Before the

PATENT AND TRADEMARK OFFICE AND

THE NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION,

U.S. DEPARTMENT OF COMMERCE

Washington, DC

In the Matter of	)
The Inquiry on Copyright Policy, Creativity,	)
And Innovation in the Internet Economy	)
Docket No. 100910448–0448–01	)

COMMENTS OF

THE INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION

October 27, 2010

Daniel Castro, Richard Bennett and Robert Atkinson

Information Technology and Innovation Foundation[1]
1101 K Street NW, Suite 610
Washington, DC 20005

[1] ITIF is a nonprofit, non-partisan public policy think tank committed to articulating and advancing a pro-productivity, pro-innovation and pro-technology public policy agenda internationally, in Washington and in the states. Through its research, policy proposals, and commentary, ITIF is working to advance and support public policies that boost innovation, e-transformation and productivity.

Introduction

The Information Technology and Innovation Foundation (ITIF) is pleased to submit these comments in response to the Notice of Inquiry from the Depart of Commerce's Internet Policy Task Force seeking input on the challenges of protecting copyrighted works online and the relationship between copyrights and innovation in the Internet Economy. In these comments, ITIF argues that unchecked digital piracy is a threat to the economic welfare of the United States and that more can, and should, be done to limit unauthorized use of copyrighted content online.[1]

Critics of stronger enforcement of intellectual property online claim that such efforts will harm the Internet and negatively impact the Internet ecosystem. This claim seems to assume that piracy is the bedrock of the Internet economy, an assertion not backed up by any evidence. There are many ways to use the Internet that do not infringe on content licenses, such as interpersonal communication, shopping, social networking, education, and legal downloading of content. As these uses are valuable they will continue to grow regardless of the steps taken to limit unlawful behavior. Moreover, limiting anti-piracy technologies will certainly limit innovation in this part of the Internet economy. This type of innovation is not only useful for developing better anti-piracy tools, but the same technology can be applied to develop new features and services for consumers. And to the extent that these and related technologies (e.g., filters to identify spam or malware) improve, the overall Internet innovation ecosystem will benefit since the Internet will be more trustworthy and secure.

Rather than limiting Internet innovation, as some assert, protecting copyrighted works online is necessary for innovation to continue to thrive on the Internet. While some anti-piracy proposals impose too much of a burden on businesses and consumers, many anti-piracy efforts do not negatively impact the Internet ecosystem. The goal of policymakers should be to identify and encourage as many of these tools and techniques as possible. The Internet is a tremendous enterprise of user empowerment, free speech, and innovation, but it also facilitates an enormous amount of unlawful acts. While the Internet is a vast, distributed system that has no central point of control, it should not be without any control whatsoever. Rather, the responsibility for maintaining the Internet commons falls upon each user, each service provider, and each business and institution that uses it, operates it, and benefits from it. The U.S. government needs to put in place a framework that facilitates and encourages responsible control.

In recent years, the combination of broadband Internet access and cheap storage has led to a growing increase in digital piracy. Piracy has significant costs in terms of lost jobs, and higher prices and relatively less content (both in terms of quantity and quality) for law-abiding consumers and organizations. While there is no silver bullet for stopping piracy, there is a large array of "lead bullets" that collectively can significantly reduce its prevalence. These include teaching consumers that digital piracy is unethical and illegal, applying technical means to stop piracy, restricting the financial gains of copyright infringers, and engaging in stronger enforcement of the legal rights of content owners.

Digital Piracy Remains a Significant Problem for the United States

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 industries that produce creative works—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.

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 Hotfile) and online streaming services (e.g. YouTube, Metacafe, and Livestream.com). While all of these technologies have legitimate uses, the technologies are 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 some P2P networks are focused on distributing legal content.[2] Websites like the Pirate Bay, and isoHunt, and Btjunkie routinely rank among the most popular websites on the Internet and offer the ability to illegally download virtually all popular TV series, movies, recently released songs, software and games.[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.

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. But it ultimately also hurts law-abiding consumers who must pay higher prices for content, enjoy less content, relatively lower quality 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 (and no one could tell if the car you are driving is stolen), 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.'"[4] This survey also reflects the mentality of many people who think that "everybody is doing it" or that piracy is just "a function of the Internet."[5] Moreover, the Internet gives users a sense of anonymity where the risk of getting caught is relatively low and that of punishment even lower.

While the exact cost of digital 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]

Neither are software companies immune from piracy. The Business Software Alliance estimates that worldwide four out of ten software programs installed on a PC were pirated.[12] 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.[13] 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.

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.[14]

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.[15] 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.[16] Alexa.com, which provides a global ranking of websites, currently lists RapidShare as the 26th most popular website in the world, and no wonder since users can pirate content using its services with impunity.[17]

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.[18] 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.[19] 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.[20] 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.

New Tools Are Necessary to Prevent Internet Piracy

While the existing notice and takedown regime has provided a good initial step at combating piracy clearly more can and needs to be done. 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 or that society in general, and the U.S. in particular (as the leading producer of digital content) 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.

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 and the government should engage with all stakeholders, including content owners, website operators, ISPs, ad networks and other intermediaries, on how to improve the global response to piracy.

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.

Change 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 studies 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 illegally 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 Russian websites, including MP3Million.com and LegalSounds.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. In addition, as discussed below, the federal government should develop a blacklist of sites that exist primarily to illegally distribute copyrighted content and widely publicize this list so that consumers who want to do the right thing can have the information they need to do so.

