AKIN GUMP
STRAUSS HAUER & FELD LLP
Attorneys at Law

ORIGINAL

TOM W. DAVIDSON
202.887.4011/fax: 202.955.7719
tdavidson@akingump.com

December 22, 2009

VIA MESSENGER

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

EX PARTE OR LATE FILED

Received & Inspected
DEC 2 8 2009
FCC Mail Room

Re: **The Walt Disney Company**
***Ex Parte* Presentation in CSR No. 8233-C; CSR No. 8234-M**

Dear Ms. Dortch:

Submitted herewith on behalf of The Walt Disney Company are an original and four copies of a written summary of an *ex parte* presentation to be filed in the above referenced proceedings.

Please direct any questions concerning this matter to the undersigned.

Sincerely,

Tom W. Davidson, Esq.

Enclosures

No. of Copies rec'd 0
List ABCDE

The Walt Disney Company

ORIGINAL

December 18, 2009

Received & Inspected
DEC 2 0 2009
FCC Mail Room

EX PARTE OR LATE FILED

Ms. Marlene Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554

Re: Ex Parte Presentation in MB Docket No. 07-269; GN Docket No. 09-191; WC Docket No. 07-52; CSR No. 8233-C; CSR No. 8234-M

Dear Ms. Dortch:

On December 16, 2009, Chairman Julius Genachowski, Sherrese Smith, Paul deSa and David Goldman met with the following Disney and ESPN representatives: George Bodenheimer (Co-Chairman Disney Media Networks & President, ESPN and ABC Sports), Ed Durso (EVP of Administration ESPN), Preston Padden (EVP, The Walt Disney Company), Susan Fox (VP, The Walt Disney Company) and Bill Bailey (VP, The Walt Disney Company). During this meeting, the Disney and ESPN executives addressed several issues.

First, the Disney and ESPN executives reiterated the points made in Disney's Reply Comments in MB Docket No. 07-269 (the Video Competition Report Proceeding), stressing that the negotiation of retransmission consent agreements should be left to the private marketplace and that the FCC should not intervene in those negotiations or require interim carriage of broadcast stations. The Disney and ESPN executives responded (again) to unsupported tying allegations against Disney, citing to the three affidavits on this subject that Disney has filed in various FCC proceedings. The Disney and ESPN executives also referred to an attached press release, which explained that during the last retransmission consent cycle, Disney offered free retransmission consent to 91 small cable operators (out of a total of 113 cable operators with whom Disney negotiates retransmission consent).

With respect to ESPN360.com, the Disney and ESPN executives stressed that the business model for ESPN360.com has nothing to do with net neutrality and stressed the facts regarding ESPN360.com that are set forth in Disney's Reply Comments (that ESPN360.com now is available to approximately 50 million broadband subscribers; that it provides access to thousands of full game telecasts, many of which would not

otherwise be available; that ESPN does not force any distributor to carry any of its products; and that ESPN.com is EPSN's advertising-supported site offering more sports video online than anybody). Further, Disney/ESPN discussed and submitted the attached Empiris paper regarding the economics of ESPN360.com.

During this same meeting, the Disney and ESPN executives also raised the issues of Internet piracy and distributed the attached paper prepared by The Information Technology & Innovation Foundation.

Pursuant to Section 1.1206 of the Commission's rules, an original and one copy of this letter are being filed as notice of this meeting. The proceedings at issue are not restricted and therefore presentations are permitted, but must be disclosed.

Sincerely,

Susan L. Fox

cc: Chairman Julius Genachowski
Sherrese Smith
Paul deSa
David Goldman

CERTIFICATE OF SERVICE

I, Cynthia L. Taylor, a secretary in the law firm of AKIN GUMP STRAUSS HAUER & FELD LLP, hereby certify that on this 22nd day of December, 2009, I caused copies of the foregoing Ex Parte Presentation to be mailed via first-class postage prepaid mail to the following:

Seth A. Davidson
Robert M. Nelson
Fleishman and Harding LLP
1255 23rd Street, N.W., Eighth Floor
Washington, DC 20037

Clifford M. Harrington
John K. Hane
Paul A. Cicelski
Pillsbury Winthrop Shaw Pittman
2300 N Street, N.W.
Washington, DC 20037

Neal M. Goldberg
Michael S. Schooler
Stephanie L. Podey
National Cable & Telecommunications Association
25 Massachusetts Avenue, N.W., Suite 100
Washington, D.C. 20001-1431

Matthew M. Polka
President and Chief Executive Officer
American Cable Association
One Parkway Center
Suite 212
Pittsburgh, PA 15220

Jeremy M. Kissel
Scott C. Friedman
Cinnamon Mueller
307 North Michigan Ave.
Suite 1020
Chicago, IL 60601

Ross J. Lieberman
Vice President of Govt. Affairs
American Cable Association
4103 W Street, N.W, Suite 202
Washington, DC 20007

William T. Lake
Chief, Media Bureau
Federal Communications Comm.
445 12th Street, SW
Washington, DC 20554

Steven Broeckaert
Media Bureau
Federal Communications Comm.
445 12th Street, SW, Room 4-A865
Washington, DC 20554

Robert Ratcliffe
Deputy Chief, Media Bureau
Federal Communications Comm.
445 12th Street, SW, Room 3-C250
Washington, DC 20554

Sherrese Smith
Legal Advisor, Chairman Genachowski
Federal Communications Comm.
445 12th Street, SW
Washington, DC 20554

Diana Sokolow
Media Bureau
Federal Communications Comm.
445 12th Street, SW, Room 4-A860
Washington, DC 20554

Mary Beth Murphy
Media Bureau
Federal Communications Comm.
445 12th Street, SW, Room 4-A766
Washington, DC 20554

Jamila Bess Johnson
Joshua Cinelli
Legeal Advisor, Commissioner Copps
Federal Communications Comm.
445 12th Street, SW, Room 2-C234
Washington, DC 20554

Rick Kaplan
Legal Advisor, Commissioner Clyburn
Federal Communications Comm.
445 12th Street, SW
Washington, DC 20554

Rosemary C. Harold
Legal Advisor, Commissioner McDowell
Federal Communications Comm.
445 12th Street, SW, Room 8-C302
Washington, DC 20554

William D. Freedman
Brad Gillen
Legal Advisor, Commissioner Baker
Federal Communications Comm.
445 12th Street, SW, Room 3-C830
Washington, DC 20554

Nancy Murphy
Media Bureau
Federal Communications Comm.
445 12th Street, SW, Room 3-C375
Washington, DC 20554

Corie Wright
501 Third Street, NW, Suite 875
Washington, DC 20001

Angela Campbell
Institute for Public Representation
600 New Jersey Ave., N.W.
Washington, DC 20001

Kathryn A. Zachem
Vice President, Regulatory and State Legislative Affairs
Comcast Corporation
2001 Pennsylvania Ave., N.W.
Suite 500
Washington, DC 20006

Cynthia L. Taylor

FOR IMMEDIATE RELEASE

July 8, 2008

Disney Offers No-Charge Retrans Deals to More Than 90 Small Cable Operators in 10 ABC-Owned Station Markets

The Walt Disney Company today announced the unilateral decision to offer retransmission consent agreements at no charge to more than 90 small cable operators in the 10 ABC-owned station markets. These small operators, representing 91 of 113 (80 percent) of the operators in the aforementioned markets, will be receiving a three-year proposal (2009-2011), which will not require a fee or carriage of any other affiliated network.

"We are very pleased to support our smaller affiliates with this offer," said Preston Padden, Executive Vice President, Government Relations, The Walt Disney Company. "American Cable Association President Matt Polka, the ACA Board, and each of the FCC Commissioners deserve credit for raising the concerns that led our Company to adopt this new policy."

