrates that by using robotic spiders to locate infringements and electronically generate take

---

[29] The DMCA was designed to transform Copyright from a printing-press-age doctrine focused on the right to *copy* a work, into a digital age law which gives the rights holder the exclusive right to *control access* to the work. *See* Jane C. Ginsburg, *Copyright and Control Over New Technologies of Dissemination*, 101 COLUM. L. REV. 1613, 1635B1636 (2001).

[30] Complaint at 3, Viacom Int'l, Inc., v. YouTube, Inc., No. 07CV2103, 2007 WL 775611 (S.D.N.Y. Mar. 13, 2007) [hereinafter Viacom Complaint].

[31] Ellen Lee, *Hunting for Pirated Clips a Growing Industry: Clients Like Viacom Want Search of Online Video-Sharing Services*, FT. WAYNE J. GAZETTE (IND.), Mar. 25, 2007, at 3H.

[32] 17 U.S.C. § 512(c) (2000). *See also* Council Directive 2000/31/EC of the European Parliament, 8 June, 2000, art. 14 (instructing the EC member states to provide "hosting" immunity, and conditioning such immunity on the service provider "expeditiously" removing or disabling access to infringements whenever it becomes *aware* of the infringement).

down notices, copyright holders can externally impose a form of technical filtering.

If the web site host is profiting from the infringements, it may be tempted to hinder robotic scanning, erect barriers to the service of automated take down notices, and shield file-sharing customers through the creation of closed systems, or "dark nets," which cannot be externally monitored for copyright infringement. However, employing such countermeasures constitutes strong evidence of scienter, and could render the ISP liable for willful infringement. 17 U.S.C. § 512(c)(1). In fact, in its Complaint, Viacom specifically alleges the countermeasures employed by YouTube, including "hidden" videos (those embedded in other web sites), rules and functions which hinder robotic scanning, and implementation of dark net-style applications.[33] Based on these tactics, Viacom averred willful infringement, potentially allowing Viacom to collect statutory damages of up to $150,000 per infringed work. 17 U.S.C. § 504(c). Multiply that by the tens of thousands of infringed works which appear on sites like YouTube, and it is clear that any ISP host allowing its web site to be used as a bazaar for copyright infringement risks being robotically policed, deluged with DMCA notices, and sued for billions of dollars.[34]

So the tide has turned, and ISP operators who contemplate exploiting the mass infringement of copyrights to drive their business should start implementing technical measures to defeat their own illicit business plan, else they may find their statutory immunity under the DMCA is illusory.

IV. UNDERBLOCKING, OVERBLOCKING, CIRCUMVENTION & AGILITY

The technical challenge in protecting copyrights at the backbone level is complicated by the problems of underblocking, overblocking, and circumvention.

Circumvention must be combated through the use of countermeasures with "agility," that is, there must be a rapid response to each new circumvention as it arises. To have agility requires a command center and the same kind of detection and rapid response capabilities organized to combat computer viruses.

---

[33] Viacom Complaint, at § 8, 42-43.

[34] The DMCA does not include a notice/takedown procedure for transitory and caching systems. *See* 17 U.S.C. §§ 512(a)-(b) (2000). As such, this tactic is only effective for *hosting* ISPs.

Underblocking is a problem only in the sense that the filtering regime must block enough infringements to effectively frustrate and deter infringers. Total blocking is impossible, but partial blocking will greatly bolster copyrights. If the system hinders enough infringement attempts to make it too much work to steal, consumers will be driven to acquire copyrighted materials legally.

Overblocking is by far the most important technical challenge, for several reasons. First, the blocking system must permit the authorized distribution of copyrighted works, such as licensed downloads and authorized streaming. If the Internet is configured to block passage of copyrighted materials, a "key" system must operate across the controlled elements of the Internet to allow legal transmissions to pass. That requires coordination among a great many entities, and some form of central control.

Second, hackers will diligently reverse engineer the block-and-key system and seek to exploit holes in the protocol. Hence, the technology must be "dynamic" (agile), and remain one step ahead of the criminals and hackers. As with viruses, this can only be dealt with by a centralized command and control system for detection, analysis and response.

Finally, there must be a protocol so fair use transmissions and materials in the public domain can be unblocked at the request of parties with a legitimate objection to blocking. That means an administrative entity must be created to key fair uses through the system, and an adjudicative system must be available when there is a dispute about such matters. The only practical means for most of these adjudications would be some form of ODR.

V. JURISDICTION OVER THE INTERNET

Current governmental jurisdiction over the Internet consists of a global patchwork of overlapping, territorial authorities. Under the "long arm" doctrine,[35] judicial power can be, and sometimes is, exercised across jurisdictional lines.[36] However, Internet governance, to the extent it exists at all, is fragmented across hundreds of geopolitical

[35] John Di Bari, *A Survey of the Internet Jurisdiction Universe*, 18 N.Y. INT'L L. REV. 123 (2005).

[36] *See, e.g., Gutnick v Dow Jones & Co.* [2001] VSC 305 (28 Aug. 2001), appeal dismissed *Dow Jones & Co. v. Gutnick* [2002] HCA 56 (10 Dec. 2002), where the Australian courts allowed a defamation lawsuit to proceed against a New York-based publication because there were 1700 subscribers who used Australian credit cards to access the web site.

boundaries, with no single authority having the ability to regulate the Internet system-wide.[37]

The sole exception to this anarchistic situation is jurisdiction over the internet "root," which the U.S. government tenuously controls through an authorization contract between ICANN and the U.S. Department of Commerce.

The U. S. claim to root authority dates back to the 1960s, when the Advanced Research Projects Agency ("ARPA"), a unit of the U.S. Department of Defense ("DOD"), financed the research and development leading to the creation of the Internet. Originally known as the ARPANET, the system was devised as a Cold War communications system which could (at least in theory) survive a nuclear exchange with the Soviet Union.[38]

Pre-ARPANET communication systems depended on telephone lines and "circuit switching," whereby switches opened a continuous circuit between the caller and receiver.[39] Switched circuits are broken if any part of the circuit is destroyed. The ARPANET was invented as a distributed, "packet-switching" system, whereby computer communications are broken down into small bundles, or "packets," which are transmitted separately, then reassembled at the receiving end. The packets could follow a myriad of pathways, and would be automatically re-routed around any segment of the path which was interrupted.[40] In theory, a message would reach its destination if any pathway still remained open. Thus, if Chicago was destroyed by a thermonuclear explosion, an ARPANET message could still transit from Los Angeles to Washington D.C. by way of St. Louis, or New Orleans, or Atlanta.