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, although 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.

Some DRM proposals do not strike the appropriate balance between the needs of copyright holders and consumers. For example, the Security Systems Standards and Certification Act (SSSCA) proposed by Sen. Ernest Hollings (D-SC) in 2001 would have imposed broad DRM requirements on many general purpose technologies, such as PCs. DRM may also impose 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. These types of more narrowly-focused DRM technologies are more efficient and cost-effective than the heavy-handed DRM proposals of the past.

Differential Network Pricing

Users who download pirated content consume bandwidth that could otherwise be used for legitimate purposes. Since many users have unlimited service plans they do not have any financial incentive to restrict their Internet use to non-copyright infringing activities. One solution to this is for Internet service providers (ISPs) to replace "all you can eat" unlimited service plans with volume-bounded service plans or usage-sensitive pricing plans. This is already happening in many places. 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."[21] Although these bit caps were typically found in island countries with limited international transmission capacity, they have now appeared in OECD countries as well. Currently there are offers with explicit bit caps in two-thirds of OECD countries. 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.[22] 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.[23] The actions were taken by the ISPs because 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.

Network Management

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.[24] By this logic, charging consumers more for keeping their air conditioners on at 65 degrees all summer compared to those who conserve energy, is also "discrimination" and should be prohibited by public

utility commissions. But because such systems provide a better (and relatively lower cost) Internet experience for the majority of law-abiding customers, they are actually pro-consumer.[25]

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.[26]

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.[27]

P2P network pollution

Because a great deal of piracy begins with users uploading torrent files to indexer sites like The Pirate Bay and Btjunkie, 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.[28] 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.[29] 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 Btjunkie, 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.[30]

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.

Deep Packet Inspection

Some ISPs have also begun to use deep packet inspection (DPI)-based content recognition systems to identify users who download copyrighted material. Critics of DPI, such as Public Knowledge, claim that DPI-based content recognition will reduce Internet performance, violate free speech and personal privacy,

and raise the price of Internet access, all the while failing to protect rights holder interests in any significant way.[31] Each of these criticisms is incorrect.

First, content identification systems do not affect latency. Some content recognition systems use parallel processing to perform additional pattern-matching activities (beyond the destination network address) at the same time that basic routing functions are performed and do not add delay. Other, less expensive systems send a copy of each packet to be examined to an out-of-band system that performs analysis in its own time. Since these systems are not in the forwarding path of network traffic, they also do not add delay.

Second, content identification systems are not a threat to personal privacy or free speech. Internet packets are routinely examined by automated systems on the Internet today and always will be; the nature of Internet routing requires examination in order for packets to be delivered. Privacy only becomes an issue when packets are retained, analyzed, shared, or viewed by an individual. As long as these activities are performed in a responsible way in accordance with legal guidelines, there is no particular basis for worry. It is certainly true that a poorly-designed piracy detection system may incorrectly flag some lawful transactions and that is why it is imperative that such systems are not allowed to disrupt such transactions or take punitive actions against suspected pirates without proper human oversight. However license enforcement systems currently in use or in development target entire downloads of movies, television programs, and music on a repeated basis by major infringers. The gulf between this kind of behavior and the minor instances of confusion with protected activities is so large as to strain credulity. Free speech rights do not imply the right to make unlawful copies of other people's copyrighted works, regardless of the final purpose. Proper oversight can ensure that protected forms of speech which use a portion of copyrighted material within the bounds of the law are recognized as such by content identification systems.

Third, the cost of content recognition can be high or low according to the particular implementation strategy for the system. The ultimate goal of such systems is simply a meaningful reduction in lost sales of licensed material and to capture new sales, and this can be accomplished by a system of spot checks in random locations sufficient to communicate to would-be pirates the possibility of detection. Changing behavior in a positive direction is the goal of criminal justice; perfecting humanity is not. Policymakers should allow experimentation to determine the actual cost of content recognition. If these systems are in fact uneconomical (i.e., the cost is significantly more than the benefits of reduced piracy), this fact will come to light and the experiment will be halted until such time as the economics change. Until such time, ISPs should be allowed to balance the utility they provide against the costs of such systems.

Blocking Internet users from websites that index or track pirated content

Critics of piracy mitigation have focused most of their criticism on the supposed drawbacks of filtering, and have tended to ignore alternate approaches that are either supplemental or independent to filtering. One alternate approach focuses on the websites and technologies that exist for the sole, primary, or significant purpose of enabling digital piracy. Enabling digital piracy is a profitable business, and there can be little doubt that profiting from unlawful activity is indefensible. There is also little difficulty in recognizing such sites, as they often fail to respond to legitimate takedown notices, or fail to do so in a timely manner, and prominently display indexes of unlawful content.

One such site is The Pirate Bay, which a Swedish court found in 2009 to have engaged in unlawful conduct. In a statement, the court said, "The court has found that by using Pirate Bay's services there has been file-sharing of music, films and computer games to the extent the prosecutor has stated in his case. This file-sharing constitutes an unlawful transfer to the public of copyrighted performances."[32] The four founders of The Pirate Bay were sentenced to a year in prison and ordered to pay fines of $3,620,000. Pending appeal, the web site is still operational, although it has stopped operating a BitTorrent tracker in favor of an alternate form of content discovery known as Distributed Hash Tables (DHT) that is more difficult to block. As explained by The Pirate Bay, "The development of DHT has reached a stage where a tracker is no longer needed to use a torrent. DHT…is highly effective in finding peers without the need for a centralized service."[33] The Pirate Bay apparently hopes to escape future liability by discontinuing its "tracker" service. While The Pirate Bay is not directly involved in transferring packets between unlawful file sharers, it provides the vital role connecting digital pirates to each other, acting as a procurer of piracy services.

