How Website Blocking Is Curbing Digital Piracy Without "Breaking the Internet"

BY NIGEL CORY | AUGUST 2016

A free and open Internet is not antithetical to website blocking, as not every website—those actively facilitating child pornography or terrorism are two examples—has a right to exist. Blocking websites to stop copyright infringement should not be considered any differently.

Many countries ask domestic Internet service providers (ISPs) to block access to websites engaged in illegal activities—such as those facilitating cybercrime, child pornography, or terrorism—because this is one of the few means available to respond to illegal materials hosted abroad. However, when it comes to addressing other legitimate public policy objectives, such as curbing digital piracy, some of these same countries are reluctant to ask ISPs to block websites dedicated to distributing illegal copies of movies, music, and other copyright-protected works. As a result, online piracy continues unabated. But where countries are using website blocking to fight digital piracy, the record shows it has been effective in driving users from illegal to legal sources of copyrighted material online.

This was a key conclusion of a recent study in which Carnegie Mellon University examined the real-world impact of website blocking in the United Kingdom.[1] Unfortunately, the results of this study will likely face many familiar misperceptions about website blocking: that such policy tools should not apply to the Internet, that it will be ineffective, that it is a form of censorship, that it will be expensive for ISPs, and that it will be abused by content rights holders. However, these objections are often based on a very skewed view of the Internet, one that does not recognize the need to extend laws that exist in the offline world to the online one.

Website blocking is not antithetical to a free and open Internet. Even the most vocal supporters of Internet freedom recognize that it is legitimate to remove or limit access to some materials online, such as sites that facilitate child pornography. At the same time,

some governments can and do cast too wide a net against Internet content, taking down or limiting access that is not illegal, but only upsetting to those in power. The key issue about Internet freedom, therefore, is not whether the Internet is and should be completely free or whether governments should have unlimited censorship authority, but rather where the appropriate lines should be drawn, how they are drawn, and how they are implemented.

Defending the open Internet globally should be a key task of governments, particularly democratically elected ones. Advocating limits on accessing illegal content online does not violate open Internet principles, nor does it limit the legitimacy of governments pushing for a more open and free global Internet. And, in particular, given the pervasiveness of digital piracy throughout the world—action that is by definition illegal, not to mention unethical—governments can and should do more to limit access to this content.

In the vitriolic debates over the Stop Online Piracy Act (SOPA) in the United States, many opponents of taking action to limit access to foreign websites dedicated to piracy argued that website blocking would "break the Internet," although they never satisfactorily explained how this breakage would occur or why the Internet was not already broken, since some site blocking already existed before the SOPA debate.[2] Nonetheless, no policymaker wanted to be accused of being responsible for breaking the Internet. Five years later, we have evidence to evaluate. Meanwhile, 25 nations have enacted policies and regulations regarding website blocking to find a better balance between preserving the benefits of a free and open Internet and efforts to stop crimes such as digital piracy. And the Internet still works just fine in these nations.

This report analyzes the prevalence, persistence, types, and cost of digital piracy, which the vast majority of academic literature shows harms content creators. It then analyzes website blocking—how it works, different blocking mechanisms, the costs of website blocking, and the types of websites currently being targeted by the wide range of countries that allow website blocking. The report then rebuts a number of common criticisms of website blocking.

DIGITAL PIRACY IS PERSISENT, EXTENSIVE, AND COSTLY

The ease with which copyrighted material can be copied and shared online across jurisdictional borders makes it challenging for rights holders to protect their works as they do in the offline world, where customs agents typically can intercept physical goods, such as CDs and DVDs, that contain illegal copies of songs, movies, TV shows, and other content. (Illegal materials hosted on overseas servers cannot be permanently removed without the cooperation of the local authorities, and in many cases, this is not provided.

New technologies are constantly being created to copy and disseminate digital content, often without the owner's consent. This makes it difficult to fight digital piracy, as many digital technologies and processes are used for both legitimate and illegitimate purposes. While illegal copying in the past was tedious, such as using cassette tapes to record music, it has become automated and prolific following the creation of first-generation file-sharing

platforms such as Napster, which undermined copyright laws around the world. (Box A outlines the primary types of digital piracy.)

A common response to growing concerns about digital piracy has been that there were not enough legal alternatives with timely content. While this was never a valid argument, as accessing content without the permission of the copyright holder was always illegal, it is irrelevant now given the number of legitimate content services continues to grow. For example, there are more than 450 legitimate movie and television streaming services available around the world, and over 115 in the United States alone.[3] The country at the center of this report, the United Kingdom, had 62 legal online music services in 2014, which was more than the United States (59).[4]

A recent Carnegie Mellon University study shows that the expanding use of website blocking in the United Kingdom has been effective in getting people to shift from illegal to legal content online.