The ARPANET, and its successor, the Internet, are based on packet switching, whereby communications are chopped up into small bundles (packets) which are transmitted separately, then reassembled at the receiving end. Each packet consists of an address header (with

---

[37] As summarized by the FCC: "No single entity controls the Internet; rather, it is a worldwide mesh or matrix of hundreds of thousands of networks, owned and operated by hundreds of thousands of people." FCC Internet Policy Statement 05-151, September 23, 2005.

[38] JANET ABBATE, INVENTING THE INTERNET 8-46 (1999).

[39] J.R. OKIN, THE INTERNET REVOLUTION: THE NOT-FOR-DUMMIES GUIDE TO THE HISTORY, TECHNOLOGY, AND USE OF THE INTERNET 129-130 (2005).

[40] ABBATE, *supra* note 38, at 37B41. In a packet-switching system, the individual packets may take very different routes. If the connection between any two nodes is congested, or severed by an atomic bomb, the routers will simply send the packets along different pathways, until they reach their destination. This technology tends to frustrate any efforts to censor or block, because the system logic may view filtering as damage and instinctively try to route the packets around it. WENDY M. GROSSMAN, FROM ANARCHY TO POWER: THE NET COMES OF AGE 57 (2001).

delivery instructions) and a payload of content. The packets are dispatched by the sender's computer, then forwarded node to node by a series of router computers until they reach the correct address, where the packets are aggregated to re-create the complete message.

The ARPANET connected together computer networks which used divergent operating software, so special ("IP/TCP") protocols were devised, which allowed different computer systems to communicate with each other.[41] As a result of the invention of the IP/TCP protocols, it became practical for academic, business and military computers to be interconnected and make use of each other's databases and computing resources. Thus, it was an American invention, developed and implemented with U.S. tax dollars, which formed the technological foundation for the Internet.

As more computer systems were connected to the ARPANET, the growth of the system began to accelerate, and its resources became enhanced, making it still more attractive for additional networks to join. As a result, traffic over the ARPANET grew very rapidly. Additionally, as part of a shift to civilian control, in 1983 the DOD split its Internet activities into the classified MILNET and the civilian ARPANET.[42]

In the mid-1980s, the National Science Foundation ("NSF"), a U.S. Government agency, began spending hundreds of millions of taxpayer dollars to build the NSFNET, which was linked together by a backbone of high-speed cables.[43] This system quickly replaced the aging ARPANET, which was permanently shut down in 1990.[44]

Early in the history of the Internet, a system was devised to give *addresses* to the computers and resources on the system. Using the IP address system, one can access a particular computer or resource by entering an IP address number, e.g., 205.178.190.46. To keep track of all the IP numbers, a root directory was created. The directory was originally maintained in a single file at the Stanford Research Institute ("SRI"). However, as the number of computers using the system grew, so did the root file, and having the file on a single computer caused a bottleneck. To keep the system functioning, engineers distributed exact copies of the master root list of IP addresses to server computers at

---

[41] "IP" stands for Internet Protocol, a system of addressing the individual packets. The receiving computer has a unique IP Address, so the inclusion of the IP address in the packet header ensures delivery to the correct destination. "TCP" refers to Transmission Control Protocol, a standard software which ensures that all of the computers along the Internet pathway will be able to read and use the IP Address correctly.

[42] OKIN, *supra* note 39, at 104.

[43] MILTON L. MUELLER, RULING THE ROOT: INTERNET GOVERNANCE AND THE TAMING OF CYBERSPACE 85 (2002); ABBATE, *supra* note 38, at 191.

[44] OKIN, *supra* note 39, at 103.

multiple locations, and the subsidiary root servers were updated frequently. Thus, the Internet root system was born.

Since it is difficult to remember (and correctly type) a long number, the Domain Name System ("DNS") was devised in 1983, which allowed the use of text domain names (also known as Uniform Resource Locators, or "URLs") to express an IP address.[45] With the DNS system in operation, instead of key punching "205.178.190.46," a user could type the domain name "Schleimerlaw.com," whereupon a DNS name server computer would consult its cached copy of the root directory, translate "Schleimerlaw.com" into "205.178.190.46," and direct the transmission to the computer-readable number.[46]

When a domain name is registered, it is published in the worldwide system of name-server directories (the DNS system), and it is this listing which enables the servers to translate the domain name into the computer-readable number. A web site only becomes visible to other computers on the Internet when its domain name is registered and listed in the DNS system. Ergo, if a domain name is removed from the DNS directories, then the web site effectively disappears, because the name server computers no longer have the ability to translate the domain name into a numerical IP address. In practical terms, what that means is, DNS deletion can be used for blocking. For example, if a domain name like "steal.music.com" was deregistered, the web site could still be accessed by typing in the numerical IP address, but typing in "steal.music.com" would no longer work. Thus, a form of system-wide banishment can be implemented by the party which controls the DNS system.

Control over the root in the early years was maintained by Jonathan Postel, at the USC Information Sciences Institute ("ISI").[47] As the system grew, the academic researchers, led by Postel and a faction of founding Internet engineers, created the Internet Assigned Numbers Authority ("IANA"), which parceled out IP addresses and domain names.[48] From its inception, it was Mr. Postel who actually ran the IANA.

Overhanging this ad hoc system of control was the United States Government, which was still funding the American engineers and con-

[45] Harold Feld, *Structured to Fail: ICANN and the "Privatization" Experiment*, in WHO RULES THE NET? INTERNET GOVERNANCE AND JURISDICTION 333, 336 (2003) (early Internet engineers developed the domain name system because "human beings do not remember long strings of numbers very well. . . .").

[46] GROSSMAN, *supra* note 40 at 42-43.