The ABC Owned Television Stations include WABC-TV in New York, KABC-TV in Los Angeles, WLS-TV in Chicago, WPVI-TV in Philadelphia, KGO-TV in San Francisco, KTRK-TV in Houston, WTVD-TV in Raleigh-Durham, KFSN-TV in Fresno, WJRT-TV in Flint and WTVG-TV in Toledo.

##

Contacts:

Disney – ABC Television Group

Julie Hoover
212-456-6641
Julie.T.Hoover@disney.com

Karen Hobson
818-569-7789
Karen.hobson@disney.com

EMPIRIS

THE ECONOMICS OF ESPN360.COM

Jeffrey A. Eisenach*
November 2009

ESPN360.com (ESPN360) is an Internet-based sports programming service that allows users to view popular television sports events over their broadband connections. The service is made available to subscribers of high-speed Internet Service Providers (ISPs) who pay ESPN a license fee. More than 110 U.S. ISPs, including both large carriers like AT&T, Comcast, and Verizon, and small ones like Allwest Broadband, Grande Communications, and the Wabash Mutual Telephone Company, make ESPN360 available to their subscribers.[1] Nearly 50 million households have access to ESPN360.

Recently, the American Cable Association (ACA) has alleged that ESPN360 somehow violates "net neutrality" principles because it does not charge consumers directly for access to its programming, but instead charges ISPs.[2] More broadly, some have expressed concerns that ESPN360's business model might raise costs to broadband providers, ultimately leading to higher broadband prices (and/or lower penetration), and thus harm consumers.[3]

From an economic perspective, these concerns are simply unwarranted. At the broadest level, there is no evidence of market failure in the intensely competitive market for broadband content, and hence no basis for concluding that the market is failing to maximize consumer welfare. More specifically, economic analysis makes clear that ESPN360 increases the value of broadband connections, thereby driving broadband adoption and allowing ISPs to spread the

* Jeffrey A. Eisenach is Chairman of Empiris LLC, a Washington, DC-based economic consulting firm, and an Adjunct Professor at George Mason University Law School.
[1] See http://espn.go.com/broadband/espn360/affl.jsi.
[2] See http://americancable.org/node/1628.
[3] See http://www.independentcable.com/Issues/July-09.pdf at 4.

high fixed costs of their networks over a larger subscriber base. Thus, rather than imposing a charge that ISPs might choose to "pass through" to their customers, ESPN360 can reduce broadband prices *for all consumers,* thereby further increasing broadband penetration. In these respects, ESPN360 is no different from a variety of "free" services ISPs offer subscribers as a means of increasing subscribership, such as anti-virus and content filtering software provided by firms like MacAfee, and online games provided by firms like Oberon Media.

ISPs license ESPN360 because they believe it will attract additional subscribers.[4] It is not surprising that ISPs would reach this conclusion, as sports programming is consistently among the most popular programming with subscribers on any platform. For example, in 2008, market research firm Beta Group found that cable operators ranked ESPN as the most valuable network on their cable systems for the ninth consecutive year.[5] The same survey showed that ESPN also ranked first in helping cable operators sell interactive and broadband services.

Second, by increasing subscribership, ESPN360 and other value-added services benefit both ISPs and consumers by allowing ISPs to capture economies of scope and scale. Economies of scope occur because broadband ISPs typically provide – in addition to broadband – either telephone service, cable TV services, or both (the "triple play"), and there are significant cost savings associated with providing multiple services to the same subscriber. Economies of scale are a result of the fact that broadband networks have high fixed costs and relatively low variable costs, so that the average total cost of serving each subscriber declines with the number of subscribers.

---

[4] Unlike ESPN's traditional video products, which allow cable operators to earn significant revenues by inserting local advertisements into ESPN programs (known as "avails"), ESPN360 does not currently generate advertising revenue for ISPs.

[5] See www.multichannel.com/article/print/179824-ESPN_Disney_Discovery_Top_Programmers_In_Helping_Ops_Sell_Advanced_Services_Beta_Study.php.

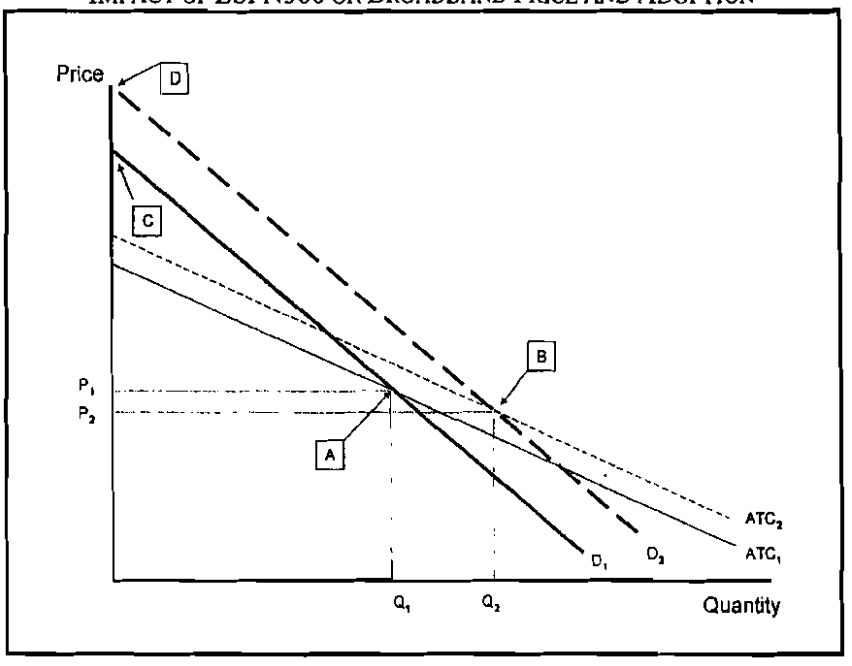
In these conditions, and under reasonable assumptions, a service like ESPN360 *reduces the average cost of providing broadband service*, and thus not only increases the value of the broadband providers' service, but also *reduces prices* for *all* consumers. This effect is illustrated in Figure One, below.

As the figure shows, the initial (pre-ESPN360) equilibrium occurs at point A, where the demand curve, D_1, intersects with the Average Total Cost curve, ATC_1.[6] At this point, the quantity of broadband services purchased (i.e., the number of broadband subscribers, since each household presumably purchases one connection) is Q_1 and the price is P_1. Now, assume that ISPs subscribe to ESPN360, for which they incur a fee, shifting their average total cost curves outward by the amount of the fee, as represented in the figure by the shift in the average total cost curve from ATC_1 to ATC_2. At the same time, however, ISPs incur this fee only to the extent it increases demand for broadband services, as represented by the outward shift in the demand curve, from D_1 to D_2.

As the figure shows, the net effect of these changes is to move the equilibrium from point A to point B, where ATC_2 intersects D_2. The important point about point B, of course, is that $P_2 < P_1$ and $Q_2 > Q_1$ – that is, *the price is lower and the quantity (i.e., the number of broadband subscriptions) is higher than in the pre-ESPN360 equilibrium.*

[6] The ATC curve is assumed to be identical to the supply curve. In equilibrium, firms cannot charge prices below average total cost, since they would incur economic losses and ultimately exit the industry, nor will they charge more than long-run ATC, as doing so would attract entry. See e.g., F.M. Scherer, *Industrial Market Structure and Economic Performance* 2d. ed. (Houghton Mifflin, 1980) at 15-16.