Even before the Swedish court rendered its verdict, there was no doubt that The Pirate Bay existed for unlawful purposes. Not only does the site offer detailed, hand-created indexes of unlawfully copied TV shows (http://thepiratebay.org/tv) and music (http://thepiratebay.org/music), it also provides access to unlawful versions of software, books, and games. Moreover, while the owners of the site claim they are acting on moral grounds (fighting for internet freedom) the site is supported by the sale of advertising.

It should come as no surprise that the site has been ordered off the Internet by the court. What is surprising is that Internet service providers have not acted to block websites such as this that clearly facilitate the exchange of illegal content when it would be quite simple as a technical matter to block them. Blocking these websites could be achieved by blocking DNS queries or connections to IP addresses hosting these piracy websites. For example, an ISP could blackhole DNS queries to the domain names, such as thepiratebay.org, or redirect them to the Justice Department.[34] While The Pirate Bay may respond by changing its domain name, blackhole lists can generally be updated as easily as new domains can be registered. But absent federal government mandates to block sites like The Pirate Bay, it may not be in the interest of any individual ISP to block these sites since doing so would reduce its attractiveness to customers who want to engage in digital piracy and would surely also incur the wrath of so-called public interest advocacy groups who at best turn a blind eye to digital piracy. An ISP could also block the IP addresses used to host such websites. In both of these approaches, the government or some other well-recognized and responsible party may need to be responsible for publishing a real-time list of domain names or IP addresses to block.

In September 2010, Senators Patrick Leahy (D-VT) and Orrin Hatch (R-UT) introduced S. 3804, the "Combating Online Infringement and Counterfeits Act" (COICA) which would implement this recommendation.[35] The legislation would not target minor violations of copyright. Rather, it would target "Internet sites dedicated to infringing activities" which it defines as a site that is "primarily designed, has no demonstrable, commercially significant purpose or use other than, or is marketed by its operator…to offer" unauthorized access to copyright-protected content. COICA provides two legal remedies for addressing online infringement depending on whether the infringing site is based domestically or abroad. For domestic sites, the Attorney General can request a judge issue a court order to require that a U.S.-based domain registrar (e.g. GoDaddy.com) or the U.S.-based registry (e.g. VeriSign) to suspend the domain name. Doing this would mean that users who type in this domain in their browser would receive

an error message stating that the site is unavailable. For nondomestic sites where the United States does not have jurisdiction to require that the domain name be suspended, the Attorney General can request a court order requiring ISPs to block access to the infringing sites, credit card companies to suspend processing transactions for them, and ad networks to suspend serving ads to these sites. The Attorney General would also (through the U.S. IP Enforcement Coordinator) publish a list of all domain names that the courts have found to be infringing on copyright-protected content. In addition, the Attorney General would also publish a list of sites alleged to be dedicated to infringing on copyright-protected content, but where a court order has not yet been obtained. ISPs, credit card companies and ad networks would all have legal immunity for taking action against any site appearing on this list. The Attorney General would provide a set of procedures for owners and operators of sites to have their domain removed from the list and to obtain judicial review.

While blocking is one possible solution, that technology—like like virtually every technology ever invented—can obviously be used for both good and bad purposes. Several countries, some of which have anti-democratic aims—such as China, Cuba, Iran and North Korea—have blocked access to certain websites with varying degrees of success. However, blocking technologies can be used for pro-democratic, pro-consumer purposes. In the United Kingdom, as many as 80 percent of ISPs use the blacklist published by the Internet Watch Foundation, a non-profit organization that maintains a list of offensive websites.[36] According to its mission statement, the Internet Watch Foundation works to minimize the amount of "child sexual abuse content hosted anywhere in the world and criminally obscene and incitement to racial hatred content hosted in the UK."[37] So clearly this is a precedent for limiting what is available on the Internet and it does not lead to the so-called slippery slope that the apologists for Internet piracy claim is next.

These systems are not perfect, of course, and there have been isolated incidents in which they've filtered legitimate content. This is why such systems need to provide a means of correcting classification errors. If a country chooses to implement this type of solution, it should be careful to craft policies that ensure that the technology is not abused to limit legitimate free speech and openness, and that mistakes can be remedied. For example, any publisher of a blacklist of unlawful file sharing sites to which ISPs would be required to block access should be required to provide a credible and responsive means for wrongly identified services to protest and be removed from the list and for correctly identified services to be unblocked after removing the offending content. Real-time blacklists have proved useful for combating spam and distributed denial of service attacks, hence it is reasonable to apply them to piracy as well, with suitable controls. There is nothing inherent about the Internet, nor should there be, that precludes the limitation of some kinds of content on it. Just as in society as a whole, there are limitations in all societies on some kinds of content and behavior.

Blocking Internet users from websites that offer pirated content

In addition to P2P networks, a large amount of pirated digital content is available on websites for either direct download or streaming. Just as with legitimate websites, these sites generally come in two formats, an ad-supported model and a paid content model.