[47] TIMOTHY BERNERS-LEE, WEAVING THE WEB: THE ORIGINAL DESIGN AND ULTIMATE DESTINY OF THE WORLD WIDE WEB 127 (1999).

[48] *Id.* at 127-128.

sidered the growing Internet to be subject to plenary U.S. Government jurisdiction. The question of legal control became gradually more ambiguous as foreign scientists, foreign institutions, and multi-national commercial interests connected their computer systems to the NSFNET, but the U.S. Government still considered itself to be the owner of the Internet, which had its birth as a government program.

The final transformation of the Internet into a mass consumer medium was the result of two major events: commercialization and implementation of the Hyper Text Transfer Protocol ("HTTP") and Hypertext Markup Language ("HTML"), which made the Internet user friendly.

HTTP and HTML were created by Timothy Berners-Lee with the help of his colleagues at the Conseil Européan pour la Recherche Nucléaire ("CERN"), of Geneva, Switzerland.[49] The invention of HTTP and HTML led to creation of the "world wide web,"[50] and the CERN scientists were instrumental in creating the World Wide Web Consortium ("WWWC"), a standards-setting entity which actively promoted HTTP and HTML.

Before HTTP and HTML, engineers and hobbyists were the only people on the Internet, because the user had to know at least one computer language and give instructions to the computer by typing text commands, using a specialized syntax. With the advent of HTTP and HTML, the system could be operated with a mouse, using icons, hyperlinks, dialog boxes, and browser software. All of a sudden, it was possible for ordinary people to "go on line," and hundreds of millions of people did just that.[51]

As their inventions led to the rise of a new mass medium, the European scientists at CERN naturally wanted to play a role in Internet governance, as did many of the other international players in the rapidly-expanding system. However, root authority remained in the grip of the U.S. Government, which delegated its administrative functions to three U.S. entities, the IANA, the Information Sciences Institute ("ISI") of the University of Southern California, and Network Solutions, Inc. ("NSI"), a Virginia corporation. Through the 1990s, these entities collectively operated the root server system and controlled the DNS, and they did so pursuant to U.S. Government contracts. This sit-

[49] ABBATE, *supra* note 38, at 214-216.

[50] JOHN DAVIES, RUDI STUDER & PAUL WARREN, SEMANTIC WEB TECHNOLOGIES: TRENDS AND RESEARCH IN ONTOLOGY-BASED SYSTEMS xi-xii (2006).

[51] OKIN, *supra* note 39, at 109-110

uation was characterized by Professor Timothy Berners-Lee as "U.S.-centric."[52]

In May, 1991, the NSF amended its Acceptable Use Policy and began allowing commercial use of the Internet.[53] This step, combined with implementation of user-friendly software, touched off a period of exponential growth for the Internet.[54] As the Internet became a mass medium with unlimited commercial potential, a number of private ISPs began offering backbone services,[55] transmission links spread across the globe like a spider-web, and more foreign networks linked in.

The international contingent, especially the Europeans, became increasingly resistant to American control over the Internet root.[56] This discontent was shared by the original "Internet Community," described as "an amorphous network of geeks,"[57] who had long exercised a loose jurisdiction over the root through the IANA. Most of the prominent members of the "geek" faction, led by Jonathan Postel, favored transferring root authority to an international organization. In 1997 an ad hoc committee was formed through an alliance between members of CERN, elements of the European Union, the International Telecommunications Union, and certain ISPs.[58] The committee drafted a Memorandum of Understanding ("MoU"), and the Postel group held a formal signing ceremony in Geneva, Switzerland.[59] The MoU purported to establish an international agreement for assuming control over the Internet root, and the committee unilaterally asserted root authority without the consent of the U.S. Government.[60]

Certain aggressive Internet entrepreneurs, and some members of the geek faction, also began to use self-help to wrestle control of the root away from the U.S. Government, including a successful hack of the root server system which lasted for five days,[61] and the formation of alternate root systems.[62] These efforts came to a head in 1998, when Jonathan Postel used his administrative role at ISI, his engineering authority as de facto supervisor of the DNS system, and his status as the so-called "God of the Internet," to stage a virtual coup, unilaterally

---

[52] BERNERS-LEE, *supra* note 47, at 129

[53] MUELLER, *supra* note 43, at 86, 105-106.

[54] ABBATE, *supra* note 38, at 197

[55] *Id.* at 198-200

[56] MUELLER, *supra* note 43, at 150-51; ABBATE, *supra* note 38, at 211-212.

[57] MUELLER, *supra* note 43, at 103.

[58] GROSSMAN, *supra* note 40, at 48-51.

[59] MUELLER, *supra* note 43, at 146.

[60] GOLDSMITH & WU, *supra* note 19, at 38-40.

[61] MUELLER, *supra* note 43, at 154.

[62] *Id.* at 148-149, 152-153; GROSSMAN, *supra* note 40, at 46.

redirecting most of the secondary root servers away from the authoritative "A" root server, which was operated for the U.S. Government by Network Solutions.[63]

The U.S. Government had maintained a benign attitude toward the aforementioned groups, but collectively these actions threatened fragmentation of the Internet. After bringing an end to Postel's coup, Ira Magaziner, a prominent advisor to President Clinton, publicly announced that any further attempts to use self-help to divert control of the root would be regarded as a criminal matter.[64]

On July 1, 1997, President Clinton issued a directive instructing the Secretary of Commerce to privatize the Internet root and promote international participation.[65] On February 20, 1998, the U.S. Department of Commerce published a "Green Paper," and requested comments on restructuring the Internet.[66] Hundreds of comments were received from academics, businesses, ISPs and foreign interests, followed by conferences, lobbying, and negotiations.

On June 3, 1998, the National Telecommunications & Information Administration ("NTIA"), a unit of the U.S Department of Commerce, issued a "White Paper," calling for the transfer of root authority to a private entity, with an international board of directors.[67] Thereafter, ICANN was formed as a California non-profit corporation, and on February 26, 1999, ICANN entered into a formal agreement with the U.S. Department of Commerce, which provided for the following delegation of functions:

> a. Establishment of policy for and direction of the allocation of IP number blocks;
> b. Oversight of the operation of the authoritative root server system;
> c. Oversight of the policy for determining the circumstances under which new top level domains would be added to the root system;
> d. Coordination of the assignment of other Internet technical parameters as needed to maintain universal connectivity on the Internet; and
> e. Other activities necessary to coordinate the specified DNS management functions, as agreed by the Parties.[68]

---

[63] MUELLER, *supra* note 43, at 161-162.

