THE INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Steal These Policies: Strategies for Reducing Digital Piracy

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

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.

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.

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 property 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.

THE INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Steal These Policies: Strategies for Reducing Digital Piracy

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

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.

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.

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 Christian 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.

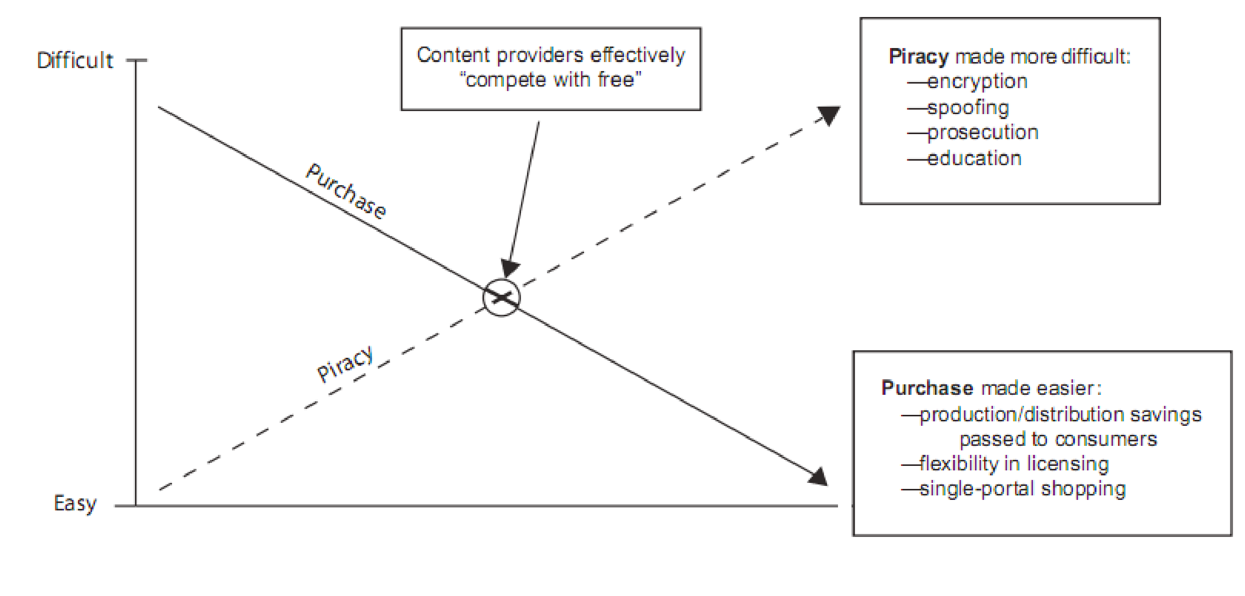
The Impact of Piracy in the United States and Abroad

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


Difficult
Easy
Content providers effectively "compete with free"
Purchase
Piracy
Piracy made more difficult:
—encryption
—spoofing
—prosecution
—education
Purchase made easier:
—production/distribution savings passed to consumers
—flexibility in licensing
—single-portal shopping

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 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 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

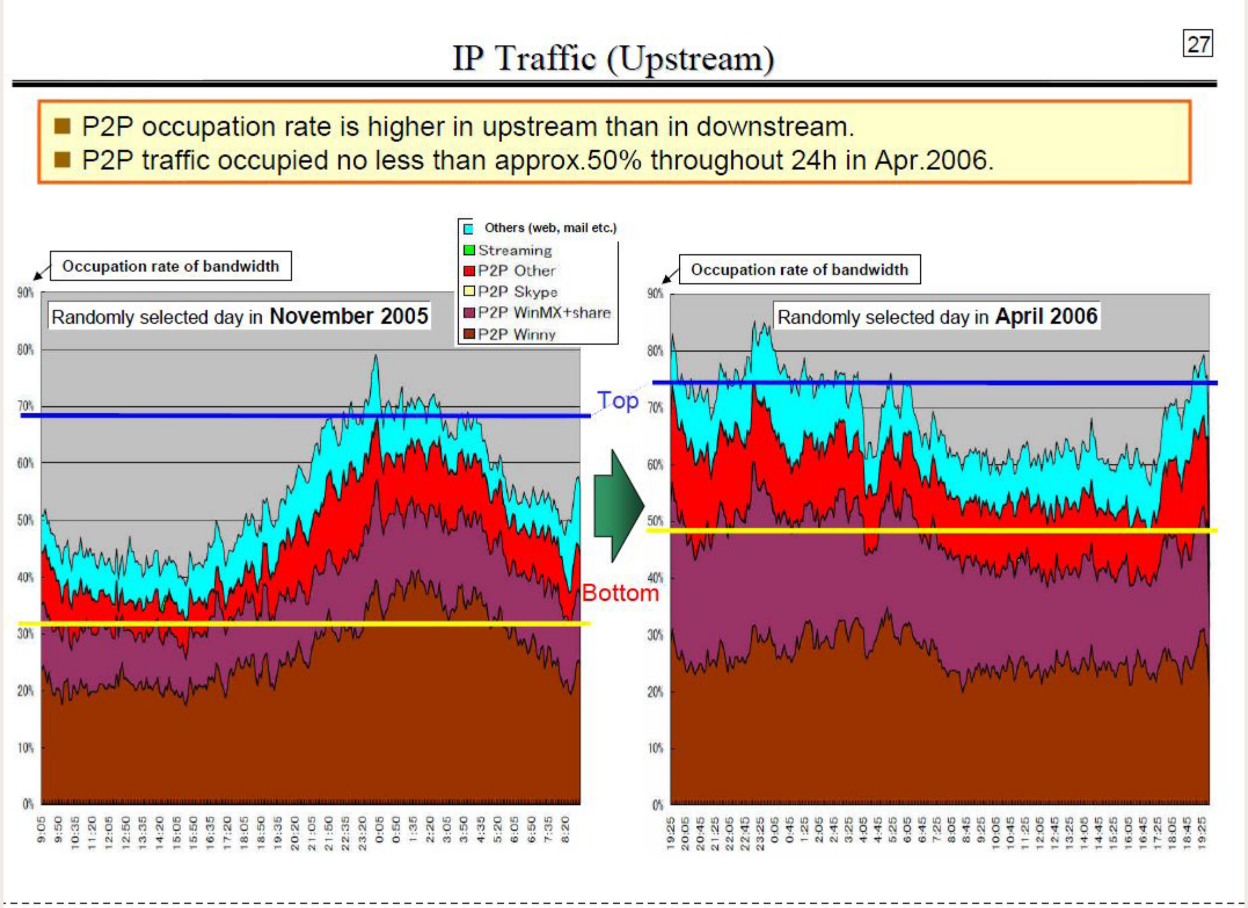
Industry groups have implemented various technical controls to mitigate file sharing. The most common control has been digital rights management (DRM) technology, or technical controls embedded within the content to prevent unauthorized use. Examples of DRM include the FairPlay system used by Apple to 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, 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.

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



IP Traffic (Upstream)

27

- P2P occupation rate is higher in upstream than in downstream.
- P2P traffic occupied no less than approx.50% throughout 24h in Apr.2006.