FIGURE ONE:
IMPACT OF ESPN360 ON BROADBAND PRICE AND ADOPTION



The figure also shows the sizeable gain in consumer welfare associated with the introduction of ESPN360. In the pre-ESPN360 equilibrium, consumer surplus is given by the area of the triangle P_1AC, whereas the addition of ESPN360 increases consumer surplus to P_2BD.[7]

It should be noted that these benefits would be less likely to be achieved if ESPN360 were forced to change its business model and sell subscriptions directly to consumers rather than through ISPs, for two reasons. First, by conditioning access to ESPN360's programming on actually having a broadband subscription, ESPN360 both avoids free riding (multiple users of individual accounts) and links the value of its programming directly to increased broadband

[7] It should be apparent from examining the figure that $P_2 < P_1$ is not a necessary condition for either $Q_2 > Q_1$ or for an increase in consumer surplus: That is, both broadband penetration and consumer welfare could increase *even if* broadband prices increased, since ESPN360 both adds value to existing subscribers and attracts new subscribers regardless of whether broadband prices go up or down.

adoption. Second, by offering ESPN360 content as a means by which ISPs can engage in efficient product differentiation, the current business model gives ISPs the ability to more successfully market their service, thus further increasing broadband adoption.[8] Finally, while there are sound efficiency rationales for calculating the charge for ESPN360 on a per-subscriber basis (i.e., it creates efficient incentives for promotion and marketing efforts), a per-subscriber fee structure is otherwise irrelevant to the points made above: Average Total Cost would increase by the same amount, regardless of how the fee is determined.

In sum, by increasing the value of broadband connections to consumers, and by giving ISPs the ability and the incentive to market that increased value proposition to their subscribers and potential subscribers, ESPN360 increases consumer welfare and raises overall broadband penetration.

[8] For an excellent treatment of the importance of product differentiation in declining cost industries such as broadband infrastructure, see Hal R. Varian, "Differential Pricing and Efficiency," *First Monday* 1;2 (August 1996) at 2.

Steal These Policies: Strategies for Reducing Digital Piracy

BY DANIEL CASTRO, RICHARD BENNETT AND SCOTT ANDES | DECEMBER 2009

We need to open a broad dialogue that engages all stakeholders, including government, content owners, website operators, technology developers, and ISPs and other intermediaries, on how to improve the global response to piracy.

Executive Summary

The rise of broadband Internet access and cheap storage, along with the growth of digital content, has enabled digital piracy to flourish around the world. Piracy enables the unauthorized distribution of music, movies, television programs, software, video games, books, photos, and periodicals quickly and easily, to the detriment of creative artists and legitimate rights holders. These practices threaten not only the robust production of digital content in the future, but U.S. jobs in the present. Unfortunately, many advocates, believing that information should be free, would have government not only turn a blind eye to digital piracy, but actively tie the hands of companies who seek to limit digital piracy. This report makes the case that digital piracy is a serious problem with significant ramifications for the U.S. economy, that a number of approaches, including technical solutions such as content identification, are needed to reduce piracy, and that governments should support legitimate industry efforts to reduce digital piracy, including those that focus on the revenue streams of those engaging in piracy.

There is no "silver bullet" that will solve the piracy problem—no single technical or legislative proposal will completely solve such a complex issue—but there are many "lead bullets" that can help reduce piracy. Just as preventing theft in the offline world requires a combination of industry-backed technical controls such as locks, closed-circuit TV, and anti-theft packaging as well as a government-funded system of law enforcement, digital piracy requires a coordinated approach. Much of this effort will likely come from industry, but government has an important role to play in protecting the intellectual prop-

ITIF

erty of copyright holders as a strong legal system is the bedrock of commerce in both the digital and analog world. In addition, government should not preclude those impacted by digital piracy, including copyright holders and ISPs, from taking steps to limit digital piracy.

Not every effort to reduce digital piracy should be embraced, of course, but there should be no doubt that efforts clearly directed at digital piracy can be and usually are different from the over-broad, ineffective methods that are often held up for criticism. In fact there are many technologies available to confront digital piracy that are cost-effective and only impinge on the "freedom" to steal. Much more can and should be done to limit digital piracy and we need to open a broad dialogue that engages all stakeholders, including government, content owners, website operators, technology developers, and ISPs, on how to improve the global response to the problem of piracy. Toward that end, this report recommends that policymakers:

- **Support, rather than impede, anti-piracy innovation, including the development of new technical means.**
- **Encourage coordinated industry action to take steps to fight digital piracy, including steps like ISP implementation of graduated response systems.**
- **More actively pursue international frameworks and action to protect intellectual property, including digital content.**

Widespread piracy over the Internet seriously harms artists, the famous and struggling alike, who create content, as well as the technicians who produce it. It ultimately also hurts law-abiding consumers who must pay higher prices for content, enjoy less content, or pay higher prices for Internet access to compensate for the costs of piracy. Moreover, digital piracy not only results in the unauthorized distribution of content, it hurts the ability of content producers to create legitimate business models for selling digital content; as the saying goes, "It's hard to compete with free." While many companies have rallied to the challenge and created compelling businesses to sell content legally, on the whole, digital content is more profitable to distribute illegally than legally and always will be.

As the leading global producer of digital content, the impact of piracy on the United States is substantial, with U.S. companies annually losing billions of dollars and eliminating or never creating tens of thousands of jobs. Although piracy is a serious problem in the United States, it is even more serious in many other parts of the world, especially emerging markets. The Business Software Alliance found, for example, that although software piracy declined or remained the same in over eighty percent of countries, global piracy still increased by 3 percent in 2008 because of rapidly expanding growth in PC ownership in high piracy regions such as Asia and Eastern Europe.

Digital piracy will never be completely stamped out, but it can be dramatically reduced. To do so, though, requires the implementation of a wide array of means, including education of consumers, a range of technical solutions, and of course, more aggressive enforcement of the legal rights of copyright holders.

To change social behavior, some content owners have tried to educate users on the impact of piracy through marketing campaigns. These tactics work in parallel with efforts to provide users legal means to access content, such as developing new forms of distribution like the iTunes store or Hulu.

Technical controls, including digital rights management (DRM), network management, and content identification systems, can also be used to make piracy more difficult. DRM technology prevents unauthorized use, such as enforcing licensing requirements on software or preventing content from being duplicated. Network management techniques, including bit caps and traffic shaping, can help reduce piracy and at the same time the load on broadband networks, reducing costs and improving the quality of Internet access for the vast majority of law-abiding broadband users. Content identification systems recognize copyrighted content so that copyright owners can take steps to reduce digital piracy. Using these systems, copyrighted content can be detected by automated means if others try to share it on filesharing networks or websites. The technology can be deployed at various locations, including on peer computers on file sharing networks, on the servers of user-generated content websites, on consumer electronics, and at the ISP level as data passes through networks into and out of network endpoints.

Some advocacy groups aligned with the information commons movement have condemned the use of many of these technical controls largely because they believe that copyright holders should have fewer rights and that piracy is not a problem. They argue that such tools are ineffective, costly and destructive to the rights of Internet users. These criticisms, however, are flawed and inaccurate. Anti-piracy solutions, including content identification technology such as watermarking and fingerprinting, are mature, highly accurate and widely available. The cost of these systems varies by implementation, but if the benefit in reduced piracy outweighs the cost of implementation, then it makes strategic sense to use the technology. These systems can easily be implemented with safeguards to ensure user privacy and protect free speech while still protecting the rights of copyright owners.

These advocates also express fears that anti-piracy measures would somehow violate the Internet architecture. The Internet architecture is no more friendly to piracy than to law-abiding uses; the Internet was designed to serve as a testbed for experimentation with legitimate network applications, protocols, and services, not as a monument to technology as it existed at a particular moment in time. If the Internet has a central principle, it is one of continual improvement. As problems emerge in the use and management of the Internet, engineers devise solutions. With the advent of a global piracy industry, piracy has become a problem that demands—and has produced—a number of solutions.

Additional technical controls may also help reduce piracy. ISPs and search engines could implement policies that block websites that host or link to pirated content. Pirated content is increasingly found not only on P2P networks, but also on websites for users to download or stream. These websites are supported by advertising or by selling the content to users. Blocking these websites at the ISP level and from search engine results, as well as pressuring advertising networks and credit card companies to refrain from supporting these websites, will help reduce this form of piracy.