Currently, Internet users can easily go online and, with just a few clicks, find full-length Hollywood movies to watch for free. Websites like Movie2k.com (www.movie2k.com) provide indexes of movies and television video programming available to watching instantly for free online. These websites link to

streaming sites such as Movshare (www.movshare.net), Stream2k (www.stream2k.com), MegaVideo (www.megavideo.com), Divxstage (www.divxstage.net), and Novamov (www.novamov.com) that allow users to upload and share movie-length videos at no cost to the user. Live programming is also recorded and distributed online through websites like Livestream.com and Justin.tv. This form of piracy is used to pirate live sports events, such as NBA, NFL and MLB games, to Internet users, including international users who cannot otherwise gain access to the programming. This form of piracy is particularly strong in China where millions of users watch pirated U.S. sports programming online.[38] One reason that pirates are using websites to distribute copyrighted content is that bandwidth and storage are relatively cheap and these costs can be supported by advertising.[39] These ad-supported websites offer copyrighted content online at no cost to the user and profit by selling advertising for content that they have pirated.

Other websites sell pirated content online while often masquerading as legitimate businesses. These piracy sites often have the look and feel of legitimate online stores such as iTunes or Amazon.com. One such site is the Russian website LegalSounds.com, which poses as a music store and charges membership fees. A hapless consumer wishing to obtain digital music lawfully could easily be confused by the LegalSounds.com website, which includes a "legal-sounding" terms of service agreement and the trappings of a legitimate service. When a site is named "LegalSounds.com" and says prominently on its home page "download music that is free, legal," it is not surprising that many law-abiding consumers would believe that they are not breaking the law. One might reasonably conclude that the content offered is legitimate and enroll in the service.

Existing laws against fraud and false advertising apply to such sites, but the Internet enables them to spring into existence, change identities, and move about much faster than the legal system can keep up with them. Moreover, many of these sites are in nations where the service is legal or where the national government turns a blind eye to enforcement. Once again a simple blocking solution at the ISP level may be the most effective means of preventing Internet users from using these websites to engage in digital piracy domestically. Such a system could divide the burden of initial enforcement between rights holders and ISPs and could be overseen by the Federal Trade Commission or the Department of Justice. Real-time mechanisms such as this are necessary to deal with real-time Internet offenses and are entirely appropriate, provided that falsely identified parties have equal real-time recourse to prevent abuse.

Blocking Internet users from search engine services providing access to piracy websites

Another enforcement measure that does not depend on filtering is blocking access to piracy services by Internet search services such as Google and Bing. There is no compelling reason why these services should provide easy access to unlawful content or why they should be immune from responsibility for the action of selling advertising for indexing piracy sites. If these services know enough about the searches they perform and the sites they index to match ads with searches, they surely should know enough to block unlawful sites from their search results. (In fact, in 2009 The Pirate Bay was "accidentally" removed from Google's search results, but Google manually reinstated the website.[40]) All it takes for search engines to stop the practice of facilitating piracy is a commitment to not support websites that engage in unlawful acts. A search engine that can place appropriate ads on a page showing pirated content can suppress the content as well. However, for such sites to do this, they need to know that they will not be attacked by government or by those opposed to serious efforts to fight digital piracy.

Blocking funding for websites and organizations that support piracy

Websites and organizations that facilitate piracy require funding to stay in business. As described earlier, these websites often get funding through online advertising or through direct sales of pirated content. One way to reduce piracy is to block these sources of funding so as to make piracy unprofitable or less profitable.

Many websites that facilitate piracy fund their efforts through online advertising. For example, the website isoHunt promotes its website to potential advertisers as follows: "[Our website] attracts more than 16 million unique visitors every month. Do you sell products that you think will attract early adopters? MP3 players, computer / console hardware, or gadgets of all sorts? Advertise with us!"[41] Online advertisers include major brands that advertise either directly on these websites or indirectly through advertising networks that do not choose to distinguish between websites that facilitate piracy and those that do not. For example, a review by ITIF in 2009 of the advertisers on the websites The Pirate Bay and isoHunt found brands such as Amazon.com, Blockbuster, British Airways, and Sprint.[42] Responsible companies should not advertise on websites that facilitate piracy and responsible ad networks should not buy placement on these websites.

Banks should also restrict customers from using their credit and debit cards to make payments to the websites that sell pirated content. Similar restrictions have already been put in place by banks and credit card issuers to limit payments and credits for online gambling with some success.[43] This type of effort was used briefly to limit piracy when the recording industry requested that Visa and MasterCard block credit card payments to the Russian website allofmp3.com that was selling unauthorized copies of digital music. Unfortunately, after the operators of allofmp3.com sued to reverse this action, a Russian court ruled in favor of the website owners and stated that credit card companies could only break their contracts when their customer was found guilty of a crime.[44]

Enforcing Legal Rights of Content Owners

Content producers have also used legal means to protect their interests, including pursuing criminal and civil penalties against organizations and individuals engaged in or enabling copyright infringement.

Lawsuits against organizations facilitating digital piracy

Content producers have used legal means to shut down organizations that facilitate illegal file sharing. Major file sharing enterprises, such as Napster and Grokster, have been rightly shut down by court order following lawsuits by industry groups such as the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA).[45] While the U.S. Department of Justice filed motions in support of the industry in these efforts, it took relatively little action to prosecute the individuals or organizations engaging in this activity.