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

BOX 1: THE DEBATE OVER CONTENT IDENTIFICATION TECHNOLOGIES

Currently an important debate exists about the use deep packet inspection (DPI)-based filtering systems by Internet service providers (ISPs) and the relative merits and demerits of such systems. The recent paper by the advocacy group Public Knowledge, "Forcing the Net Through a Sieve," represents one side of the DPI debate.[34] While DPI opponents like to rely on emotional terms such as "technological arms races" and "false positives" and to make various assumptions about system performance effects, in fact piracy mitigation with DPI deals with a set of issues virtually identical to the largely non-controversial question of virus detection and mitigation.

Like DPI vendors, anti-virus manufacturers are engaged in a technological arms race with virus creators, who rely on highly advanced, open-source production systems to evolve better viruses in order to escape detection and removal.[35] No one seriously argues that personal computer users should stop using anti-virus software because of the challenges to keeping virus signatures and detection algorithms up to date. Rather, users are advised to rely on multiple systems of detection and removal in light of the deficiencies of each such system. Similarly, no credible source advises users not to employ anti-virus software because the dangers of having their computers hijacked by a botnet are so low. Those who suffer most from botnets are the targets of botnet abuse such as distributed denial of service attacks, and not those whose computers are hijacked. A concern for the overall health of the Internet ecosystem argues for aggressive tracking and removal of such threats.

However, advocates who argue the shortcomings of DPI-based content recognition systems tend to overstate their current shortcomings and underestimate their potential benefits.[36] The Public Knowledge report builds a content recognition strawman that claims that content recognition will reduce Internet performance, violate well-established principles of personal privacy and free speech, violate the Internet architecture, and raise the price of Internet access, all the while failing to protect rights holder interests in any significant way. Public Knowledge summarizes the harms as follows:[37]

1. **"Copyright filters are both underinclusive and overinclusive. A copyright filter will fail to identify all unlawful or unwanted content while harming lawful uses of content."**

Even to the extent that this criticism is correct, it is ultimately irrelevant. There are no completely perfect systems, applications, or protocols on the Internet or in any other aspect of modern life; we do not evaluate technical systems by comparing them to abstract ideals of perfection, but by balancing the utility they provide against the harm and inconvenience they entail. Given that the harm to American society from digital piracy is large and growing, the utility of copyright filters is not insignificant. Content recognition systems are no less perfect than personal anti-virus tools and much more precise than spam detection technology, so they are highly useful for the purpose for which they were designed. The imperfect nature of such systems simply argues for their oversight by responsible people and mechanisms. It is certainly true that a poorly-designed piracy detection system may incorrectly flag some lawful transactions; it is imperative that such systems are not allowed to disrupt such transactions or take punitive actions against suspected pirates without proper human oversight. Piracy is fundamentally a social problem more than a technical one, hence it is inappropriate to apply purely technical controls to it.

That being said, some technical systems have been shown to be highly accurate, such as the digital fingerprinting systems that prevent YouTube and similar services that host user-generated content from hosting copyrighted material. For such systems to be effective, however, the content hosting service has to agree to implement necessary procedures to check that uploaded content does not match materials in a database of copyrighted content, and also remove pirated content. Copyright owners must also supply each of these sites with copies of the fingerprints or watermarks used to identify their content.

2. **"Copyright filter processing will add latency. Copyright filters will slow ISP networks, discouraging use, innovation and investment and harming users, businesses and technology policy initiatives."**

This criticism is simply unfounded in technical fact. As packets pass through a network, they are examined and forwarded multiple times by Internet routers and switches. Internet routing is a pattern-matching activity that extracts a destination network address and matches it to an interface by consulting a large table of network address and interface associations. The technology that performs routing typically runs at close to "wire speed," the rate at which a packet would transit the router if the destination interface were known in advance. 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.

The purpose of content recognition systems is to reduce the total amount of unlawful transactions as a whole, not to prevent the forwarding of specific unlawful packets. As this is the goal, it is simply necessary for the rights holder or network operator to identify the persons who engage in such transactions, not to recognize and suppress each and every pirated packet. If disrupting the transaction is the goal, it can certainly be accomplished by systems that require a few minutes of passive examination to recognize that a particular in-progress stream contains unlawful content, for example. This passive monitoring time does not affect the timeliness of the overall transfer; it is simply reaction time on the part of the monitor. In particular, the widely used Audible Magic system that matches digital fingerprints is an out-of-band system that has no impact on network performance at all.

3. **"The implementation of copyright filters will result in a technological arms race. Users will act to circumvent the filters and the architects of the filters will find themselves caught in a costly, unwinnable arms race."**

This criticism is extremely weak. Any use of technology in the interest of law enforcement faces attempts by law-breakers to circumvent the system: bank robbers wear masks and burglars litter crime scenes with other people's cigarette butts, yet we still track them down and prosecute them. Each technology that employs pattern recognition must be periodically updated to keep up with the state of the art in criminality, and the costs of doing so probably decline with time and experience. Anti-virus systems in particular need to be updated on a regular basis to remain effective, yet they're widely used, and the overall rate of change in piracy-enabling systems is much slower than it is for viruses. Moreover, if there is any blame here it is on the side of "users" (i.e., pirates) who seek out and use better technology in order to engage in piracy. Simply saying that because pirates will continue to use better technology that content holders and ISPs should give up is to declare piracy a socially acceptable practice.

4. **"Copyright filters do not make economic sense. The monetary costs associated with copyright filtering far outweigh any perceived benefits."**

Unfortunately Public Knowledge did not offer data to support this claim in even the most rudimentary fashion. 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. This point simply argues for 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.

5. **"Copyright filters will discourage investment in the Internet economy. Copyright filters will disrupt the Internet ecosystem, severely undermining our most promising engine for economic growth."**

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 so 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.

6. **"Copyright filters will harm free speech. Due to technological limitations, copyright filters will harm lawful, protected forms of speech such as parody and satire."**

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. Creators who wish to make parodies of copyrighted works should be willing to come by the original copies of the works they parody legally. Moreover, 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.

7. **"Copyright filters could undermine the safe harbor provisions that shield ISPs from liability. Under the Digital Millennium Copyright Act (DMCA), ISPs are shielded from liability for their users' actions. Copyright filters could undermine these safe harbors, which have allowed the Internet to become the most important communications medium of the modern era."**

There are provisions in Title II of the DMCA (pertaining to safe harbors) that "preserves strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment."[38] Likewise, the legislation was drafted in a way to not "discourage the service provider from monitoring its service for infringing material. Courts should not conclude that the service provider loses eligibility for limitations on liability under section 512 solely because it engaged in a monitoring program."[39] Moreover, even if these DMCA provisions do not provide strong enough protections, which appears to not be the case, the law could be changed. In a regime in which ISPs are specifically directed to cooperate with content producers to limit piracy, the notions of safe harbors and limited liability would obviously need to be contingent on anti-piracy cooperation. In fact, it is unlikely that ISPs will in fact be willing to go forward with large-scale experiments in digital piracy reduction without some form of legal protection.

8. **"Copyright filtering could violate the Electronic Communications and Privacy Act (ECPA). Copyright filtering could constitute unlawful interception under ECPA."**

ISP-level filtering of copyright content may or may not constitute a violation of ECPA. For example, ISPs may adjust their terms of use to gain consent from their customers to allow this activity or give users a higher bit cap if they permit ISP-level content filtering. If, however, a court decision or industry consensus emerges that states ECPA does prevent ISPs from implementing filtering technology, then the law should be changed. Currently Reps. Rick Boucher (D-VA), Bobby Rush (D-IL) and Cliff Stearns (R-FL) have stated their intent to introduce legislation in 2010 that may clarify and define the boundaries of personal privacy and delineate permitted practices relative to Internet Protocol payload examination.