[64] MUELLER, *supra* note 43, at 162.

[65] *Id.* at 157.

[66] 15 CFR, Chapter XXIII at 8825, Docket No. 980212036

[67] United States Department of Commerce, National Telecommunications & Information Administration, Management of Internet Names and Addresses, Docket No. 980212036-8146-02, June 3, 1998. *See also* MUELLER, *supra* note 43, at 172-175.

[68] Memorandum of Understanding between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers, http://www.icann.org/general/icann-mou-25nov98.htm.

Significantly, the computer which holds the authoritative root file continues to be operated by Verisign (successor to and former owner of Network Solutions), pursuant to a contract with the U.S. Government. Furthermore, ultimate root authority has never been transferred to ICANN,[69] and the privatized root has been operated by ICANN for the past nine years pursuant to a written contract with the U.S. Department of Commerce. Because that contract periodically comes up for renewal, ultimate root authority officially remains within the jurisdiction of the U.S. Department of Commerce.[70]

The U.S. Government's continuing control over the root is actually based on the power of incumbency. At any time, foreign governments and ISPs could withdraw from the American-controlled root, or form their own root. They refrain from doing that out of fear of splitting the root, which would cause the Internet to lose connectivity and disintegrate. As explained by prominent media attorney Harold Feld:

"[T]he vast majority of the technical and policy community view splitting the root as the ultimate collapse of Internet stability and a potential doomsday scenario for the globally accessible Internet."[71]

The formation of ICANN, and recruitment of an international board of directors, constituted an adept use of diplomacy by the Clinton administration, which kept formal control of the root in the hands of the U.S. Government, but mollified the foreign interests by giving them a role in the administration of ICANN. Continued administration of root authority thereafter became a matter of global acquiescence, which has lasted for almost a decade. As described by Professors Jack Goldsmith of Harvard Law School and Timothy Wu of Columbia Law School:

> ICANN has delivered the goods. It decentralized the sale and distribution of domain names, resulting in a dramatic drop in the price of registration. It has established an effective mechanism for resolving trademark disputes that has diminished the problem of 'cybersquatting'. . .[and] it has maintained enough stability in the naming and numbering system that people rarely worry about the Internet collapsing. . . .While it once spoke of ultimately giving up all control, the Commerce Department later insisted that it had 'no plans to transfer to any entity its policy authority to direct the authoritative root server.'[72]

By its nature, the scope of root authority is limited. ICANN governs only *part* of the system for allocating and registering domain

[69] GOLDSMITH & WU, *supra* note 19, at 169.
[70] Mueller, *supra* note 43, at 186.
[71] Feld, *supra* note 45, at 351.
[72] GOLDSMITH & WU, *supra* note 19, at 170.

names and IP addresses and it coordinates operation of the "A" root server (located in Herndon, Virginia) and the 12 secondary root servers (designated B-M),[73] most of which are located in the United States.[74] Many of the subsidiary root servers are operated by U.S. government agencies,[75] and a substantial percentage of foreign Internet traffic still traverses U.S. soil, but the volume diminishes each year, as more and more foreign backbone elements are brought on line. As a physical matter, this means that many of the Internet Points of Control are on U.S. territory, but those points are gradually shifting overseas as foreign components of the Internet expand.

ICANN's plenary jurisdiction is limited to the generic top-level domains, such as .com, .org, and .net, and it has only limited jurisdiction over the hundreds of country code top-level domains, such as .uk (United Kingdom) and .jp (Japan).[76] These country code domains were created years ago, by Jonathan Postel and the IANA, and they are directly or indirectly controlled by the various national governments.

In 2006, the Chinese began to implement their own top-level domain system, without ICANN's consent, using Chinese characters, even though the Chinese deny they are splitting the root and making a direct challenge to ICANN root authority.[77]

The unilateral action of the Chinese illustrates how easily the existing root authority could be upended. Clearly, the U.S. Government's control of the root cannot be used to impose a system of copyright controls on the rest of the world, without risking fragmentation of the Internet. Rather, the best way to achieve world-wide copyright protection would be to form an agreement between the major copyright owners, the multi-national corporations which own and operate the backbone, and as many of the major ISPs which provide backbone and Internet service to consumers as possible, and then seek ratification of, or at

---

[73] Viktor Mayer-Schönberger and Malte Ziewitz, *Jefferson Rebuffed: The United States and the Future of Internet Governance*, 8 COLUM. SCI. & TECH. L. REV. 188 (2007)

[74] 9 of the 13 root servers are headquartered in the United States, but the new "anycast" software has globally distributed their functions, so there are now more than 100 major root name server locations, with the majority outside the United States. ICANN Fact Sheet, March 1, 2007

[75] U.S. Government DNS root servers are operated by NASA, the Defense Information Systems Agency, the U.S. Army and the National Science Foundation. Domestic root name servers are also operated by Network Solutions, Inc./Verisign, the University of Southern California-ISI, the University of Maryland, and Cogent Communications. Foreign root name servers are operated by WIDE Project (Japan Registry Services Co., Ltd.), Netnod Internet Exchange i Sverige AB (Sweden) and Réseaux IP Européens Network Coordination Centre (RIPE NCC), based in the United Kingdom.

[76] MUELLER, *supra* note 43, at 207-08.

[77] *Closing China's Internet Gap*, South China Morning Post, Dec. 14, 2006, at 19.

least acquiescence to, the *fait accompli,* by the major sovereign governments. ICANN could, but would not necessarily have to, play a major role in this process.