Initially, the makers of file sharing software and operators of file sharing networks used two main arguments in defending the legality of their operations: one, that they did not make copies of copyrighted content and thus were not infringing on copyrights; and two, that their activity was protected under the ruling in the Betamax case that protected technology makers from being liable for misuse by users. Specifically, in the case Sony Corp. of America v. Universal City Studios, Inc., the majority opinion wrote that "the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial non-infringing uses."[46]

Many of these arguments came out in Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd., in which the file-sharing service Grokster was sued by content producers for distributing P2P file sharing software. The record companies and movie studios showed that not only did the Grokster file sharing service enable the exchange of any electronic file, including copyrighted files, but that Grokster specifically encouraged this type of use and profited from it. In a unanimous decision, the U.S. Supreme Court ruled against Grokster, stating, "We hold that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties."[47] This case made clear that the owners of applications or services designed to enable file sharing of copyrighted content could be held liable for infringement by third-parties. Moreover, this case was part of a series of court rulings around the world in countries such as Australia, South Korea, and Taiwan, that found certain P2P file sharing networks liable for copyright infringement.[48]

In response to legal pressure in certain countries, organizations that facilitate unauthorized online file sharing, such as The Pirate Bay, have located themselves in countries where weaker laws and weaker enforcement protect them from criminal and civil lawsuits for copyright infringements. For example, The Pirate Bay operated for many years in Sweden before authorities began criminal prosecution of the individuals involved in the website's operations, leading the head of the MPAA to brand Sweden "an international piracy haven."[49] Some lawsuits have been successful in restricting websites that enable piracy. For example, in 2009, a Dutch court forced the four-year-old torrent tracking website Mininova to remove all links to infringing content and it has since dropped in rank from the 96th most popular website in the world to the 2,552nd.[50]

Digital piracy, both online and for physical media, is especially high in countries like China and Russia which generally have less protection for intellectual property. For these nations, piracy is a way to get content from developed nations without paying (and to enable those hosting pirate sites to make money), thereby increasing the trade surplus they enjoy with many nations. Agreements between countries are necessary to coordinate effective responses to digital piracy. International treaties and trade agreements such as the World Intellectual Property Organization (WIPO) Copyright Treaty and the Anti-Counterfeiting Trade Agreement (ACTA) can help facilitate enforcement of intellectual property rights worldwide.

Lawsuits against Internet users engaging in digital piracy

In addition to pursuing legal action against businesses supporting copyright infringement, organizations such as RIAA and MPAA have filed numerous lawsuits against Internet users suspected of distributing copyrighted content without authorization. While RIAA has been much more prolific in filing lawsuits against thousands of Internet users suspected of copyright violations, MPAA has filed hundred of lawsuits as well.[51] These lawsuits target individuals based on the IP address of suspected file sharers and typically result in out-of-court settlements. The motivation behind these lawsuits is to stop some of the most egregious examples of file sharing (e.g., users that upload large numbers of unauthorized files) and to increase the risk associated with unauthorized file sharing. However, pursuing lawsuits against individuals is an expensive process and does not scale well to the millions of users on the Internet who choose to download copyrighted content.

In combination with the lawsuits by content creators, these industries have also established amnesty programs to provide a means for users who download copyrighted content to avoid expensive lawsuits. RIAA created the Clean Slate program in 2003 that promised not to prosecute individuals who deleted and destroyed all unauthorized content that they had downloaded and promised not to infringe on copyrights in the future. More recently, Nexicon, Inc., a company that develops content identification tools and works on behalf of copyright owners, launched GetAmnesty.com. If Nexicon identifies the IP addresses of an Internet user suspected of downloading or sharing a copyrighted file, Nexicon will contact the user and provide a list of the files it believes were illegally downloaded. The user then has the option of paying for the copyrighted content on the GetAmnesty.com website and in return the rights' holders who contract with Nexicon will agree not to file a lawsuit against the user for distributing or downloading the copyrighted content.

Notice and response to copyright infringement

In large part because of some opposition by the public, in 2008 RIAA halted its strategy of suing individuals suspected of illegally pirating large amounts of digital music and announced that it would instead work with ISPs to alert Internet users of potentially illegal activity. Under this framework, the content producers identify individual Internet users suspected of illegal file sharing by their IP address and then send the ISP the relevant information including the name of the infringing work, the filename, a time and date stamp, the IP address, IP port, and the file sharing network downloaded from. The ISP does not turn over any personally identifiable information to the copyright owners, but instead relays the message to their customers.

Discovering the IP address of Internet users engaged in online piracy on peer-to-peer networks is relatively straightforward. One such means is to request a piece of unlawful content and thereby enter the "swarm" of P2P users engaged in sharing or seeding it at the same time. Members of a P2P swarm are allowed to see the IP addresses of each other member of the swarm, without encryption. These addresses are perfectly transparent, which belies the claim that file sharers have any expectation of privacy. By providing notice of copyright infringement, users become aware that they are responsible for their actions online and can take steps to stop unauthorized use, such as ceasing to download pirated material, securing a wireless router or supervising a teenager, before facing more serious consequences for misuse. Even after serving notice, content producers still retain the right to sue individual Internet users for copyright violations. Such notices can be reasonably effective, if for no other reason than some consumers may not be aware that they are engaging in illegal action, while others who do know may not know that they are being identified as engaging in illegal actions.