Other opponents of ISP-level filtering may use the argument that such technology violates their personal privacy. However, Internet packets are examined by automated systems as a matter of course 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. For example, the email service Gmail depends on the exact examination of highly personal communication in order to serve up targeted ads, but only a computer examines the packets and the email data are not shared or read by humans.[40]

As a general matter, Public Knowledge and most other advocates who oppose efforts to limit digital piracy express the fear that anti-piracy measures violate the Internet architecture, which in their minds mandates a particular form of service from the infrastructure. As Public Knowledge wrote in its recent report opposing efforts to limit digital piracy, "The Internet was designed to be an open system from end-to-end, which is to say, a system that moves content between hosts and clients as quickly as possible on a first-come, first-served basis—regardless of the nature of that content."[41]

On the face of it, such a statement is overly simplistic at best. The Internet was not designed to be an open system that moved viruses and other malware as quickly as possible. This kind of all-or-nothing view of the Internet fails to understand what the Internet is. As ITIF demonstrated in a report, "Designed for Change," on Internet architecture, the actual nature of the Internet is and always has been quite different.[42] The Internet was designed to serve as a testbed for experimentation in network applications, protocols, and services, not to serve as a monument to network technology as it may have existed at any particular moment in time. If it has a central principle, then it is one of constant change. As problems emerge in the use and management of the Internet, engineers devise solutions. With the advent of high-speed broadband access, piracy has become a problem that demands a solution. As with myriad other problems, it will be resolved by technical and behavioral systems in a manner perfectly consistent with the Internet's actual and legitimate heritage.

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 recently found 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."[43] 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."[44] 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. 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.[45] 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. 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.

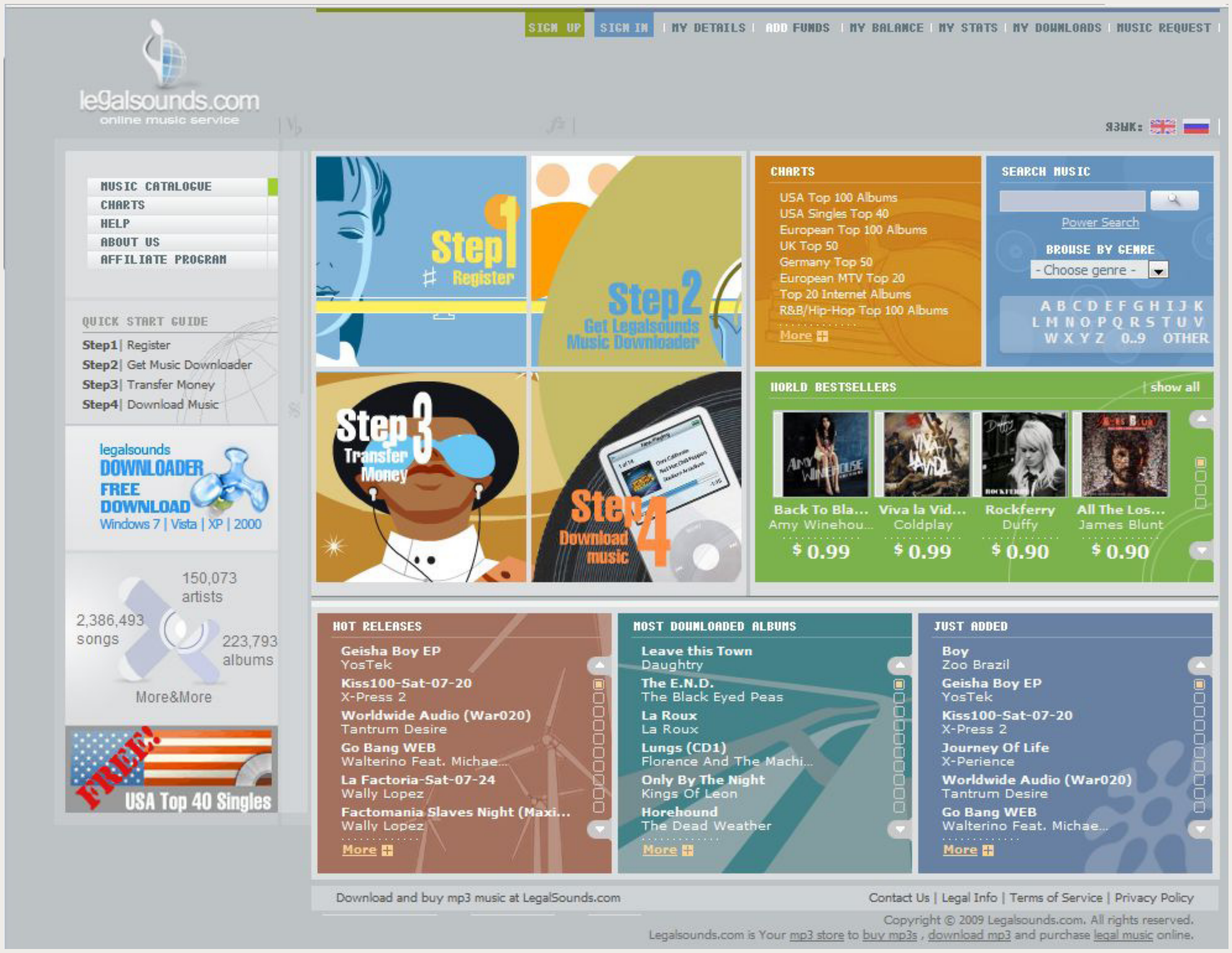
While blocking is one possible solution, that technology can obviously be used for both good and bad purposes. Several countries, some of which have anti-democratic aims—such as China, Cuba, Iran and North Korea—have blocked access to certain websites with varying degrees of success. However, as is the case with all technologies, 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.[46] 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."[47] 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. Australia's Communications Minister Stephen Conroy has also put forward the idea of implementing a national level filtering plan for website content, including filtering child pornography, gambling websites and other content that "offend against the standards of morality."[48] In February of 2009, the plans appeared to be derailed when it did not seem the government would have the votes to pass the required legislation. 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) and Watch Movies (www.watch-movies-online.tv) 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.[49] One reason that pirates are using websites to distribute copyrighted content is that bandwidth and storage