Legal strategies also are a key tool to fight piracy including prosecuting the individuals and companies that upload and download pirated content. In the ruling against the file-sharing company Grokster, the U.S. Supreme Court made clear that owners of applications or services designed to enable file sharing of copyrighted content could be held liable for infringement by third-parties. Some individuals establishing such piracy tools or websites have responded by trying to find shelter to continue this activity in countries with weak enforcement regimes.

Content owners have also begun to send notices of copyright infringement to Internet users so they become aware that they are responsible for their actions online and can take steps to prevent unauthorized use, such as securing a wireless router or supervising a teenager, before facing more serious consequences for misuse. Content owners can identify individual Internet users suspected of illegal file sharing and then ask the user's ISP forward on the notice to the user. ISPs can provide a graduated response to continued violations of copyrighted content by the same user, by providing additional warnings, and incremental punishment, up to and including a termination of the service. A number of countries, including France, the United Kingdom, South Korea, and Taiwan have implemented or are in the process of implementing this type of "three strikes" system with safeguards in place to ensure citizens' rights are protected. Such legal regimes and cooperative agreements between rights holders and ISPs can both reduce digital piracy.

Government policies can and should play a key role in helping reduce digital piracy. They can start by supporting technological innovation. Just as government should not restrict multi-purpose innovations that may inadvertently aid illegal activity—such as cryptography, networking protocols and multimedia encoding—neither should it restrict innovations that can reduce illegal activity—such as digital rights management, content identification and filtering, and network management. Restricting such innovation would mean that the technology would not improve over time. Or as a bumper sticker might say, "If you outlaw innovation, only the outlaws will innovate." But the federal government should do more than not restrict anti-piracy innovation, government agencies like the FCC should affirm that they takes piracy seriously and encourage anti-piracy innovation and use. The federal government needs to take a clear position that it supports reasonable industry action to fight digital piracy. And the FCC should also develop a process whereby

industry can consult with them on proposed uses of anti-piracy technology and consumer advocates and others can bring forward concerns about actual uses.

Government should also support coordinated industry action to fight piracy. In a competitive market, a classic prisoner's dilemma exists where companies would be better off by implementing anti-piracy measures, but may not because the cost of acting alone is too risky. Going forward there is an opportunity for more industry collaboration to fight piracy. The federal government should encourage stakeholders to develop best practices and collaborative self-regulation regimes, such as ISPs implementing a graduated response system. Other approaches, however, such as blocking websites, may require governmental approval before industry can act. Toward this end, there is a need for a process by which the federal government, with the help of third parties, identifies websites and organizations around the world that are materially engaged in piracy so that ISPs and search engines can block them, advertising networks and other companies can refuse to place ads with them, and banks and credit card companies can refuse to process payments to them.

Finally, it is time for the U.S. government to take global theft of U.S. intellectual property generally, and digital content specifically, much more seriously. In particular, this means that the U.S. government should take a much more proactive position on pressuring other nations to abide by rules regarding digital content. This includes taking more cases to the World Trade Organization (WTO), working more closing with the World Intellectual Property Organization (WIPO) and other global bodies, and including requirements for reducing content theft and penalties for failure to do so in future trade agreements. And while the specific terms of the Anti-Counterfeiting Trade Agreement (ACTA) are not yet public, this type of multilateral trade agreement is necessary to create a stronger intellectual property rights regime and protect the rights of U.S. copyright holders globally. Nations that turn a blind eye to piracy should face significant pressure and penalties for doing so.

Because we all share the responsibility for maintaining the health and vitality of the Internet, the time has come for Internet enterprises and governments to take some measure of responsibility for maintaining its integrity. There is no legitimate reason for web sites that enable piracy to exist—the Internet was not meant to be a gigantic piracy machine. The time has come for the law to catch up with technology by adopting a reasonable set of enforcement measures to make piracy less prevalent and less blatant on the Internet.

Steal These Policies: Strategies for Reducing Digital Piracy

BY DANIEL CASTRO, RICHARD BENNETT AND SCOTT ANDES | DECEMBER 2009

We need to open a broad dialogue that engages all stakeholders, including government, content owners, website operators, technology developers, and ISPs and other intermediaries, on how to improve the global response to piracy.

The rise of the broadband Internet and cheap storage has led to an explosion of digital piracy (the copying of digital content without the rights holder's permission). Piracy has significant costs in terms of lost jobs and higher prices for law-abiding citizens. While there is no silver bullet for stopping piracy, there is a large array of "lead bullets" that collectively can significantly reduce digital piracy. These include teaching consumers that digital piracy is unethical and illegal, applying technical means to stop piracy, and engaging in stronger enforcement of the legal rights of content owners.

As with any law enforcement initiative, efforts at reducing digital piracy involve balancing costs and benefits. While street crime could be reduced by doubling the number of police, most communities find an equilibrium where the marginal cost of an additional police officer does not outweigh the corresponding reduction in crime. With regard to digital piracy, it is hard to argue that this equilibrium has been reached—that society would not be better off with greater efforts to stop digital piracy. The extent of piracy is so large, and the costs of enforcement quite reasonable, that it is clearly in the public interest to take more aggressive steps to curb it.

Relying on statements such as "the Internet was designed to be an open system" and beliefs that the Internet is based on a "true free and sharing spirit," a number of advocacy groups argue that government should actually restrict private sector efforts to reduce digital piracy while at the same time doing little to enforce intellectual property rights.[1] Not every effort to reduce digital piracy should be embraced. But there should be no doubt that efforts clearly directed at digital piracy are different from the over-broad, ineffective methods that are often held up for criticism. In fact there are many cost-effective technological systems to confront digital piracy and digital pirates that only impinge on the "freedom" to steal. Much more can and should be done to limit digital piracy. We need to open a broad dialogue that engages all stakeholders, including government, content owners, website operators, technology developers, and ISPs and other intermediaries, on how to improve the global response to piracy. Toward that end, this report recommends that policymakers:

- **Support, rather than impede, anti-piracy innovation, including the development of new technical means.**

- **Encourage coordinated industry action to take steps to fight digital piracy, such as ISP implementation of graduated response systems.**

- **More actively pursue international frameworks and action to protect intellectual property, including digital content.**

THE PROBLEM OF DIGITAL PIRACY

Of all the industries that have been revolutionized by the rise of digital technology and the global Internet, few have been hit as hard as the content industries—the producers of music, movies, television programs, software, video games, books, photos, and periodicals. The Internet has made global distribution of content easier than ever, with the ultimate promise of slashing costs by reducing the role of middlemen who produce, distribute, and sell the physical copies. Unfortunately, the digital era also has a serious downside for content producers and others in the industry as it has made it easier than ever for consumers to get access to content without authorization or without paying for it.

Of course, virtually every product sold to consumers is vulnerable to theft, which is why retail stores spend money to prevent shoplifting. The use of technology to make unauthorized copies of content is not new—many of these same problems were encountered with VCRs or Xerox machines. But unlike the analog technologies of the past, today's digital technology allows an infinite number of perfect copies to be made inexpensively from just one original and further allows those copies to be distributed almost without cost around the world using the Internet. Completely eliminating this kind of piracy is impossible. Once one digital copy of a song or film is created without copy-protection measures, individuals can quickly distribute it over the Internet until it is widely available. The growing availability of high-speed Internet connections and cheap storage means that users can download content regardless of the size of its digital footprint—from small music recordings and e-books to large, high-definition films and television programs. Despite these obstacles, however, it is possible and desirable to significantly reduce digital piracy.