Major ISPs in the United States, including Comcast, Verizon, and AT&T, participate in this arrangement with some copyright holders. For example, as of 2009, Comcast reports that it has issued 2 million notices on behalf of copyright owners.[52] 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. Cox Communications, for example, has made this a standard practice. As described by a Cox spokesperson, "When we receive notifications from RIAA or other copyright holders stating that their copyrighted material is being infringed by a customer, we pass that information along to the customer so they can correct the problem, or dispute the notice directly with the copyright holder if they feel the notice was sent in error. This notification is the most helpful thing we can do for the customer and is expected of us, as an ISP, under the DMCA. We attach a copy of the notice

from the copyright holder with our message to the customer."[53] Although Cox sent out many notices, it has only terminated access for one-tenth of one percent of those users. Comcast has stated that it has no plans to terminate access for its users. Several universities, including the University of California, have implemented rules to suspend the Internet access of students that use campus networks for illegal file sharing. Such practices, including alternatives such as bandwidth capping, browser redirection, and temporary suspension of service, can play an important role in limiting the actions of Internet users who repeatedly engage in digital piracy.

A notice system has been used with some success in other countries as well. In particular, some other nations have required ISPs to participate in these programs. For example, Sweden implemented the European Union's antipiracy directive, the Intellectual Property Rights Enforcement Directive (IPRED) in April 2009. The Swedish IPRED law requires ISPs, with a court's approval, to identify users suspected by copyright holders of illegally downloading copyrighted content. Copyright holders can then send a letter of warning to these Internet users, and if illegal activity continues, file a civil lawsuit against the infringers. A more effective law would not require court approval to send notices from copyright holders through the ISPs, as long as the notices are issued without revealing personal information. The International Federation of the Phonographic Industry (IFPI) Sweden recently noted that the legislation, in combination with growing popularity of online music services, appears to have been successful and reported that revenue for the record labels rose 18 percent in the first nine months of the year overall, and 80 percent in the digital market.[54] The legislation also had an immediate impact on Internet use the day it came into effect, with Internet traffic within Sweden dropping 33 percent because users were engaged in less illegal downloading of digital content.[55] The legislation has more recently become less effective, as some ISPs have taken action to reduce its impact by erasing all of their logs so that they are unable to comply with court orders. Some government officials have proposed new regulations that would require ISPs to maintain Internet usage logs for a minimum period, such as six months.[56]

In addition to using civil lawsuits and a voluntary system of graduated response from ISPs, some countries have implemented or are considering implementing "three strikes" laws that punish Internet users who download or distribute copyrighted material. These laws work by punishing repeat copyright infringers by cutting off their Internet access. France was one of the first countries to pass a three strikes law, and other countries including the United Kingdom, South Korea, and Taiwan have followed suit with their own legislation and regulations in this area. In France, the revised law approved by the Constitutional Council in October 2009 creates a new government agency that sends warning letters to Internet users suspected of downloading copyrighted content. Users who refuse to heed notices face losing their Internet access for up to a year and additional fees. Protections have been put in place to protect free speech by requiring that no users can lose their Internet access without their case first going before a judge.[57]

In the United Kingdom, the Digital Economy Act, approved in April 2010, has created a similar graduated response. The Act requires ISPs to forward on notices of copyright infringement from rights holders, track the number of notifications sent to a customer, and send this data to the copyright holders. The copyright holder then can take this information to a court to get the customer's name and address to take legal action against the user. ISPs that fail to fulfill these requirements face stiff financial penalties. Internet users who infringe on copyrighted content face increasing penalties from a warning to suspending

an Internet user's account. The Act does not make file sharing a criminal offense punishable with jail time.[58]

Industry has also implemented this technique of using service bans to discourage piracy. In 2009, for example, Microsoft banned a small percentage of users from the Xbox Live service for modifying their Xbox 360 consoles to play pirated games. While users can still use their console for playing games offline, they cannot use the Xbox Live service for online game play, which is a key part of many of the most popular multiplayer games.[59]

Conclusion

Digital piracy harms the U.S. economy, U.S. businesses and U.S. consumers. There is no legitimate reason for web sites that directly enable piracy to exist. The Internet was not meant to be a gigantic piracy machine. It was not designed or built for the primary, sole, or major purpose of facilitating unlawful transactions. Policymakers must do more to protect IP domestically and internationally by providing new tools to combat digital piracy and enforce copyright protections online.