Figure 3: LegalSounds.com Music Service

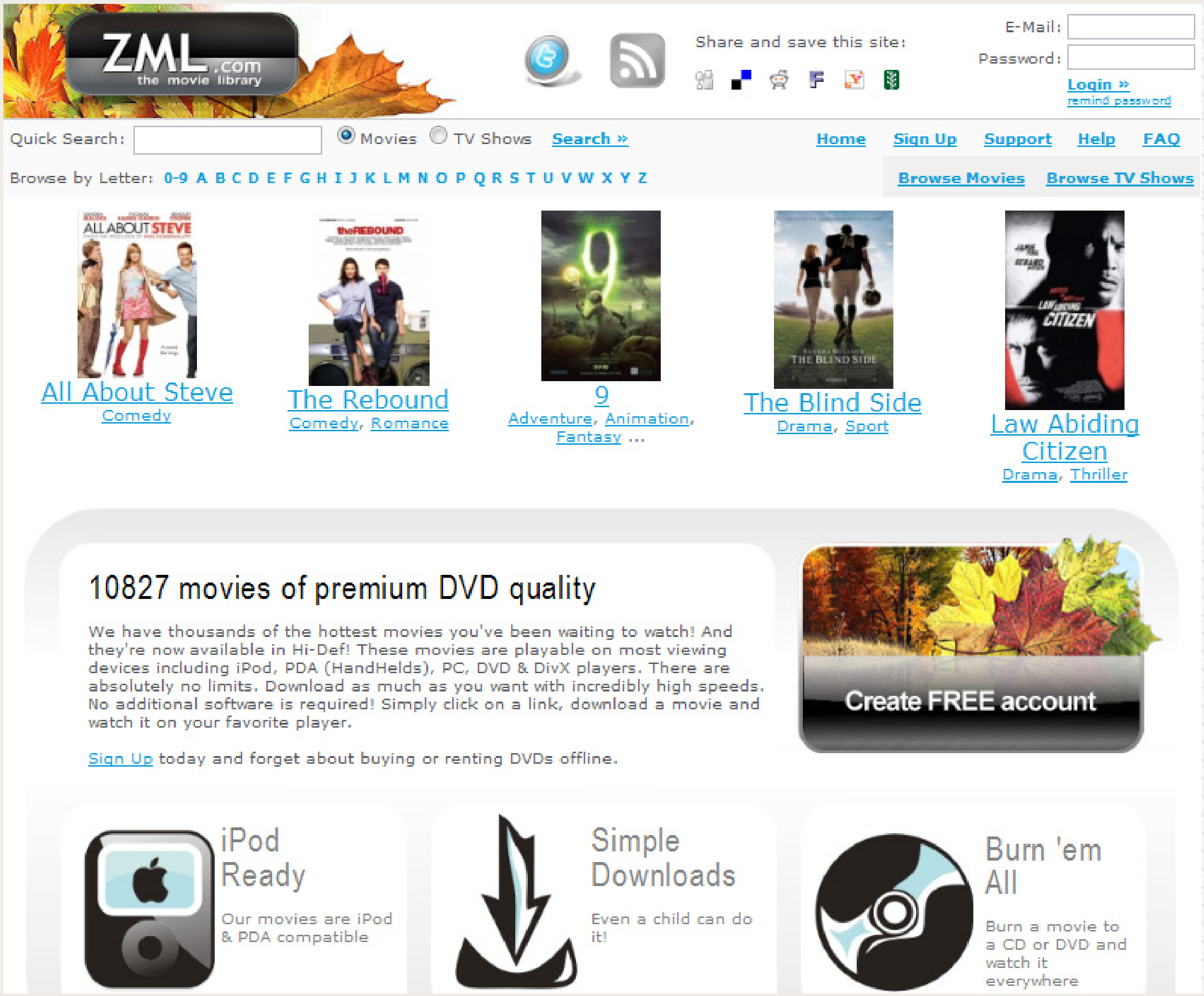


are relatively cheap and these costs can be supported by advertising.[50] These ad-supported websites offer copyrighted content online at no cost to the user and profit by selling advertising for content that they have pirated.

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. The same is true for the Russian site ZML.com that hosts movies for download.

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. Real-time mecha-

Figure 4: ZML.com: A Russian Movie Piracy Site



10827 movies of premium DVD quality

We have thousands of the hottest movies you've been waiting to watch! And they're now available in Hi-Def! These movies are playable on most viewing devices including iPod, PDA (HandHelds), PC, DVD & DivX players. There are absolutely no limits. Download as much as you want with incredibly high speeds. No additional software is required! Simply click on a link, download a movie and watch it on your favorite player.

Sign Up today and forget about buying or renting DVDs offline.

iPod Ready

Our movies are iPod & PDA compatible

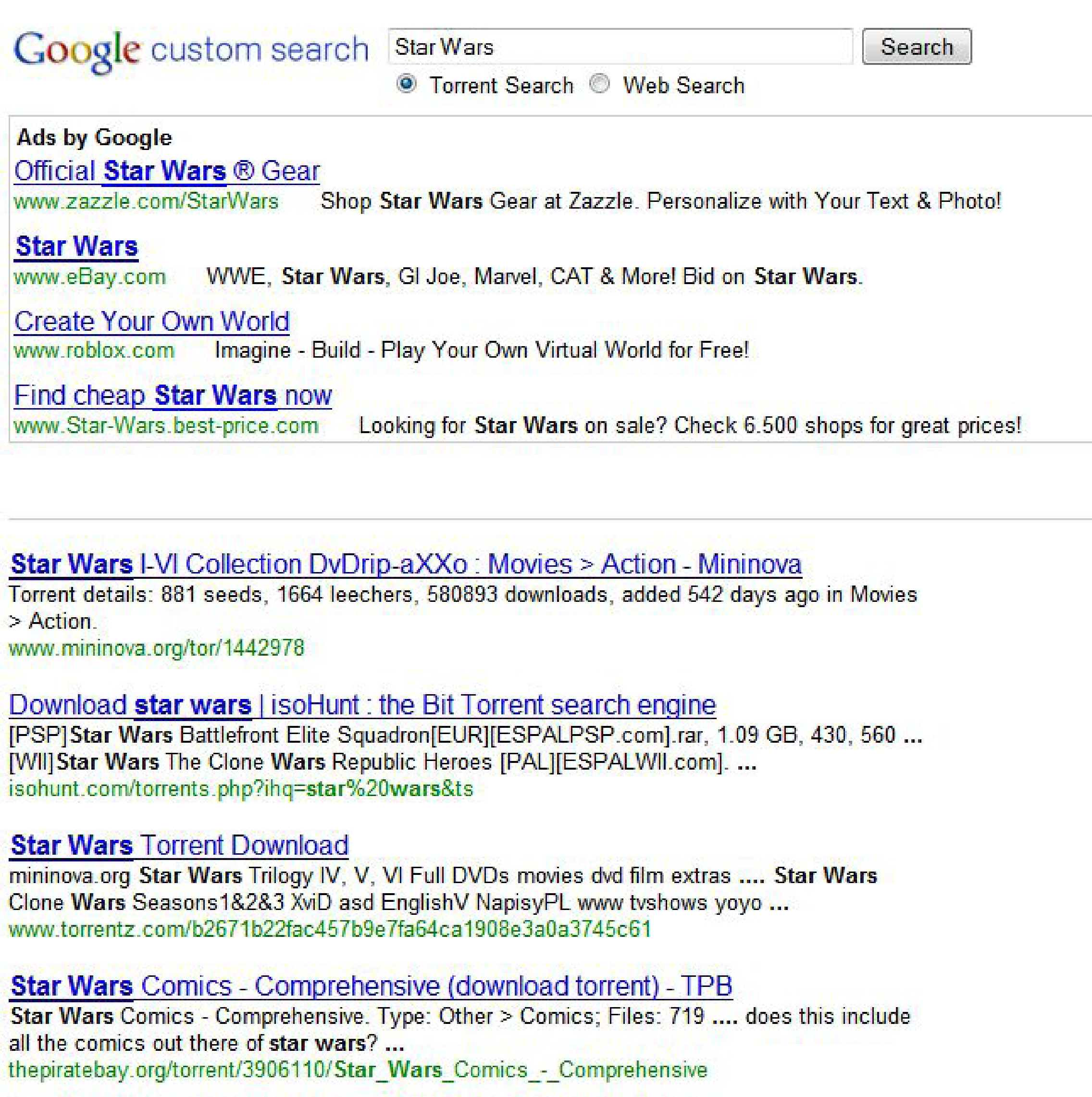
Simple Downloads

Even a child can do it!