Much of the illegal exchange of content has been facilitated by digital tools that facilitate file sharing between users, including peer-to-peer (P2P) file sharing networks (e.g. Napster, Gnutella, Kazaa, and BitTorrent), hosted online file shares (e.g. Rapidshare, Megaupload, and Drop.io) and online streaming services (e.g. YouTube, Metacafe, and Livestream.com). While all of these technologies have legitimate uses, the technology is also used for the unauthorized distribution of digital content on a global scale. In some cases, such as with some P2P file sharing networks, this has even become the principal use of the technology, although such networks are occasionally used to distribute legal content.[2]

Websites like Mininova, the Pirate Bay, and isoHunt, routinely rank among the most popular websites on the Internet and offer the ability to download virtually all popular TV series, movies, and recently released songs

Websites like Mininova, the Pirate Bay, and isoHunt, routinely rank among the most popular websites on the Internet and offer the ability to download virtually all popular TV series, movies, and recently released songs (although recently a court order forced Mininova to remove its unlawful content).[3] Unauthorized file sharing has been exacerbated by the growth of Web 2.0, or websites that cater to user-generated content, as many Internet users make no distinction when uploading between content they are authorized to upload and content they are not.

This is not merely a battle between giant media conglomerates and a group of cyberlibertarians who want to rethink copyright law (although Christrian Engström, a representative of the Swedish Pirate Party has stated that its "manifesto is to reform copyright laws and gradually abolish the patent system").[4] Widespread piracy over the Internet seriously harms the artists, both the famous and struggling, who create content, as well as the technicians—sound engineers, editors, set designers, software and game programmers—who produce it. It ultimately also hurts law-abiding consumers who must pay higher prices for content, enjoy less content, or pay higher prices for Internet access to

compensate for the costs of piracy. Moreover, digital piracy not only results in the unauthorized distribution of content, it hurts the ability of content producers to create legitimate business models for selling digital content. As the saying goes, "It's hard to compete with free." While many companies have rallied to the challenge and created compelling businesses to sell content legally, on the whole, illegal content still remains widely available and commonplace.

While most individuals do not shoplift DVDs out of retail stores, many people feel comfortable downloading movies without paying for them. Why do so many people knowingly choose to continue to download unauthorized content? One reason is that it is so easy to find and download copyrighted content online. If stealing cars was as easy as pointing and clicking, the rate of motor vehicle theft would probably be much higher. A Pew Report found that "75% of teen music downloaders ages 12-17 agree that 'file-sharing is so easy to do, it's unrealistic to expect people not to do it.'"[5] This survey also reflects the mentality (and reality) among many groups that "everybody is doing it." Moreover, the Internet gives users a sense of anonymity where the risk of getting caught is relatively low and that of punishment even lower.

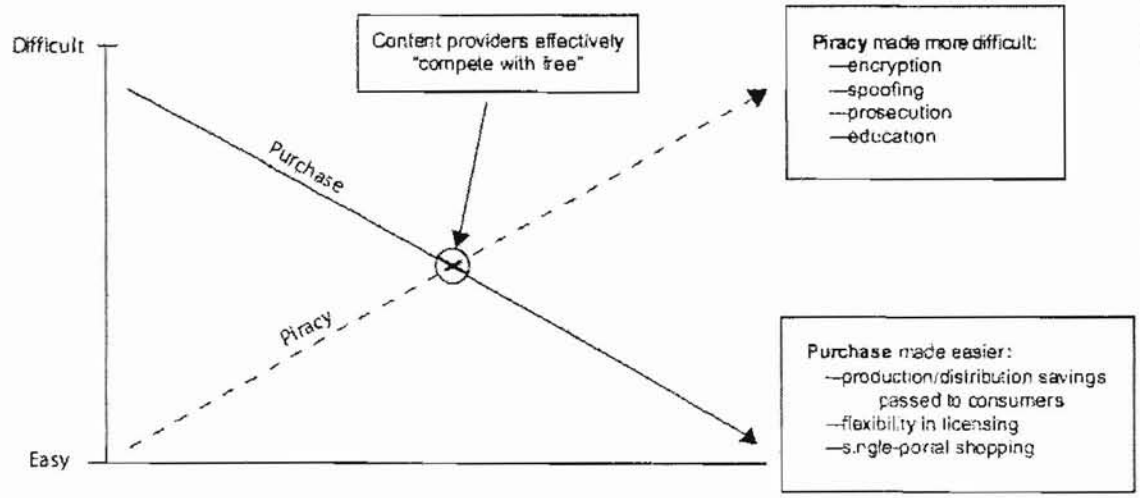
The Impact of Piracy in the United States and Abroad

Piracy is a major problem in the United States. While the exact cost of piracy is difficult to measure, the impact is substantial, with one estimate finding that the U.S. motion picture, sound recording, business software, and entertainment software/video game industries lost over $20 billion dollars in 2005 due to piracy, and retailers lost another $2 billion, for a combined loss of over $22 billion.[6] It is likely that these losses are even higher today because a larger share of the population has broadband connectivity.[7]

Some users may see this as a victimless crime. However, piracy has a negative impact on the economy. The recording industry has been hardest hit thus far, because digital song files are small enough to transmit quickly, even over relatively slow Internet connections. In 2005, music piracy was associated with the loss or lack of realization of over 12,000 jobs in the sound recording industry in the United States.[8] It is estimated that the United States recording industry and related industries in 2006 lost over $3.5 billion to online piracy and approximately $1.5 billion in physical piracy.[9] The International Federation of the Phonographic Industry (IFPI) estimates that the figure is as high as 20 illegally downloaded songs for every purchased track.[10]

Other content industries have been impacted by piracy as well. The motion picture industry has lost significant amounts of money to pirated movies both online and on DVD. According to a report published by LEK Consulting, the U.S. motion picture industry lost $6.1 billion to piracy in 2005, which one report argues eliminated or prevented the creation of 46,597 jobs in the motion picture industry.[11]

Figure 1: Competing with Free



Neither are software companies immune from piracy. Although the United States has the lowest software piracy rate out of any of the 110 countries studied by the Business Software Alliance in 2005, piracy levels as a percent of total market size are comparatively small in the United States because the software market in the United States is significantly larger than in any other nation. However, the total quantity of pirated software in the United States is larger than anywhere else in the world. With pirated software equaling 20 percent of legitimate sales, the total value of pirated software is estimated to be over $9 billion in the United States.[12] Moreover, although piracy rates have hovered around 20 percent for the last several years, total software piracy has steadily increased in line with the growth in software sales.

Although software piracy declined or remained the same in more than 80 percent of countries, global piracy still increased by 3 percent in 2008 because of rapidly expanding growth in PC ownership in high-piracy regions such as Asia and Eastern Europe.

Videogame piracy is a growing problem in both the developed and developing world. In 2008 the Entertainment Software Alliance detected more than 700,000 copyright infringements a month across more than 100 countries and sent out 6 million copyright infringement notifications. Indeed, according to a report by the International Intellectual Property Alliance, in December 2008, 13 titles were illegally downloaded 6.4 million times. The top two titles alone accounted for nearly three-fourths of illegal downloads. The report, which evaluated piracy in 219 countries, found that two P2P networks, BitTorrent and eDonkey, were the largest sources of gaming piracy.[13]

Although not as common as music, movie, software, or videogame piracy, e-book piracy is growing, particularly as more content is sold in digital format. While hard data on book piracy is scarce, many publishing industry analysts see evidence of an alarming increase in piracy, due in part to the advent of the e-book reader. For example, John Wiley & Sons (publisher of the Dummies series) reports that in April 2009 it sent out 5,000 notices of online copyright violation—more than double the number of notices sent in the previous year.[14] In addition, e-book piracy appears to be more concentrated on certain websites than music, software, or motion picture piracy. Indeed, some industry observers estimate that as much half of e-book piracy is housed on RapidShare, a Switzerland-based file hosting company that has advertised more than 10 petabytes of user uploaded files.[15] Alexa.com, which provides a global ranking of websites, currently lists RapidShare as the 26th most popular website in the world.[16]