Endnotes

1. For more on the problem of digital piracy, see Daniel Castro, Richard Bennett and Scott Andes, "Steal These Policies: Strategies for Reducing Digital Piracy," Information Technology and Innovation Foundation (December 15, 2009), http://www.itif.org/files/2009-digital-piracy.pdf.
2. While P2P file sharing is dominated by copyright content, some people mistakenly associate P2P only with file sharing networks. However, P2P technology encompasses many types of applications and services from the Skype-to-Skype dialing procedure to video streaming on mainstream websites like CNN. (Note: Skype is not truly a P2P application; it only does session initiation by P2P, the rest is a straight UDP session.)
3. As of November 2009, the Pirate Bay was ranked as 109th and isoHunt was ranked as 187th. "Alexa Top 500 Global Web Sites," web page, ND, http://www.alexa.com/topsites/global (accessed Nov. 28, 2009).
4. Mary Madden, "The State of Music Online: Ten Years After Napster," Pew Internet & American Life Project, 2009, http://www.pewinternet.org/Reports/2009/9-The-State-of-Music-Online-Ten-Years-After-Napster.aspx.
5. Eliza Krigman, "IP Enforcement Policies Stir Censorship Debate," Tech Daily Dose, October 22, 2010, http://techdailydose.nationaljournal.com/2010/10/ip-enforcement-policies-stir-c.php.
6. Stephen Siwek, "The True Cost of Copyright Industry Piracy to the U.S. Economy," Policy Report 189, The Institute for Policy Innovation, September 2007.
7. Measuring losses to piracy is an imperfect science because pirated software is not a perfect substitute for legally purchased software. The methodology varies by study on how to best quantify losses due to global piracy. First, it is uncertain what the actual rate of piracy is: some studies take the number of actual confiscated pirated products in police raids and assume they represent some percentage of the total number of pirated goods while other studies rely on surveys to estimate the number of pirated goods. The majority of studies evaluated here follow the latter methodology. Beyond this point there is a larger issue of determining to what degree pirated material represents a loss to the industry. In other words, how many pirated products would have been purchased legally if piracy was not an option? Some studies assume a one-to-one substitution, all pirated material would have been purchased and thus the market value of pirated goods represents the actual loss, an overly optimistic assumption. Other studies take a different approach and use surveys to determine what percentage of those who use pirated material would have purchased these goods if piracy was not an option. As with all survey research there is a large degree of uncertainty in the conclusions of these surveys. On the one hand, it is plausible that individuals are likely to tell a surveyor they would purchase legitimate goods when in reality they would not; on the other, it is also plausible that those who openly admit to owning pirated material are likely to be those who do not think piracy is wrong and are more likely to state that they would be unwilling to purchase legal copyrighted material. The point in all this is there is much uncertainty in the data.
8. These figures are for direct losses. Stephen Siwek, "The True Cost of Sound Recording Piracy to the U.S. Economy," Policy Report 188, The Institute for Policy Innovation, September 2007
9. These figures are for direct losses. Stephen Siwek, "The True Cost of Sound Recording Piracy to the U.S. Economy," Policy Report 188, The Institute for Policy Innovation, September 2007.
10. IFPI, IFPI 2008 Digital Music Report, IFPI, 2008, 8, http://www.ifpi.org/content/library/dmr2008.pdf.
11. Stephen Siwek, "The True Cost of Motion Picture Piracy to the U.S. Economy," Policy Report 186, The Institute for Policy Innovation, September 2006.
12. Business Software Alliance, "Piracy Impact Study: The Economic Benefits of Reducing Software Piracy," (2010), http://portal.bsa.org/piracyimpact2010/studies/piracyimpactstudy2010.pdf.
13. Business Software Alliance, Sixth Annual BSA-IDC Global Software 08 Piracy Study, BSA, May 2009, http://global.bsa.org/globalpiracy2008/studies/globalpiracy2008.pdf.
14. International Intellectual Property Alliance, Special Report 301, February, 2009.
15. Motoko Rich, "Print Books Are Target of Piracy on the Web," New York Times, May 11, 2009, http://www.nytimes.com/2009/05/12/technology/internet/12digital.html.

16. Randall Stross, “Will Books Be Napsterized?” New York Times, October 3, 2009, http://www.nytimes.com/2009/10/04/business/04digi.html.
17. “Alexa Top 500 Global Web Sites,” Alexa, ND, http://www.alexa.com/topsites/global;1 (accessed Nov. 28, 2009.)
18. Business Software Alliance, Sixth Annual BSA-IDC Global Software 08 Piracy Study, BSA, May 2009, http://global.bsa.org/globalpiracy2008/studies/globalpiracy2008.pdf.
19. IFPI, IFPI 2008 Digital Music Report, IFPI, 2008, http://www.ifpi.org/content/library/dmr2008.pdf.
20. Business Software Alliance, Sixth Annual BSA-IDC Global Software 08 Piracy Study, BSA, May 2009, http://global.bsa.org/globalpiracy2008/studies/globalpiracy2008.pdf.
21. Organization for Economic Co-Operation and Development (OECD),"Broadband Growth and Policies in OECD Countries," 2008, p 48.
22. Ibid.
23. “Three Strikes, Three Countries: France, Japan and Sweden | Electronic Frontier Foundation,” http://www.eff.org/deeplinks/2008/03/three-strikes-three-countries.
24. Robb Topolski, “Re: [p2pi] Follow-Up from Comcast Presentation,” June 6, 2008, http://www.ietf.org/mail-archive/web/p2pi/current/msg00072.html.
25. See George Ou, A Policymakes Guide to Network Management.
26. Gartner, “Gartner Reports Napster Banned at 34 Percent of Colleges and Universities,” Press release, August 30, 2000, http://www.gartner.com/5_about/press_room/pr20000830a.html.
27. For a guide to how network management techniques work, see George ou…
28. “p2pnet news » Blog Archive » HBO: poisoning BT downloads,” http://www.p2pnet.net/story/6515.
29. Jeffrey Lotspiech “The advanced access content system's use of digital watermarking” International Multimedia Conference, Proceedings of the 4th ACM international workshop on Contents protection and security, 2006, 19-22.
30. See, for example, the services offer for content providers by Vedicis. http://www.vedicis.com.
31. Mehan Jayasuriya, Jef Pearlman, Robb Topolski, Michael Weinberg and Sherwin Siy, “Forcing the Net Through a Sieve: Why Copyright Filtering is Not a Viable Solution for U.S. ISPs,” Public Knowledge, 1.
32. “The Pirate Bay Trial: The Official Verdict – Guilty,” TorrentFreak, April 17, 2009, http://torrentfreak.com/the-pirate-bay-trial-the-verdict-090417/.
33. “The Pirate Bay - The world's most resilient bittorrent site,” November 11, 2009, http://thepiratebay.org/blog/175.
34. A DNS blackhole is a system that returns a non-routable address for the Internet Protocol address of an unlawful or otherwise undesirable Internet service in response to a Domain Name Service (DNS) query.
35. Daniel Castro, “Better Enforcement of Online Copyright Would Help, Not Harm, Consumers,” Information Technology and Innovation Foundation (2010), http://www.itif.org/files/2010-copyright-coica.pdf.
36. “House of Commons Hansard Debates for 13 Feb 2006 (pt 5)”, House of Commons Hansard, Volume: 442, Part: 79 (February 13, 2006), http://www.publications.parliament.uk/pa/cm200506/cmhansrd/vo060213/debtext/60213-05.htm#60213-05_spnew1.
37. “About the Internet Watch Foundation,” Internet Watch Foundation (October 21, 2009), http://www.iwf.org.uk/public/page.103.htm
38. See “2008 Special 301 Report,” Office of the United States Trade Representative (2008), 10, http://www.ustr.gov/sites/default/files/asset_upload_file553_14869.pdf and Tim Arango, “Online Piracy