One factor which greatly increases ICANN's influence is the popularity of the generic top-level domains. The generic domains account for approximately 70% of Internet traffic because most businesses prefer to use the generic top-level domains for image reasons. For example, a business in France with a web site bearing the ".com" suffix would have an international image, whereas the same business might look provincial if it uses ".fr" as its top-level domain name. As a technological matter, there is no functional difference between using a generic top-level domain name and a country code. Because of coordination by ICANN, Internet users anywhere on the Internet can search country-code domains and log onto web sites which use country codes, exactly the same as with generic domain names. However, the international preference for the generic domain names has enhanced the prestige and influence of ICANN, which governs the generic domains.[78]

The global preference for the generic domains has strengthened ICANN's implementation of Online Dispute Resolution (ODR) for domain name disputes. The ODR system, technically a form of administrative review, only resolves domain name disputes based on naming issues. The system was formed primarily to deal with trademark infringements, especially "cybersquatting" (registering an infringing domain name for the purpose of selling it to the trademark owner at an exorbitant price) and "typosquatting," which involves registering misspelled versions of a trademark to harvest traffic resulting from typographical errors.

ICANN's system of ODR works entirely online, thus avoiding the oppressive costs entailed in litigating and enforcing judgments across international boundaries.[79] The need for an ODR system was recognized during the mid-1990s, when domain name registrations grew exponentially. Anybody could register a domain name on a first-come, first-served basis, and abuses began to crop up, most notably a wave of usurpations of trademarks and cybersquatting.

---

[78] Early browsers used ".com" as the default suffix. Thus, when a user typed in a word, such as "automobile," the browser would automatically fill in "automobile.com." This default made ".com" the dominant top-level domain, and it remains by far the most popular to this day.

[79] Critics of the ICANN system of ODR question its neutrality and denigrate its efficacy, especially outside the United States. *See e.g.*, Mayer-Schonberger & Ziewitz, *supra* note 73.

Due to the global nature of the Internet, resolving domain name disputes in territorial courts is impractical. Consider the following hypothetical: an Italian business learns that its famous trademark has been registered as a domain name by a cybersquatter in Brazil. The Italian company could file a lawsuit in the Italian courts, but that would involve a difficult battle over *in personam* jurisdiction, and the Brazilian courts might not recognize an Italian judgment. The Italian company could hire Brazilian lawyers and sue in Brazil, but that risks being "home-towned" in a Brazilian court. The domain name registrar might be in the United States, so U.S. lawyers would also have to be hired, to enforce the Brazilian or Italian judgment. In other words, hundreds of thousands of dollars would be spent on legal fees, with no guarantee the infringing web site would be removed from the Internet, and the delay would be considerable.

By contrast, under ICANN ODR, the entire dispute can be quickly arbitrated online, without even hiring a lawyer, for as little as $1,000, and the arbitration award can be technologically enforced through the DNS system.

The ODR system was created by ICANN in collaboration with the World Intellectual Property Organization ("WIPO"), with the active encouragement of the U.S. Department of Commerce, but implemented through entirely private means.[80] Pursuant to ICANN's Uniform Domain Name Dispute Resolution Policy ("UDRP"), ICANN-accredited registrars require their registrants to enter into a stipulation to arbitrate domain name disputes as a condition to registering a domain name.[81] As a result, during the last nine years more than 18,000 domain name disputes have been expeditiously and inexpensively resolved in the private sector, with minimal judicial involvement.

ICANN arbitration is not universal. It only governs the generic domains, there are non-accredited registrars who do not bind their registrants,[82] the country code domains are outside ICANN's authority, and the loser can still go to court. However, the success of ICANN arbitration has led many countries to voluntarily subscribe to the ODR system for domain name dispute resolution,[83] and court battles after ICANN arbitration are a rarity.

---

[80] MUELLER, *supra* note 43, at 190-194.

[81] ICANN, Uniform Domain Name Dispute Resolution Policy, http://icann.org/dndr/udrp/policy.htm (last updated May 17, 2002).

[82] George B. Delta & Jeffrey M. Matsurra, *Law of the Internet, 2d Ed.*, § 5.04.

[83] Jonathan Zittrain, *Be Careful What You Ask For: Reconciling a Global Internet and Local Law*, in WHO RULES THE NET? INTERNET GOVERNANCE AND JURISDICTION 13, 23 (2003).

Significantly, the DNS system allows ICANN arbitration awards to be administratively enforced, through technical means.[84] Thus, if an ODR arbitrator determines that a domain name is infringing a trademark and the losing party does not file a lawsuit within 10 days after the award, the offending domain name is deregistered and deleted from the DNS root indices. The arbitrators can alternatively specify that it shall be transferred to the complainant, and the transfer award is carried out through technical means.[85]

Early on, WIPO proposed that the ODR system also include copyright issues.[86] This proposal was not adopted, but the popularity and success of ODR for domain name disputes suggests that ODR arbitration could be extended, and adapted, to deal with overblocking disputes simply by having the private authority which administers the copyright-protection technology also implement the ODR determinations.

VI. Internet Points of Control

If a copyright protection system is to be implemented on the Internet, it should be applied in three places: the origination ISPs, the routers on the backbone (including servers located at geopolitical and system edge boundaries), and at the destination ISPs. The destination ISPs are particularly important both for technical reasons and because their service areas tend to fall within the boundaries of a particular sovereign government. That is one reason why the destination ISPs are the points of control most commonly utilized by those countries which have implemented "country-wide filtering regimes. . . . . "[87]

The technology which would be deployed for copyright filtering would be similar to that of the systems already in use for censorship. A partial survey revealed that, as of 2006, 26 out of 40 countries analyzed were using some form of internet censorship through filtering.[88] Copy-

---

[84] *Id.* at 23

[85] An ICANN arbitration determination may be tried de novo if the losing party files a lawsuit within 10 days. UDRP && 4(k), 5(e). *Sallen v. Corinthians Licenciamentos LTDA*, 273 F.3d 14, 26 (1st Cir. 2001)("[T]he UDRP clearly contemplates judicial intervention and. . .the judicial outcome will override the UDRP one."); *Parisi v. Netlearning, Inc.*, 139 F.Supp.2d 745 (E.D.Va.,2001) (ICANN arbitrations are not binding under the Federal Arbitration Act).

[86] Mueller, *supra* note 43, at 191.

[87] Zittrain, *supra* note 9, at 673.