Although piracy is a problem in the United States, the issue is far worse in many other parts of the world, especially in emerging markets. For example, the Business Software Alliance found that although software piracy declined or remained the same in more than 80 percent of countries, global piracy still increased by 3 percent in 2008 because of rapidly expanding growth in PC ownership in high-piracy regions such as Asia and Eastern Europe. Indeed, even though emerging markets only account for 20 percent of the software market, they make up 45 percent of software piracy.[17] Emerging markets account for a large portion of piracy in the music industry as well. China in particular has a high rate of piracy where over 90 percent of downloaded songs are illegal. Many Latin American countries similarly experience high rates of music piracy: it is estimated that there were 2.6 and 1.8 million illegally downloaded songs in Mexico and Brazil, respectively, in 2006. The rampant piracy appears to have had a negative impact on the market in these countries with the retail and online music markets declining by 25 and 50 percent respectively in each country.[18] Moreover, absent concerted and serious efforts to combat digital piracy in the United States and abroad, it is likely that the overall rate of piracy will increase as more people acquire Internet-connected computers and the average broadband speed increases.

While digital piracy is a problem for many nations with domestic content industries, it is a particular problem for the United States since the U.S. leads in global production of digital content.[19] As these industries form a core part of America's competitive advantage, creating higher wage jobs and export sales that help offset the large trade deficit, their decline would have disastrous consequences. Aggressive efforts to fight digital piracy will therefore have important benefits for American workers and the American economy.

DEFINING PIRACY

One obstacle to combating digital piracy is the disagreement over its definition. In general, digital piracy is the unauthorized copying and distribution of copyrighted content. Common examples of this include downloading and uploading movies, music, e-books, software, and other copyrighted content online. Digital piracy happens both on and off the Internet. For example, digital piracy includes both the online distribution of movies on P2P networks as well as the sale of counterfeit DVDs.

Individuals and organizations operating websites and Internet services that facilitate piracy often do so with the clear intent of profiting at the expense of the copyright holders.

However, not all unauthorized use of copyrighted content necessarily constitutes piracy. Various gray areas exist where the line between what is strictly legal or illegal is blurred. For example, fair use principles allow for the limited use of copyrighted content for specific applications, such as for some academic and editorial purposes. What constitutes fair use is not always clear-cut. The website Totalnews.com was sued by major publishers for violating their copyright for displaying news articles from major websites like Washington Post and CNN in a frame on its own website.[20] Publishers have also criticized blogs and other news aggregators for reprinting an excessive amount of content, for which the third-party website earns advertising revenue. Even Google has fallen under criticism for its use of snippets of text from publishers in its Google News service, a practice that led News Corp CEO and Chairman Rupert Murdoch to ask, "Should we be allowing Google to steal all our copyrights?"[21]

What is more clearly piracy is the reproduction and distribution of material protected by copyright without the publishers' permission, including on P2P networks. As P2P file sharing networks have evolved, the middlemen that facilitate the exchange of copyrighted content have gradually removed themselves from the process so that they do not host any copyrighted content on any of their servers. On a technical level, the individuals directly violating the rights of copyright holders are not necessarily the ones running the websites or applications facilitating the exchange of copyrighted files, but those individuals that upload and download these files. For example, BitTorrent, the most popular P2P protocol, allows users to download files by using a torrent file, a small file containing a series of hash values that identify a larger file. The torrent file itself contains metadata about the copyrighted file, but no copyrighted information itself. In addition, some websites act as "trackers" and maintain a list of which BitTorrent clients are using which torrents. Organizations like The Pirate Bay, which directly facilitate the illegal exchange of copyrighted content, use these facts to try to avoid legal action taken against them (although naming the organization "the Pirate Bay" does undermine its claim to innocence). As The Pirate Bay states on its website, "Only torrent files are saved at the server. That means no copyrighted and/or illegal material are stored by us. It is therefore not possible to hold the people behind The Pirate Bay responsible for the material that is being spread using the tracker."[22] While this technical distinction has not held up in court for The Pirate Bay, the argument becomes more compelling the further away an online service is from the direct infringer. For example, many other websites are even a further step removed from the process, and act not as a "tracker" or "indexer," but as merely a search engine for other websites hosting torrent files. The Pirate Bay has modified its approach to facilitating unlawful exchanges by discontinuing its tracker service in favor a decentralized system that accomplishes the same result by different means. Of course, users find both types of websites through traditional search engines such as Google and Bing, and through blogs that link to these tracking and indexing websites.

While there are legitimate debates over where the lines for fair use should be drawn, there should be no question about the fact that egregious violations of copyright—such as uploading a full-length Hollywood movie to a P2P network—are clearly illegal. Moreover, individuals and organizations operating websites and Internet services that facilitate piracy often do so with the clear intent of profiting at the expense of the copyright holders. Even websites that operate within the bounds of the law and respond to legitimate requests to take down copyrighted content still often profit from the ad revenue derived from showing unlawful content.

Finally, those who advocate sharing copyrighted content often make the critique that digital piracy has a net benefit to content producers. For example, users may listen to illegally downloaded music, but then buy more concert tickets, or "test drive" a pirated copy of a software program but then purchase the program at a later date. While some, but certainly not all, instances of digital piracy may yield benefits to the copyright owners, this is ultimately irrelevant to the debate as the copyright holders, not the users, have the legal authority to determine the conditions on under which they want to distribute their intellectual property. Moreover, if piracy were to actually lead to increased sales, rational companies would encourage it (or at least turn a blind eye to it) and thereby gain market share over their competitors.

SOLUTIONS TO THE PIRACY PROBLEM

The problem of digital piracy is not new, and content producers have tried many different strategies over the years to mitigate the problem. There is no "silver bullet" that will solve the piracy problem—no single technical or legislative proposal will completely solve such a complex issue—however, there are many "lead bullets" that can help reduce piracy. Just as preventing theft in the offline world requires a combination of industry-backed technical controls (e.g., locks, closed-circuit TV, and anti-theft packaging) and government-funded enforcement (e.g., law enforcement, district attorneys, and courts), the same is true for preventing digital piracy. Much of this effort will likely come from industry. Government, however, has an important role to play in protecting the intellectual property of copyright holders. A strong legal system is the bedrock of commerce in both the digital and analog world. In addition, government should not preclude those impacted by digital piracy, including copyright holders and ISPs, from taking steps, both technical and non-technical, to limit digital piracy.

Individual Internet users who do not perceive personal benefit from anti-piracy measures should be reminded that the long-term availability of software and entertainment in digital formats depends on the financial health and well-being of the producers and artists who create it. To the extent that piracy mitigation systems serve this end, they do offer payback to the individuals who do not have a direct financial stake in the software or entertainment industries. And of course, all Americans benefit from the U.S. economy including higher-wage jobs and more competitive industries, even if they are not employed in those industries.[23]

To achieve the goal of reducing piracy, industry and government have used various tactics, including efforts to change social behavior, implement technical controls, and enforce the legal rights of copyright holders.

Changing Social Behavior

Digital piracy exists, in large part, because individuals choose to engage in it. Content producers have worked to change this behavior through various means, including encouraging users to simply choose not to engage in the activity either because it is wrong or because it is easier to acquire content legally.

EDUCATE USERS ON IMPACT OF DIGITAL PIRACY

Content producers have worked to try to educate users about copyright issues and change public behavior. As early as 1992, the Software Publishers Association launched a famous video campaign titled "Don't Copy that Floppy" to explain the impact of piracy on industry and urge users to respect digital copyrights. The movie industry has made similar efforts such as showing anti-piracy notices at cinemas and including anti-piracy videos on DVDs. While the effectiveness of such public or private efforts to date is unknown, a long-term change in what is considered acceptable social behavior could help decrease digital piracy, the same way that changing social norms have led to reductions in littering and smoking.