Burn 'em All

Burn a movie to a CD or DVD and watch it everywhere

Figure 5: Search Engine Results Delivering Piracy Sites



Ads by Google

Official **Star Wars** ® Gear
www.zazzle.com/StarWars Shop **Star Wars** Gear at Zazzle. Personalize with Your Text & Photo!

Star Wars
www.eBay.com WWE, **Star Wars**, GI Joe, Marvel, CAT & More! Bid on **Star Wars**.

Create Your Own World
www.roblox.com Imagine - Build - Play Your Own Virtual World for Free!

Find cheap **Star Wars** now
www.Star-Wars.best-price.com Looking for **Star Wars** on sale? Check 6.500 shops for great prices!

Star Wars I-VI Collection DvDrip-aXXo : Movies > Action - Mininova
Torrent details: 881 seeds, 1664 leechers, 580893 downloads, added 542 days ago in Movies > Action.
www.mininova.org/tor/1442978

Download **star wars** | isoHunt : the Bit Torrent search engine
[PSP]**Star Wars** Battlefront Elite Squadron[EUR][ESPALPSP.com].rar, 1.09 GB, 430, 560 **...**
[WII]**Star Wars** The Clone **Wars** Republic Heroes [PAL][ESPALWII.com]. **...**
isohunt.com/torrents.php?ihq=**star**%20**wars**&ts

Star Wars Torrent Download
mininova.org **Star Wars** Trilogy IV, V, VI Full DVDs movies dvd film extras **....** **Star Wars** Clone **Wars** Seasons1&2&3 XviD asd EnglishV NapisyPL www tvshows yoyo **...**
www.torrentz.com/b2671b22fac457b9e7fa64ca1908e3a0a3745c61

Star Wars Comics - Comprehensive (download torrent) - TPB
Star Wars Comics - Comprehensive. Type: Other > Comics; Files: 719 **....** does this include all the comics out there of **star wars**? **...**
thepiratebay.org/torrent/3906110/**Star**_**Wars**_Comics_-_Comprehensive

nisms 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. There is no compelling reason why these services should provide easy access to unlawful content, as Google does with its ability to search for BitTorrent files. Google offers the ability to create a custom search for torrent files which indexes piracy sites. As shown in Figure 5, a search for Star Wars returns the instances of unlawful content. The first hit points to a collection of all six Star Wars DVDs on Mininova, a site similar in nature and purpose to the Pirate Bay.

There is no reason in principle that search engines 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, earlier this year The Pirate Bay was "accidentally" removed from Google's search results, but Google manually reinstated the website.[51]) 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.

> *Responsible companies should not advertise on websites that facilitate piracy and responsible ad networks should not buy placement on these websites.*

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!"[52] 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 recent review of the advertisers on the websites The Pirate Bay and isoHunt found brands such as Amazon.com, Blockbuster, British Airways, and Sprint, and these websites have previously included advertisements from companies such as Walmart.[53] 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.[54] 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.[55]

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).[56] 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."[57]

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."[58] 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.[59]

Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd. 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.

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 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."[60] 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 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.[61]

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

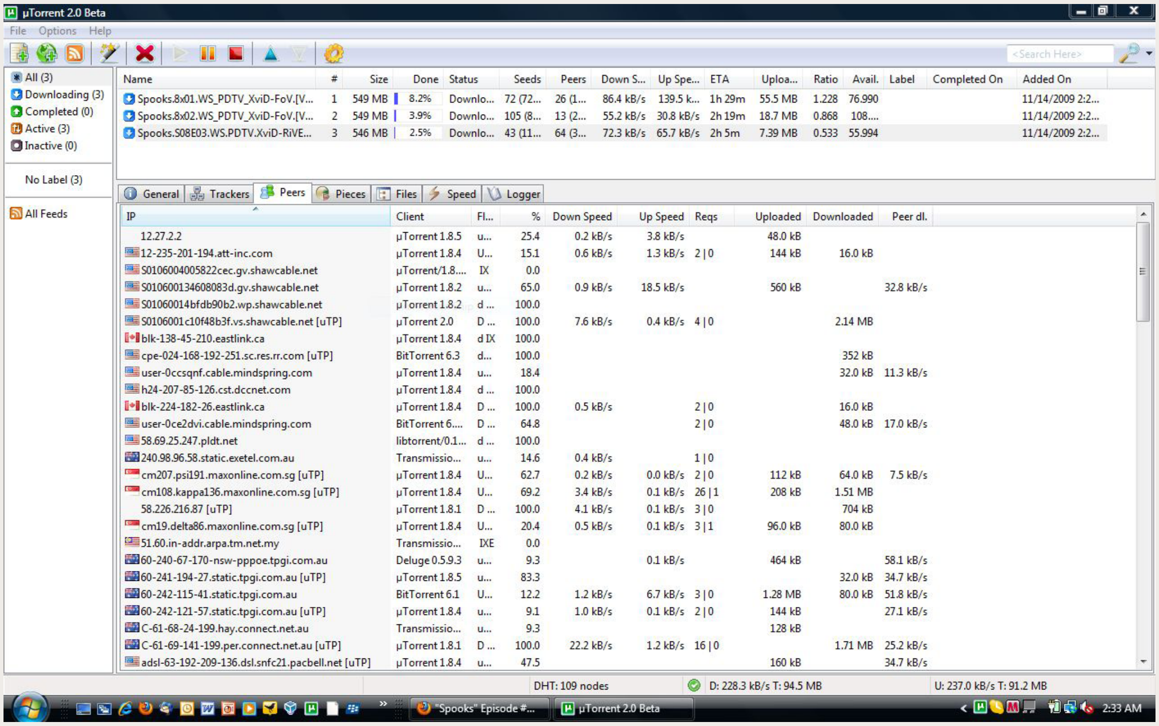
In large part because of public opposition, in 2008 RIAA halted its controversial strategy of suing individuals suspected of illegally pirating large amounts of digital music and announced that it would instead work with ISPs to alert Internet users of potentially illegal activity. Under this framework, 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. For example, here is a typical piracy swarm for the BBC television series Spooks:

By providing notice of copyright infringement, users 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. 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.[62] 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."[63] Although Cox sent out many notices, it has only terminated access

Figure 6: BitTorrent Swarm with IP Addresses



Name	#	Size	Done	Status	Seeds	Peers	Down S...	Up Spe...	ETA	Uploa...	Ratio	Avail.	Label	Completed On	Added On
Spooks.8x01.WS_PDTV_XviD-FoV.[V...	1	549 MB	8.2%	Downlo...	72 (72...	26 (1...	86.4 kB/s	139.5 k...	1h 29m	55.5 MB	1.228	76.990			11/14/2009 2:2...
Spooks.8x02.WS_PDTV_XviD-FoV.[V...	2	549 MB	3.9%	Downlo...	105 (8...	13 (2...	55.2 kB/s	30.8 kB/s	2h 19m	18.7 MB	0.868	108....			11/14/2009 2:2...
Spooks.S08E03.WS.PDTV.XviD-RiVE...	3	546 MB	2.5%	Downlo...	43 (11...	64 (3...	72.3 kB/s	65.7 kB/s	2h 5m	7.39 MB	0.533	55.994			11/14/2009 2:2...