[88] Robert Faris & Nart Villeneuve, *Measuring Global Internet Filtering*, published in Access Denied 5 (2008).

right protection was *not* a major objective of filtering in the countries surveyed.[89]

Most censorship protocols currently in use only inspect packet headers, which are cross-referenced against a blacklist of origination addresses, destination addresses and forbidden URLs. This method could be used to block pirate web sites. However, to comprehensively prevent copyright infringements, the filtering system has to conduct a "deep packet inspection" of the payload. At present, only China is known to be using this kind of dynamic assessment of payload content,[90] which would be absolutely essential to filter and block copyright infringements.

Sniffer technology, the basic tool of copyright protection, involves searching the "bit stream," looking for a unique sequence of zeros and ones. All digitized sounds, images, and texts flow across the Internet expressed as a stream of binary numbers ("bits"), and all search engines and sniffers operate the same way, by looking for a particular sequence ("string") of binary numbers.

Every musical recording and video program, when digitized, generates a unique binary string. Hence, a digitized version of the motion picture *Dr. Zhivago* is nothing but a long, and completely unique, string of zeros and ones. To protect the copyright to *Dr. Zhivago* at the backbone level of the Internet, that unique digital string would be contained in a master Database of Protected Works (DPW), and the sniffers would search the Internet bit stream, looking for exact matches of zeros and ones. When the sniffers detected an infringement, they would trigger other software which would interrupt or block the transmission, and (depending on the technology in use), cause an error message, or replace the infringement with an FBI warning, or redirect the infringer to a site where *Dr. Zhivago* could be legally downloaded.

The same methodology is used for anti-virus software, which stores the digital fingerprint of known computer viruses in databases, which are constantly updated as new viruses are discovered.

To use sniffer technology to detect copyright infringements, the DPW would have to be constantly updated as new works are created and old works fall into the public domain. Control over the DPW database would be a highly sensitive function, and ODR should be available to resolve disputes about inclusion and exclusion from the database.

---

[89] *Id.* at 9.

[90] Jonathan Zittrain & John Palfrey, *Internet Filtering: The Politics and Mechanisms of Control*, published in ACCESS DENIED 29, 36 (2008).

Sniffing technology has been developed for virus hunting, search engines, censorship, law enforcement, and spying. Beginning in 1998, the FBI implemented "Carnivore," a packet-sniffing system which was attached to Internet backbone routers. Carnivore examined the entire bit stream of an ISP and captured email from and to the target of a criminal investigation. When news of the Carnivore system became public, it was renamed "DCS1000" for public relations purposes. Subsequently, the Department of Justice ceased using it, when commercial software became available and the ISPs developed the capability to perform the sniffing function using their own technology.[91]

After September 11, 2001, the U.S. Government implemented highly advanced systems to sniff for terrorist communications on the Internet, with the cooperation of various ISPs. Since a lot of this eavesdropping was done without warrants from the FISA Court, the practice has touched off civil litigation.[92] There is no doubt, however, that very sophisticated sniffer technology has been developed, and put into practice, which is quite capable of scanning the vast traffic flow of the Internet and flagging digital strings with precision.

Blocking technology is not as advanced as sniffing, but several effective filtering techniques have been developed.

A. *TCP/IP Header Filtering, DNS Deletion/Domain Deregistration*

These methods can block pirate sites and notorious infringers. Header filtering involves inspecting the origination address of a transmission to see if it has been blacklisted, then inserting an instruction to terminate the communication when one of the proscribed addresses is detected.[93] With DNS Deletion and Deregistration, the domain name is deleted from the DNS name-servers through formal de-listing or informal "tampering."[94] When users type in the blacklisted domain name, the system fails to provide the numerical IP address and the user experiences an error message instead of being logged onto the pirate site. These methods assume that a legal determination has been made to ban traffic from a particular origination address.

B. *TCP/IP Content Filtering*

This is a method for sniffing the content of particular transmissions by looking for the fingerprints of a copyright infringement. The trans-

---

[91] DANIEL J. SOLOVE, MARC ROTENBERG & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 338-339 (2d ed. 2006).

[92] Siobahn Gorman, *AT&T Suit Has Cold War Roots*, WALL ST. J., Mar. 6, 2008, at A10.

[93] MURDOCH & ANDERSON, *supra* note 10, at 59.

[94] *Id.* at 60, 64, 66.

mission is interrupted by inserting an RST packet, which causes the user's computer to reset and terminate the transmission. This method is used by the Chinese government.[95]

C. *Proxy Filtering*

This sophisticated method involves inserting a proxy server into the bit stream.[96] By capturing, assembling and inspecting the transmission before it is forwarded to the user, the proxy computer can block illegal transmissions, cause an error message, replace the infringement with a warning message, or even redirect the infringer to a legal site. Proxy filtering requires a lot of computing power and it would be relatively expensive to implement.[97]

VII. First Amendment Issues

The methods proposed by this article involve a form of prior restraint of speech, so the First Amendment clearly is implicated. However, the enforcement of copyright is a well-recognized exception to the general rule against prior restraints, which is why the Copyright Act has a provision for injunctive relief. 17 U.S.C. § 502.

The constitutional controversy about tension between copyright and the First Amendment is often said to originate with a 1970 article by Professor Melville B. Nimmer.[98] The standard rebuttal to a First Amendment attack on copyright law is to cite the Copyright Clause, which appears in the original text of the U.S. Constitution (Article I, Section 8, Clause 8), and was therefore adopted *before* the First Amendment. The interplay between the two Constitutional provisions was discussed in *Harper & Row Publishers, Inc. v. Nation Enterprises, Inc.*,[99] in which Justice O'Connor wrote:

"[C]opyright's idea/expression dichotomy strikes a definitional balance between the First Amendment and the Copyright Act by permitting free communication of facts while still protecting an author's expression."

---

[95] Goldsmith & Wu, *supra* note 19, at 92-95; ONI, *supra* note 19, at 22 (insertion of "TCP RST" packets described).

[96] Murdoch & Anderson, *supra* note 10, at 62-64.

[97] Saudi Arabia uses proxy servers, interposed between the Saudi and global Internets, to support its censorship regime. Goldsmith & Wu, *supra* note 19, at 74.