PROVIDE USERS LEGAL MEANS TO ACCESS CONTENT

Some users acquire digital content illegally because comparable content is not available by legal means. Some content producers choose to restrict availability as part of their business model or because they fail to perceive that "long tail" markets exist, a practice that is increasingly problematic in the network era. For example, movies released in theaters often are not officially released on DVD for many months because of the studio business model, reflected in contractual agreements with file distributors, that emphasizes theatrical distribution first. The movie may also have only

a limited release and be available only in a few theaters or in certain countries. If a user wants to watch this type of movie outside of the theater during this window, the only option is to download the film illegally. Similar constraints also exist for television programming. Content producers should be encouraged to provide users legal and affordable access to copyrighted content.

In some cases releasing for sale the desired content is simply not possible. For example, movie studios cannot be expected to release a film before it is finished, even while digital pirates have previously acquired and distributed unfinished "screener" copies of movies before they are in theaters.

Pirated content is particularly appealing for people who seeking sources of entertainment that are not available where they live in licensed and legal forms. For example, British and American television series are immensely popular around the world, but limited numbers of programs are licensed for wider distribution. In most cases, the series that are licensed are not available in other countries right away, which is frustrating to fans who want their gratification immediately. Digital entertainment breeds changes in patterns of consumption, such as the desire of certain fans to view entire seasons of suspense thrillers such as Fox's *24* back-to-back rather than as isolated episodes a week apart. Some producers have been slow to recognize long-tail markets and new patterns of consumption, and have therefore failed to capitalize on the revenue opportunities they offer. In such cases, digital piracy provides clues to emergent business models or where content is popular, so there is value in passing information obtained from piracy mitigation to content producers for study. This is not to suggest that piracy only exists because of the desire of consumers for a free ride as much as to point out that producers should continue to labor to make as much content available legally as widely as possible to help reduce demand for pirated content. For example, once music was easily available legally online, through stores such as iTunes or Amazon, it became much easier for many consumers to buy music rather than steal it. Although most music is widely available online for free, purchases of digital music continue to grow—as of the first half of 2009, paid digital downloads accounted for 35 percent of total music sales.

PROVIDE USERS THE ABILITY TO IDENTIFY LEGAL MEANS TO ACCESS CONTENT

It is becoming increasingly difficult for the average Internet user to differentiate between legal and illegal content. While a user who downloads a feature-length Hollywood movie at no cost on a P2P network should not reasonably expect this to be a legal copy, most Internet users would suspect that an online video streaming website is providing legal content (especially those charging a membership fee), but have no way to verify that the copyright owner is being properly reimbursed. For example, the website Allofmp3.ru operated out of Russia and sold music files to Internet users at below-market rates based on a Russian licensing scheme that the major record labels believe is unlawful. Similar websites, including MP3Million.com, LegalSounds.com, and ZML.com, persist today and mislead users into purchasing copyrighted content from illegitimate sources. The content-producing industries should work to develop a trusted label that Internet users can rely on to distinguish between websites hosting authorized and unauthorized copyrighted content.

Implementing Technical Controls

Various technical controls can help reduce digital piracy. These controls can be implemented in one or more of the processes used to exchange and view copyrighted content—from the user's media player or personal computer to the Internet service provider used to transfer the content.

DIGITAL RIGHTS MANAGEMENT

Industry groups have implemented various technical controls to mitigate file sharing. The most common control has been digital rights management (DRM) technology, or technical controls embedded within the content to prevent unauthorized use. Examples of DRM include the FairPlay system used by Apple to enforce licensing agreements on music downloads, the content scramble system (CSS) scheme used to encrypt video on DVDs, and the DVD region code used to limit DVD playback to certain devices sold within a geographic area. Business and personal productivity software typically comes with DRM that requires a unique license key to activate the product. DRM is not a perfect solution, as individuals have produced both digital and analog means of circumventing DRM, al-

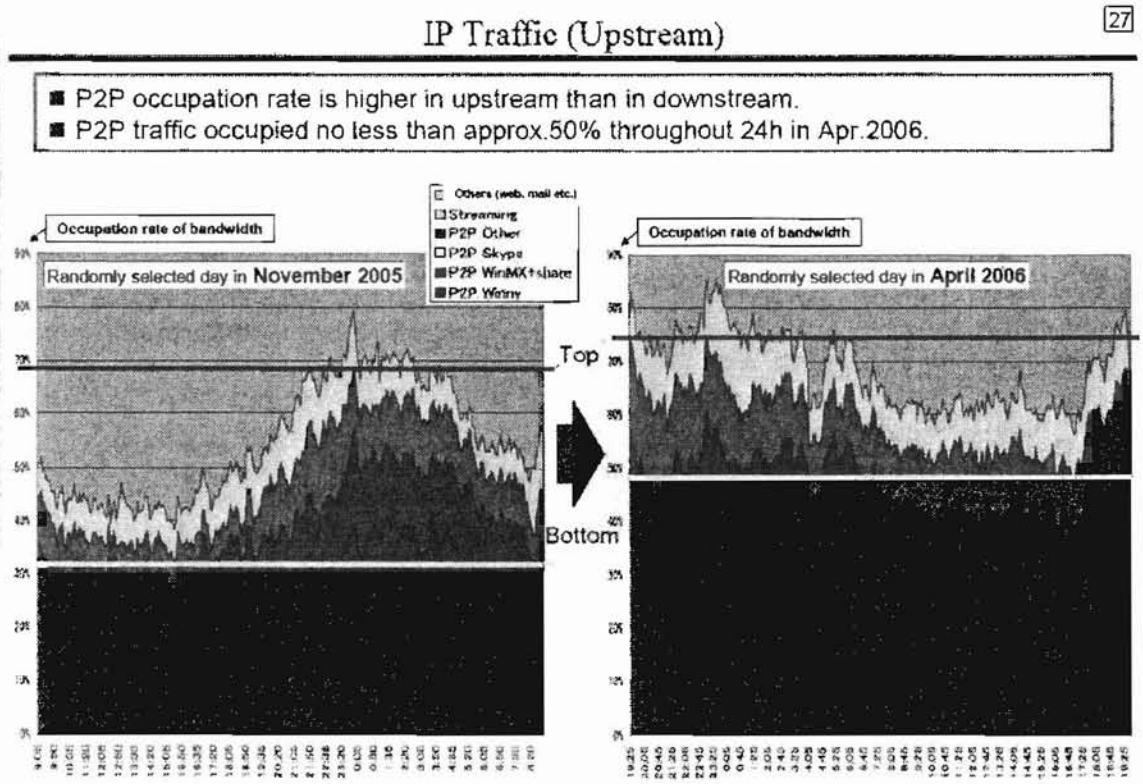
though such activity was rightly made illegal by the Digital Millennium Copyright Act (DMCA). However, DRM does deter from piracy many users who, in the absence of DRM, would illegally copy the digital content.

DRM also typically imposes additional requirements on the user that can, in some cases, reduce the value of the product. For example, DRM may require Internet access to connect to a licensing server, making use of certain software or media more difficult on an offline PC. DRM can also create interoperability challenges, especially for proprietary technology, as not all devices may support all DRM implementations. For example, an e-book downloaded from Amazon for the Kindle may not be compatible with a Sony e-Book reader. While initially most of the music sold online contained DRM, the trend within the music industry now seems to be towards DRM-free music, as Apple's iTunes store and Amazon, two of the largest online retailers, have moved away from selling music tracks with DRM. The trend with e-book retailers continues to be to implement DRM. DRM is also appearing in some computer hardware and consumer electronics. For example, as video cards have adopted digital outputs, many have implemented digital copy protection schemes to prevent unauthorized copying of high-definition digital video. Televisions in the future could also contain anti-piracy devices that would prohibit the playback of copyright-protected content.