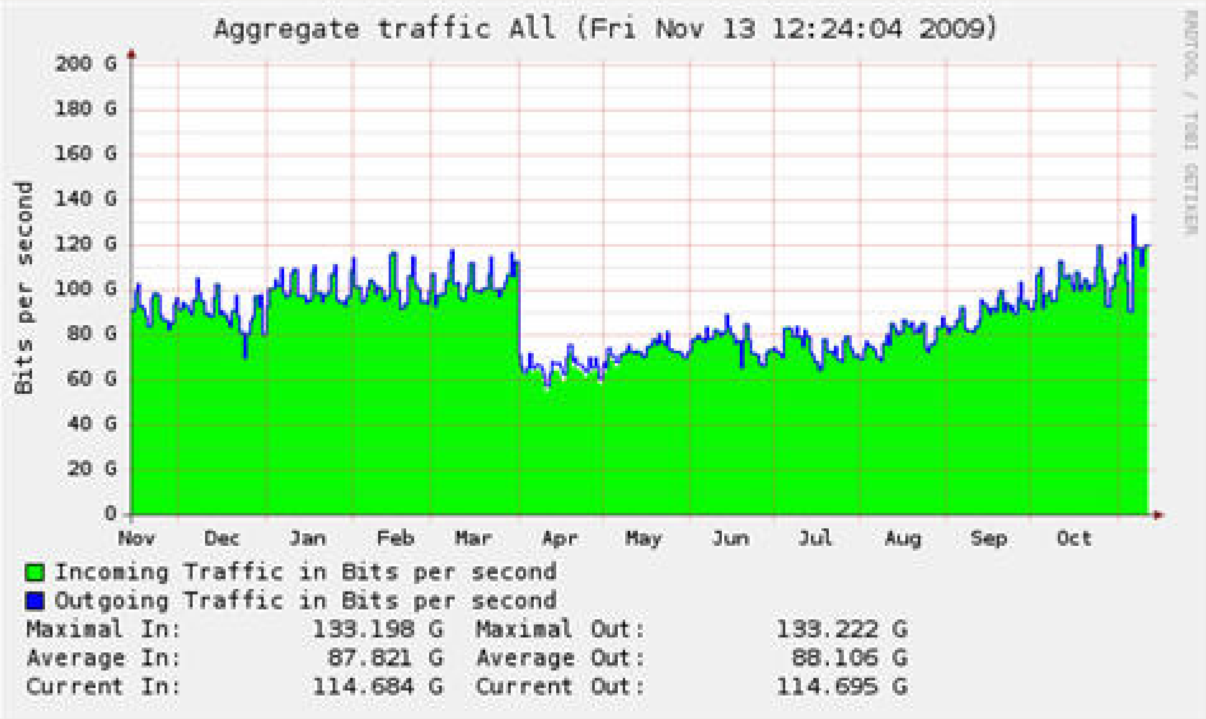
IP	Client	Fl...	%	Down Speed	Up Speed	Reqs	Uploaded	Downloaded	Peer dl.
12.27.2.2	µTorrent 1.8.5	u...	25.4	0.2 kB/s	3.8 kB/s		48.0 kB		
12-235-201-194.att-inc.com	µTorrent 1.8.4	U...	15.1	0.6 kB/s	1.3 kB/s	2 | 0	144 kB	16.0 kB	
S0106004005822cec.gv.shawcable.net	µTorrent/1.8....	IX	0.0						
S010600134608083d.gv.shawcable.net	µTorrent 1.8.2	u...	65.0	0.9 kB/s	18.5 kB/s		560 kB		32.8 kB/s
S01060014bfdb90b2.wp.shawcable.net	µTorrent 1.8.2	d ...	100.0						
S0106001c10f48b3f.vs.shawcable.net [uTP]	µTorrent 2.0	D ...	100.0	7.6 kB/s	0.4 kB/s	4 | 0		2.14 MB	
blk-138-45-210.eastlink.ca	µTorrent 1.8.4	d IX	100.0						
cpe-024-168-192-251.sc.res.rr.com [uTP]	BitTorrent 6.3	d...	100.0					352 kB	
user-0ccsqnf.cable.mindspring.com	µTorrent 1.8.4	u...	18.4					32.0 kB	11.3 kB/s
h24-207-85-126.cst.dccnet.com	µTorrent 1.8.4	d ...	100.0						
blk-224-182-26.eastlink.ca	µTorrent 1.8.4	D ...	100.0	0.5 kB/s		2 | 0		16.0 kB	
user-0ce2dvi.cable.mindspring.com	BitTorrent 6....	D ...	64.8			2 | 0		48.0 kB	17.0 kB/s
58.69.25.247.pldt.net	libtorrent/0.1...	d ...	100.0						
240.98.96.58.static.exetel.com.au	Transmissio...	u...	14.6	0.4 kB/s		1 | 0			
cm207.psi191.maxonline.com.sg [uTP]	µTorrent 1.8.4	U...	62.7	0.2 kB/s	0.0 kB/s	2 | 0	112 kB	64.0 kB	7.5 kB/s
cm108.kappa136.maxonline.com.sg [uTP]	µTorrent 1.8.4	U...	69.2	3.4 kB/s	0.1 kB/s	26 | 1	208 kB	1.51 MB	
58.226.216.87 [uTP]	µTorrent 1.8.1	D ...	100.0	4.1 kB/s	0.1 kB/s	3 | 0		704 kB	
cm19.delta86.maxonline.com.sg [uTP]	µTorrent 1.8.4	U...	20.4	0.5 kB/s	0.1 kB/s	3 | 1	96.0 kB	80.0 kB	
51.60.in-addr.arpa.tm.net.my	Transmissio...	IXE	0.0						
60-240-67-170-nsw-pppoe.tpgi.com.au	Deluge 0.5.9.3	u...	9.3		0.1 kB/s		464 kB		58.1 kB/s
60-241-194-27.static.tpgi.com.au [uTP]	µTorrent 1.8.5	u...	83.3					32.0 kB	34.7 kB/s
60-242-115-41.static.tpgi.com.au	BitTorrent 6.1	U...	12.2	1.2 kB/s	6.7 kB/s	3 | 0	1.28 MB	80.0 kB	51.8 kB/s
60-242-121-57.static.tpgi.com.au [uTP]	µTorrent 1.8.4	u...	9.1	1.0 kB/s	0.1 kB/s	2 | 0	144 kB		27.1 kB/s
C-61-68-24-199.hay.connect.net.au	Transmissio...	u...	9.3				128 kB		
C-61-69-141-199.per.connect.net.au [uTP]	µTorrent 1.8.1	D ...	100.0	22.2 kB/s	1.2 kB/s	16 | 0		1.71 MB	25.2 kB/s
adsl-63-192-209-136.dsl.snfc21.pacbell.net [uTP]	µTorrent 1.8.4	u...	47.5				160 kB		34.7 kB/s

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 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.[64] 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.[65] 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 6 months.[66]

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

Figure 7: Consequence of EU Intellectual Property Rights Enforcement Directive (IPRED) on Internet Traffic



```
🟩 Incoming Traffic in Bits per second
■ Outgoing Traffic in Bits per second
Maximal In:        133.198 G   Maximal Out:        133.222 G
Average In:         87.821 G   Average Out:         88.106 G
Current In:        114.684 G   Current Out:        114.695 G
```