[98] Melville B. Nimmer, *Does Copyright Abridge the First Amendment Guarantees of Free Speech & Press?*, 17 UCLA L. Rev. 1180 (1970).

[99] 471 U.S. 539, 556 (1985).

The Constitutional status of copyright arose again in *Eldred v. Ashcroft*,[100] where Justice Ginsburg wrote for the Court:

> The Copyright Clause and First Amendment were adopted close in time. This proximity indicates that, in the Framers' view, copyright's limited monopolies are compatible with free speech principles. Indeed, copyright's purpose is to promote the creation and publication of free expression. . . .In addition to spurring the creation and publication of new expression, copyright law contains built-in First Amendment accommodations. . . .First, it distinguishes between ideas and expression and makes only the latter eligible for copyright protection. . . .Second, the 'fair use' defense allows the public to use not only facts and ideas contained in a copyrighted work, but also expression itself in certain circumstances.

In articulating the fundamental reason why copyright trumps First Amendment doctrine, Justice Ginsburg summarized as follows:

"The First Amendment securely protects the freedom to make – or decline to make – one's own speech; it bears less heavily when speakers assert the right to make *other people's speech*."[101]

Justice Ginsburg's identification of fair use as a factor in harmonizing copyright and First Amendment doctrine underscores the importance of having an unblocking mechanism, to allow *bona fide* fair uses to pass through the blocking technology. Academics, reviewers, satirists, and others who wish to use some small snippet of a copyrighted work should be able to obtain a fair use key without undue difficulty. Likewise, ODR should be available to resolve the inevitable disputes which will arise when the snippet is deemed to be too long, or the proposed use is not considered fair.

The use of digital similarity as the technical standard is constitutional, because automatic blocking would only occur when there has been a bodily appropriation of a copyrighted work. Using sniffers, only verbatim infringements of sound recordings, images, or sections of text would be automatically blocked. Mere substantially similarity, without a bodily misappropriation, would *not* be automatically blocked.

By way of illustration, an unauthorized transmission of the original sound recording of *Satisfaction* by the Rolling Stones would be automatically blocked, because the system would recognize the distinctive digital signature of the original sound recording. Conversely, if an amateur band recorded its own version of *Satisfaction,* or recorded a song

---

[100] 537 U.S. 186, 218-219 (2003).

[101] Eldred at 221 (emphasis added). *See also* Michael D. Birnhack, *Freedom of Speech*, 4 NIMMER ON COPYRIGHT, 19E.03[B] ("Insofar as [infringers] chose to avoid the expenditure of time and skill necessary to evolve their own expressions, and instead copied the plaintiff's expression, there can be no First Amendment justification for such copying.")

which was substantially similar to the Stones' composition, and posted the infringing recording on the Internet without a composition license, the recording would not be automatically blocked because the system would not recognize the digital signature of the "cover" or "knock-off" versions. In that event, the owner of the composition copyright would either have to serve a takedown notice or obtain a determination by an arbitrator or a judge to have the infringing song added to the DPW block list.

If copyright protection is implemented by the private sector, there is also a question as to whether the First Amendment applies at all, because the First Amendment is actually a defense to any regulation which purports to compel a private party to use a private distribution system to transmit somebody else's speech.[102]

Conversely, if the U.S. Government gets directly involved in the technological protection of copyrights online, the availability of an efficient and fair system for unblocking fair uses would clearly be necessary to pass First Amendment muster.

The FCC has flirted with a quasi-First Amendment principle called "net neutrality," which would treat ISPs as common carriers, and impose a duty to transmit without filtering or discrimination. However, the FCC Policy Statement on net neutrality is expressly limited to "*lawful* Internet content" and it also contains an exception allowing the ISPs to engage in "reasonable network management."[103]

Since copyright infringements are unlawful, the principle of net neutrality does not apply when copyright infringements are blocked. Likewise, since file-sharing consumes an inordinate amount of bandwidth, the ISPs are entitled to restrict file-sharing pursuant to their recognized right to use reasonable network management.

VIII. Fourth Amendment Issues

A scanning-and-blocking system would also have the capacity to engage in surveillance as well as filtering, and could be used to collect evidence of infringement for use in civil actions and criminal prosecutions under the No Electronic Theft (NET) Act.[104]

If this inculpatory data was collected privately, there would be no Fourth Amendment obstacle to using it as evidence in support of crimi-

---

[102] *See* Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 642 (1994) ("Must carry" regulation, which compelled private distribution of content, was subject to rigorous scrutiny).

[103] FCC Policy Statement, *supra* note 37 (emphasis added).

[104] 17 U.S.C. § 506(a) (2000); 18 U.S.C. §§ 1961, 2319 (2009). *See also* Joseph D. Schleimer & Kenneth D. Freundlich, *Criminal Prosecution of Online "File Sharing,"* J. Internet L., Aug. 2001, at 14.

nal charges, because the exclusionary rule does not apply to the proceeds of a "private search."[105] If there was too much of a government imprimatur on the sniffing and data collection,[106] then a court might find there was government action, and the Fourth Amendment precedents concerning the use of scanning technology would be applicable.

The leading case in this area is *Kyllo v. United States*,[107] which held that the use of thermal imaging to scan for the heat signature of marijuana cultivation constituted a search, because "the government violates a subjective expectation of privacy that society recognizes as reasonable" by using sense-enhancing technology not in common use by the public. Justice Scalia, writing for the Court, examined the "power of technology to shrink the realm of guaranteed privacy" and concluded:

> We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area. . .constitutes a search—at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted. On the basis of this criterion, the information obtained by the thermal imager in this case was the product of a search.[108]

Kyllo was distinguished in *Illinois v. Caballes*,[109] which held that an alert signal from a drug-sniffing dog was sufficient to justify a warrantless automobile search because "the use of a well-trained narcotics-detection dog – one that does not expose noncontraband items that otherwise would remain hidden from public view. . . generally does not implicate legitimate privacy interests."[110]

The basic tool for detecting contraband on the Internet is the sniffer, and just like the drug-sniffing dog, an electronic sniffer does not expose noncontraband items. Thus, under *Caballes*, evidence of copyright infringement gathered by Internet sniffers should be admissible in support of criminal copyright infringement charges, even if the sniffing was done with government involvement. If the sniffer evidence was

---

[105] U.S. v. Jacobson, 466 U.S. 109, 113-114 (1984).