NETWORK MANAGEMENT

Internet service providers (ISPs) around the world are replacing "all you can eat" unlimited service plans with volume-bounded service plans or usage-sensitive pricing plans. A recent OECD report found that as a result of growing use of high bandwidth applications, including P2P applications, "some operators responded by imposing limitations on the amount of bandwidth that users are allowed to transmit in a given month. These bit caps were typically found in island countries with limited international transmission capacity, but they have now appeared in other OECD countries as well. Currently there are offers with explicit bit caps in two-

Figure 2: Increase in Upload Traffic in Japan and the Role of P2P Traffic



thirds of OECD countries."[24] For example, a March 2007 survey found that almost 95 percent of broadband subscribers in New Zealand had plans with a data cap of 5 gigabytes or less.[25] In Japan, ISPs also place a monthly limit on uploads, which effectively throttles P2P use; this cap is in place despite the enormous capacity of last-mile networks in Japan, which can be as high as 1 gigabit per second.[26] The actions were taken by the ISPs because, as shown in the graphs, P2P traffic makes up a significant portion of Internet traffic.

These moves are an indirect reaction to digital piracy, because pirates constitute the largest group of Internet users engaged in uploading and downloading the largest amounts of content. For example, in Japan, the Ministry of Communications reports that over 50 percent of broadband traffic is from P2P file sharing, most of it illegal. And these high bandwidth-using pirates cost ISPs more to serve, thereby, in the absence of volume-based plans, leading to higher prices for all consumers. This is a particular problem for rural ISPs, because they pay more for Internet transit than their better-connected urban counterparts and frequently rely on wireless last-mile connectivity that is harder to accelerate than wireline systems. In addition to usage caps, some ISPs around the world, particularly cable systems that have more limited upload capacity, have adopted systems that lower the priority of packets flowing to and from their heaviest users during periods of high network load.

While network traffic management systems are more a reaction to the problems piracy cause to network performance than an effort at mitigation, their use has been criticized by proponents of open access to copyrighted material on grounds that they limit free expression. Public Knowledge's technical consultant Robb Topolski has described such systems as a form of "discrimination based on user-history [sic]" that should be forbidden under network neutrality laws.[27] But to the extent that such systems provide a better Internet experience for the majority of law-abiding customers, they are actually pro-consumer.[28]

Network management tools are also used by colleges and universities where unauthorized file sharing is common. Given that these P2P file sharing networks are used predominantly for the illegal exchange of copyrighted content and their use limits the amount of bandwidth available for legitimate research and academic purposes, some university network operators have implemented network management schemes to block or degrade the use of certain P2P services. Many universities acted swiftly to implement bans on certain P2P file sharing applications in the early days of P2P file sharing networks. For example, in August 2000, 34 percent of U.S. universities banned their campus Internet users from using Napster.[29]

While network management is not a rights enforcement tool, it is a necessary part of a comprehensive mitigation strategy against harms caused to the Internet ecosystem by piracy. The Internet is a shared resource system by design, and those who attempt to consume more than a fair share of resources without paying an additional price to cover these extra costs make it less responsive to others, whether they are engaging in piracy or not. Internet regulators must remain mindful of the impact that piracy has on legitimate network users and should not limit or ban reasonable network management practices that enforce fair sharing of network resources.[30]

P2P NETWORK POLLUTION

Because a great deal of piracy begins with users uploading torrent files to indexer sites like The Pirate Bay and Mininova, rights enforcement efforts sometimes take the form of polluting these sites with bad copies of content files. The process begins with a rights holder uploading a torrent file to the indexer site and seeding one or more computers with fake copies of an apparently pirated movie or television program. HBO employed such tactics to limit the piracy of its popular series *Rome* by running systems on P2P networks that advertise that they have a portion of the pirated file but sending the wrong data to downloaders. Although P2P file sharing clients can detect and recover from this tactic, it can significantly slow down the download process.[31] A similar strategy was used by the music industry to frustrate users who attempted to download unauthorized copyrighted music files from P2P networks like Kazaa. The recording industry flooded the P2P networks with files that appeared to be high-quality recordings, but instead only contained a brief clip of the music followed by static. Techniques such as this are used to make illegal file sharing more difficult than legally acquiring the content but have generally been ineffective at significantly scaling back digital piracy.

Such strategies are often quite effective if pursued diligently enough, because piracy between parties who are not known to each other depends largely on trust, but indexer pollution has the effect of moving would-be pirates to private indexers with administrative staff who monitor torrent files for quality. Gaining access to a private indexer typically requires an invitation, and for that reason private indexers have smaller numbers of users, but such sites are much harder to invade and pollute than public indexers.

CONTENT IDENTIFICATION

Content identification systems recognize copyrighted content so that copyright owners can take steps to reduce digital piracy. Using these systems, copyrighted content can be detected by automated means if others try to share it on file sharing networks or websites. The technology can be deployed at various locations, including on peer computers, file-sharing networks, servers of user-generated content websites, consumer electronics, and at the ISP level as data passes through networks into and out of network endpoints. Various technologies can be used to identify content including digital watermarks, fingerprints, and metadata.

- **Watermarking** systems embed identifiable data in audio and video content that are invisible and inaudible to humans but easily recognized by content recognition systems. Unique watermarks are embedded in theatrical releases of movies in such a way that if someone records the movie with a camcorder and then distributes the video, the studio can still recognize the watermark and identify the source of the recording. Watermarks are also used, in conjunction with DRM, on optical media such as DVDs and Blu-ray discs to prevent and detect unauthorized copying.[32] Watermarks can be difficult to remove—even when the content is purposely altered—and are therefore an important step in limiting the unauthorized distribution of licensed material.

- **Fingerprinting** is a means of extracting easily-recognized features from audio and video content that are not deliberately placed in the content but are nonetheless essential. For example, fingerprint detection systems may look for a given musical melody or voice clip in a song or soundtrack of a movie and match it to a melody in a music database, in much the same way that music discovery systems, such as the mobile phone application Shazam, operate. Similar fingerprinting technologies are also used for video. Using fingerprints, content owners can easily determine if their content has been uploaded to a website like YouTube, for example, which enables the website to reject the upload and prevent others from viewing or downloading it. Digital fingerprints can be highly accurate and difficult to defeat, and they have been implemented in various well-known content identification systems such as Audible Magic and Vobile.

- **Metadata** systems look for the content identifiers used by piracy-enabling P2P applications, such as BitTorrent, for database matches with known unlawful content. When content is made available through piracy indexes such as the Pirate Bay or Mininova, an identifier called a hash tag is calculated based on the entire contents of a file, which enables the file to be uploaded and downloaded without ambiguity. A given piece of content may be made available for piracy in a number of formats, and each unique format will generate a new hash tag, so keeping the database of unlawful hash tags up to date can be challenging. Hash tags can also be obscured by encryption, but rights holders have found back doors into piracy encryption systems that allow them to decrypt and inspect unlawful content.[33]

Each of these systems employs a database, a feature-extraction system, and a pattern-matching engine that together are similar to the systems that are commonly used to block spam and protect personal computers from viruses and other forms of malware. As with these protection systems with which most people are familiar, content recognition systems are not perfect. Some may miss certain unlawful transactions and may falsely identify others, but on balance they are useful tools that can decrease the incidence of piracy wherever they are employed. Moreover, some tools today are highly accurate and through innovation the technology can, and likely will, improve even more.

BLOCKING INTERNET USERS FROM WEBSITES THAT INDEX OR TRACK PIRATED CONTENT

Critics of piracy mitigation have focused most of their attention on the supposed drawbacks of filtering, and have tended to ignore alternate approaches that are either supplemental or independent to filtering. One