Menaces Pro Sports," The New York Times, December 28, 2008, http://www.nytimes.com/2008/12/29/business/29piracy.html.

39. See for example, http://www.mediafire.com/.
40. Greg Sandoval, "Google: Pirate Bay booted off search by mistake," CNET News (October 2, 2009) http://news.cnet.com/8301-1023_3-10366570-93.html.
41. "Advertise on the cutting edge," isoHunt, n.d., http://isohunt.com/advertise.php.
42. "The Pirate Bay: Sponsored by Wal-Mart," TorrentFreak (January 11, 2007), http://torrentfreak.com/the-pirate-bay-sponsored-by-wall-mart/.
43. Matt Richtel, "Citibank Bans Credit Cards From Use in Web Gambling," New York Times (June 15, 2002), http://www.nytimes.com/2002/06/15/business/15GAMB.html.
44. Nate Anderson, "Russian court rules that Visa must process payments for Allofmp3.com," Ars Technica (2007), http://arstechnica.com/tech-policy/news/2007/07/russian-court-rules-that-visa-must-process-payments-for-allofmp3-com.ars.
45. Shane Ham and Robert D. Atkinson, "Napster and Online Piracy," Progressive Policy Institute, May 1, 2000, http://www.ppionline.org/ppi_ci.cfm?knlgAreaID=140&subsecID=289&contentID=646.
46. Sony Corp. v. Universal Studios, Inc., 464 U.S 442 (1984).
47. MGM Studios, Inc. v. Grokster Ltd., 545 U.S 125 (2005).
48. Marybeth Peters, "Protecting Copyright and Innovation in a Post-Grokster World," Statement of Marybeth Peters, The Register of Copyrights before the Committee on the Judiciary, United States Senate, 109th Congress, 1st Session, September 28, 2005, http://www.copyright.gov/docs/regstat092805.html#N_5_.
49. John G. Malcolm, "The Pirate Bay," Letter to the Honorable Dan Eliasson, State Secretary, Ministry of Justice, Sweden, March 17, 2006, http://www.slyck.com/misc/pirate_mpa.pdf.
50. As of October 21, 2010 on Alexa.com.
51. Motion Picture Association of America, "Motion picture industry takes action against peer to peer movie thieves handed over by several torrent sites," Press release, August 25, 2005, http://www.mpaa.org/press_releases/2005_08_25.pdf.
52. Greg Sandoval, "Comcast, Cox cooperating with RIAA in antipiracy campaign," CNET News, March 25, 2009, http://news.cnet.com/8301-1023_3-10204047-93.html?tag=mncol;txt
53. Ibid.
54. Katie Allen, "Sweden sees music sales soar after crackdown on filesharing," The Guardian, November 23, 2009, http://www.guardian.co.uk/business/2009/nov/23/sweden-music-sales-filesharing-crackdown
55. "Piracy law cuts Internet traffic," BBC News, April 2, 2009, http://news.bbc.co.uk/2/hi/7978853.stm
56. "Sweden wants to force ISPs to save user data," The Local (Sweden), May 15, 2009, http://www.thelocal.se/19478/20090515/
57. Eric Pfanner, "France Approves Wide Crackdown on Net Piracy," The New York Times, October 23, 2009, sec. Technology, http://www.nytimes.com/2009/10/23/technology/23net.html?_r=1.
58. David Meyer, "Digital Economy Bill gets tough on file-sharers," ZDNet UK, November 20, 2009, http://news.zdnet.co.uk/communications/0,1000000085,39893271,00.htm.
59. "1 Million Xbox Live Players Banned," InformationWeek, November 11, 2009, http://www.informationweek.com/news/hardware/peripherals/showArticle.jhtml?articleID=221601267.