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.[67]

In the United Kingdom, the Digital Economy bill would provide a similar graduated response. The bill 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 legislation does not make file sharing a criminal offense punishable with jail time.[68] Mobile Internet operators have raised concerns about the cost of the proposed legislation because, unlike wired broadband operators, mobile broadband operators do not use a "one IP address per customer" system, so they would have to build a new tracking database for this purpose.[69]

Industry has also implemented this technique of using service bans to discourage piracy. Recently, 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.[70]

OBJECTIONS TO RIGHTS ENFORCEMENT

Any system of rights enforcement attracts criticism, some of which is legitimate, but much of which is not. One element that must be overcome as the Internet becomes established as the dominant network for communication and entertainment is its non-commercial history. The Internet was designed to serve as a vehicle for network research rather than for commerce, hence it lacks a coherent system of controls for intellectual property rights (IPR), and any effort to ad such controls raises complaints from a traditionalist group that's loathe to accept change in the Internet. Some digital rights enforcement schemes have been overly intrusive and poorly managed, so there is an element of legitimate criticism in this dialog.

Moreover, to some extent, there are so many ways to obtain pirated content over the Internet that any scheme of enforcement can be criticized on the basis that it will simply send pirates in some other direction, but will not impact overall copyright abuse. Hence, it is worthwhile to ask pragmatic questions about the effectiveness of proposed systems, such as:

1) Effectiveness: Is the system easily defeated or circumvented with no increase in inconvenience to the casual consumer of unlawful content?

2) Intrusiveness: Does the system impose a more than diminimis burden on mainstream Internet users who are not engaged in unlawful activities and does it violate expectations of privacy in any significant way?

3) Cost: Is the system excessively costly, especially with respect to its benefits? Are ISPs (and hence consumers of ISP services) or government (and hence taxpayers) paying for a system that produces little benefit?

4) Benefit: Does the system make the enforcement of anti-piracy laws easier than it already is, without violating fundamental rights, such as self-expression and privacy?

If a proposed system of enforcement seems to do well on most of these counts, it is likely worthy of a trial to determine its real-world utility.

POLICY RECOMMENDATIONS

As noted earlier, while industry will take the lead on many of these responses to the challenge of digital piracy, policymakers also have a key role to play. Actions that policymakers should take include the following:

Support Anti-Piracy Innovation

Government policies should support technological innovation wherever possible, as innovation is a key driver of economic growth and productivity. Unfortunately, some advocacy groups often object to technical controls designed to prevent piracy, claiming they are a threat to civil liberties or harmful to consumers. For example, the advocacy group Public Knowledge has argued that anti-piracy technology, such as content identification filters for ISPs, should not be "allowed, encouraged or mandated" by government even though such technology prohibitions would impair anti-piracy innovations.[71]

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.

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. In addition, the National Science Foundation should sponsor anti-piracy research.

Encourage Coordinated Industry Action

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. If one ad network refuses to place ads on popular piracy sites, for example, another one will likely choose to do so.

Collaborative action by various industry stakeholders has been able to address this prisoner's dilemma in at least one area. A group of copyright owners and website offering user-generated content hosting came together to develop a set of principles to help reduce piracy.[72] These principles included all parties working to "ensure that the Identification Technology is implemented in a manner that effectively balances legitimate interests in (1) blocking infringing user-uploaded content, (2) allowing wholly original and authorized uploads, and (3) accommodating fair use."[73]

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 implementations of a graduated response system by ISPs. However, some anti-piracy measures, such as content filtering, could require government oversight to prevent abuses and ensure consumer rights are protected, especially in the absence of a collaborative agreement among key stakeholders. 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 around the world that are systemically engaged in piracy so that ISPs and search engines can block them, ad 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, the government should also consider providing anti-trust exemptions for collaborative industry action to address these problems.

Pursue International Frameworks to Protect Intellectual Property

The United States cannot solve the problem of digital piracy alone. Nations with weak laws to protect intellectual property provide a virtual safe haven for online operations that flout copyright law. More broadly, the lack of a strong international framework for the regulation of Internet conduct means that nations are not held responsible for the data flowing out of their networks. A comprehensive solution to this problem is urgently needed to solve many online issues in addition to Internet piracy, including cybersecurity, spam, malware, and other illegal Internet content. Global partnerships are needed to develop Internet policies that will spur nations to better enforce international standards on issues such as intellectual property rights. In particular, 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. In short, 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. For example, 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.

CONCLUSION

As many others have pointed out, the Internet is a vast, distributed system that has no central point of control. This does not mean that it is free of control. Rather, it means that each of us is the controller of our small part of the system. 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 profits by it. Governments need to put in place frameworks that facilitate and encourage responsible control. The Internet is a tremendous enterprise of user empowerment, free speech, and innovation, but it facilitates unlawful acts just as much as lawful ones.

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 such as The Pirate Bay or isoHunt to exist, for there to be piracy-oriented services such as LegalSounds.com, or for search engines to connect would-be pirates with each other. 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, and it's shameful for proponents of piracy to hide behind the excuse that filtering or blocking access to unlawful conduct is in some way analogous to the suppression of dissent in authoritarian dictatorships like China. There is clearly an enormous difference between the actions of an undemocratic government and the legitimate desire of liberal democracies to limit the ill-gotten gains of piracy promoters, advertisers, and service providers. 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.

ENDNOTES

1. Mehan Jayasuriya, et al., "Forcing the Net Through a Sieve: Why Copyright Filtering is Not a Viable Solution for U.S. ISPs," Public Knowledge, 2009, http://www.publicknowledge.org/paper/pk-filtering-whitepaper and Ronald Peeters. Michael Yang and P. Jean-Jacques Herings, "Piracy on the Internet: Accommodate it or Fight it? A Dynamic Approach," September 7, 2009, 1, http://ssrn.com/abstract=1469564.

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. Mininova was recently ranked by Alexa as the 96th most popular website in the world, the Pirate Bay website was ranked 109th, and isoHunt was ranked as 187th. "Alexa Top 500 Global Web Sites," web page, ND, http://www.alexa.com/topsites/global (accessed November 28, 2009).

4. Christian Engström, "Copyright laws threaten our online freedom," FT.com, July 7 2009, http://www.ft.com/cms/s/0/87c523a4-6b18-11de-861d-00144feabdc0.html.

5. 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.

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. Ibid.

10. IFPI 2008 Digital Music Report, IFPI, 2008, 8, http://www.ifpi.org/content/library/dmr2008.pdf.

11. Siwek, "The True Cost of Motion Picture Piracy."

12. Business Software Alliance, Sixth Annual BSA-IDC Global Software 08 Piracy Study, BSA, May 2009, http://global.bsa.org/globalpiracy2008/studies/globalpiracy2008.pdf.

13. International Intellectual Property Alliance, Special Report 301, February, 2009.

14. 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.

15. Randall Stross, "Will Books Be Napsterized?" *New York Times*, October 3, 2009, http://www.nytimes.com/2009/10/04/business/04digi.html.

16. "Alexa Top 500 Global Web Sites," Alexa, ND, http://www.alexa.com/topsites/global;1 (accessed Nov. 28, 2009).