[106] *Cf.*, Parisi v Netlearning, Inc., 139 F. Supp. 2d 745, 747 (E.D. Va. 2001), which characterized ICANN's administration of the domain name system as Aquasi-governmental. *See also* A. Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution*, 50 DUKE L.J. 17 (2000), where Professor Froomkin argues that the Department of Commerce acted *illegally* in delegating root authority to ICANN.

[107] 533 U.S. 27, 33 (2001).

[108] *Kyllo*, 533 U.S. at 34-35.

[109] 543 U.S. 405 (2005).

[110] *Id.* at 409.

gathered privately, the chances it would be admitted (and support a conviction) would be that much greater.

IX. Anti-Wiretapping Statutes and "Filtration Immunity"

"Wiretapping" is defined and prohibited by Federal law. Under 18 U.S.C. " 2510, 2511; 47 U.S.C. '605, criminal charges can be brought, and civil legal actions can be filed, based on the unlawful "interception" of electronic transmissions.[111]

The purpose of the anti-wiretapping statutes is to prevent eavesdropping, and those statutes should not hamstring ISPs in filtering objectionable material from their system. In fact, the Federal wiretapping law expressly permits a wire communication service provider to protect itself from "fraudulent, unlawful or abusive use" of its system and services.[112]

Since the major technology companies are already tapping into the Internet bit stream for virus detection and filtering, are they guilty of wiretapping? As pointed out by Professors Murdoch & Anderson, a distinction has been made between wiretapping, which entails "access to content," as opposed to mere "traffic analysis," which involves the mere sifting of "traffic data."[113] This view is supported by the self-defense exception in the anti-wiretapping statute, which permits interception of traffic to protect "rights or property of the provider. . . ."[114]

Viruses are strings of zeros and ones, just like all other data that traverses the Internet. In order to catch viruses, one has to scan the entire bit stream, including headers, payloads, and attachments; and one has to do this for every single packet which passes through one's sensors. The distinction between content and traffic data is fine-grained, because viruses, private messages, and copyright infringements are all intermixed in a packet-switching system.

Must the ISPs allow viruses to pass through their system, and wreak havoc on their customers, or risk being sued for wiretapping? The answer, clearly, should be no. Virus hunters are looking for malicious code, and there is a specific provision allowing interception of transmissions to counter attempts at "computer trespass."[115] Since

---

[111] *See also* the European Union's directive on "wiretapping," Council Directive 97/66/EC of 15 Dec. 1997, art. 5(1), which generally prohibits wire surveillance and interceptions, subject to Article 14(1), which *allows* wiretapping "necessary. . .[for] the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the telecommunications system. . . ."

[112] 18 U.S.C. § 2511(2)(h)(ii) (2000).

[113] Murdoch & Anderson, *supra* note 10, at 71.

[114] 18 U.S.C. § 2511(2)(a)(i) (2000).

[115] 18 U.S.C. § 2511(2)(i) (2000).

sniffing for copyright infringements is functionally the same activity as virus hunting, and both functions will probably be performed simultaneously, by the same equipment, copyright sniffing should be bootstrapped under the computer trespass exception.

Moreover, there is bright-line statutory authority for Internet filtering, contained in an amendment to the Communications Act, which states:

> Civil liability. No provider or user of an interactive computer service shall be held liable on account of – (A) any action voluntarily taken in good faith to *restrict access to or availability of material* that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, *or otherwise objectionable*, whether or not such material is constitutionally protected; or (B) any action taken to enable or make available to information content providers or others the technical means to *restrict access to material* described in paragraph (1).[116]

Under this statute, the ISPs should have civil immunity for sniffing out and blocking copyright infringements as objectionable material. This would be a manifestly reasonable classification, because the major ISPs have long had "Acceptable Use Policies" which specifically prohibit customers from using their systems to transmit copyright infringements. For example, AT&T's Acceptable Use Policy provides:

> AT&T IP related Service shall not be used to transmit, re-transmit, or store any content or to engage in any activity that *infringes the intellectual property rights* or privacy rights of AT&T or any individual, group or entity, including but not limited to *any rights protected by any copyright*, patent, trademark, trade secret, trade dress, right of privacy, right of publicity, moral rights or other intellectual property right now known or later recognized by statute, judicial decision or regulation.[117]

Opponents of copyright protection might argue that the intent of Congress in passing the filtration immunity statute was to protect children from pornography, and they may cite provisions in the statute in support of an argument that Congress did not intend to allow the detection, filtering, and blocking of copyright infringements.[118] The fatal defect in that argument is the express language of the statute, wherein Congress specifically authorized filtration of *any* "objectionable materi-

---

[116] 47 U.S.C. § 230(c)(2) (2000) (emphasis added).

[117] AT&T Acceptable Use Policy, http://www.corp.att.com/aup/ (accessed March 6, 2008) (emphasis added).

[118] *See* 47 U.S.C. § 230(e)(2) (2000) (Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property) and 47 U.S.C. § 230(e)(4) (2000) (Nothing in this section shall be construed to limit the application of the Electronic Communications Privacy Act of 1986 or any of the amendments made by such Act, or any similar State law.)

als," and the only express limitation on that term was the obligation of "good faith." 47 U.S.C. § 230(c). Since the statute merely authorizes the ISPs to police their own systems, and it is clearly in good faith to interpret the term "objectionable" as encompassing transmissions which are illegal, the application of the filtering statute to the blocking of copyright infringements should be upheld.

It should also be noted that ISPs can require their customers to enter into contractual waivers, allowing the inspection of the bit stream for copyright infringements, and consenting to the blocking of copyright infringements. Consent vitiates the prohibitions of the anti-wiretap statutes. 18 U.S.C. § 2511(3)(b)(ii).

Finally, it should be kept in mind that most peer-to-peer file-sharing involves a public offer to participate in a copyright infringement. Since those offers are "readily accessible to the general public," they would fall within another exception to the anti-wiretapping statute. 18 U.S.C. §§ 2510(16), 2511(g)(i).