17. Business Software Alliance, Sixth Annual BSA-IDC Global Software 08 Piracy Study.

18. IFPI 2008 Digital Music Report.

19. Business Software Alliance, Sixth Annual BSA-IDC Global Software 08 Piracy Study.

20. "TotalNews, publishers settle suit," *CNET News*, June 5, 1997, http://news.cnet.com/2100-1023-200295.html.

21. "Murdoch wants a Google rebellion," *Forbes.com*, April 3, 2009, http://www.forbes.com/2009/04/03/rupert-murdoch-google-business-media-murdoch.html.

22. The Pirate Bay Web Site, http://thepiratebay.org/about.

23. For example, higher-income employees pay more taxes than lower-income ones, thereby allowing governments to provide more public goods without raising taxes, or the same amount of public goods while lowering taxes.

24. Organization for Economic Co-Operation and Development (OECD), "Broadband Growth and Policies in OECD Countries," 2008, 48.

25. Ibid.

26. Electronic Frontier Foundation, "Three Strikes, Three Countries: France, Japan and Sweden," http://www.eff.org/deeplinks/2008/03/three-strikes-three-countries.

27. Robb Topolski, "Re: [p2pi] Follow-Up from Comcast Presentation," June 6, 2008, http://www.ietf.org/mail-archive/web/p2pi/current/msg00072.html.

28. See George Ou, "Managing Broadband Networks: A Policymakes Guide," Information Technology and Innovation Foundation, December 2008, http://www.itif.org/files/Network_Management.pdf.

29. Gartner, "Gartner Reports Napster Banned at 34 Percent of Colleges and Universities," August 30, 2000, http://www.gartner.com/5_about/press_room/pr20000830a.html.

30. For a guide to how network management techniques work, see George Ou, "Managing Broadband Networks."

31. "p2pnet news » Blog Archive » HBO: poisoning BT downloads," http://www.p2pnet.net/story/6515.

32. 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.

33. See, for example, the services offer for content providers by Vedicis, http://www.vedicis.com.

34. Jayasuriya, et. al., "Forcing the Net Through a Sieve," 1.

35. Ellen Messmer, "Botnet production eerily like commercial code practice," *Network World*, October 13, 2009, http://www.networkworld.com/news/2009/101309-botnets-commerical-code.html?fsrc=netflash-rss.

36. Jayasuriya, et. al., "Forcing the Net Through a Sieve."

37. The eight point summary of Public Knowedge's objection comes from the Executive Summary of Jayasuriya, et. al., "Forcing the Net Through a Sieve," 1.

38. S. Rep. No. 190, 105th Congress, 2d Session at 20 (1998) (Senate Judiciary Committee Report on the DMCA).

39. H.R. Rep. No. 769, 105th Congress, 2d Session at 73 (1998) (Conference Report on the DMCA).

40. Robert D. Atkinson, "Google E-mail, What's All the Fuss About?" Progressive Policy Institute, 2004, http://www.ppionline.org/ppi_ci.cfm?knlgAreaID=140&subsecID=288&contentID=252511.

41. Jayasuriya, et. al., "Forcing the Net Through a Sieve."

42. Richard Bennett, "Designed for Change: End-to-End Arguments, Internet Innovation, and the Net Neutrality Debate," Information Technology and Innovation Foundation, September 2009, http://www.itif.org/index.php?id=294.

43. "The Pirate Bay Trial: The Official Verdict – Guilty," TorrentFreak, April 17, 2009, http://torrentfreak.com/the-pirate-bay-trial-the-verdict-090417/.

44. "The Pirate Bay - The world's most resilient bittorrent site," November 11, 2009, http://thepiratebay.org/blog/175.

45. 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.

46. "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.

47. "About the Internet Watch Foundation," Internet Watch Foundation, October 21, 2009, http://www.iwf.org.uk/public/page.103.htm.

48. Asher Moses, "Web censorship plan heads towards a dead end," *Sunday Morning Herald*, February 26, 2009, http://www.smh.com.au/articles/2009/02/26/1235237810486.html.

49. 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.

50. See, for example, http://www.mediafire.com/.

51. 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.

52. "Advertise on the cutting edge," isoHunt, n.d., http://isohunt.com/advertise.php.

53. The Pirate Bay: Sponsored by Wal-Mart," TorrentFreak, January 11, 2007, http://torrentfreak.com/the-pirate-bay-sponsored-by-wall-mart/.

54. 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.

55. 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.

56. 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.

57. Sony Corp. v. Universal Studios, Inc., 464 U.S 442 (1984).

58. MGM Studios, Inc. v. Grokster Ltd., 545 U.S 125 (2005).

59. 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_.

60. 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.

61. Motion Picture Association of America, "Motion picture industry takes action against peer to peer movie thieves handed over by several torrent sites," August 25, 2005, http://www.mpaa.org/press_releases/2005_08_25.pdf.

62. 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.

63. Ibid.

64. 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.

65. "Piracy law cuts Internet traffic," *BBC News*, April 2, 2009, http://news.bbc.co.uk/2/hi/7978853.stm.

66. "Sweden wants to force ISPs to save user data," *The Local* (Sweden), May 15, 2009, http://www.thelocal.se/19478/20090515/.

67. Eric Pfanner, "France Approves Wide Crackdown on Net Piracy," *The New York Times*, October 23, 2009, http://www.nytimes.com/2009/10/23/technology/23net.html?_r=1.

68. 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.

69. David Meyer, "Mobile industry 'cannot identify pirates,'" *ZDNet UK*, November 24, 2009, http://news.zdnet.co.uk/communications/0,1000000085,39899832,00.htm.

70. "1 Million Xbox Live Players Banned," *InformationWeek*, November 11, 2009, http://www.informationweek.com/news/hardware/peripherals/showArticle.jhtml?articleID=221601267.

71. Jayasuriya, et. al., "Forcing the Net Through a Sieve," 1.

72. "Principles for User Generated Content Services," n.d., http://www.ugcprinciples.com/.

73. Ibid.

ABOUT THE AUTHORS

Daniel Castro is a Senior Analyst with Information Technology and Innovation Foundation. His research interests include technology policy, security, and privacy. Mr. Castro has a B.S. from the School of Foreign Service at Georgetown University and an M.S. in information security technology and management from Carnegie Mellon University.

Richard Bennett is a Research Fellow with the Information Technology and Innovation Foundation (ITIF) in Washington, D.C. He was vice-chairman of the IEEE 802.3 1BASE5 task group that wrote the first standard for Ethernet over twisted pair, and a contributor to the IEEE 802.11 standard's original system architecture and designer of the IEEE 802.11n packet aggregation scheme. He was active in Open Systems Interconnection (OSI) standards work, the instigator of RFC 1001 and 1002, and the inventor of the Distributed Reservation Protocol for the Wi-Media Ultra-Wideband network. A frequent conference speaker, he has testified before the U.S. Federal Communications Commission as an expert witness in their network management inquiry and before Congress on Internet privacy.

Scott Andes is a Research Analyst with the Information Technology and Innovation Foundation. His research interests include innovation and competition policy. Mr. Andes has a BS in government from London School of Economics.

ABOUT THE INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION

The Information Technology and Innovation Foundation (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.

For more information contact ITIF at 202-449-1351 or at mail@itif.org, or go online to www.itif.org.
ITIF I 1101 K St. N.W. I Suite 610 I Washington, DC 20005