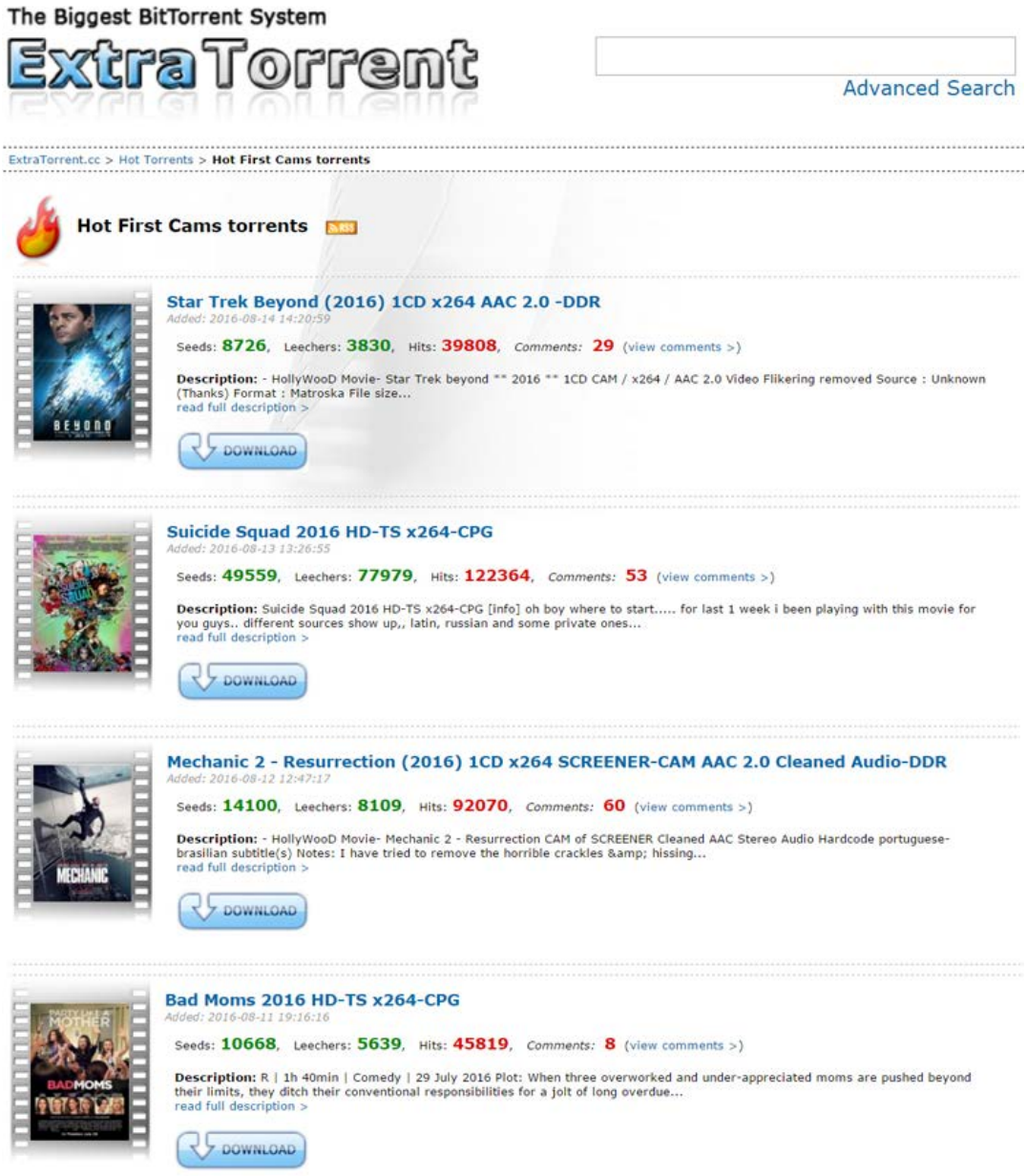
Measuring piracy—an illicit and therefore hard-to-track activity—is a difficult problem. Yet, available evidence suggests that online copyright infringement remains prevalent, driven by the free and simple availability of illegal digital content. A NetNames report, *Sizing the Piracy Universe*, demonstrated that the number of users regularly accessing illegal copies of media content (such as songs and movies) and the amount of bandwidth consumed by infringing uses of content significantly increased between 2010 and 2013. This finding held true even in regions where there are a growing number of legitimate distribution services for online content. In January 2013, the report estimated that 432 million unique Internet users sought illegal copies of media content.[5] In more recent years, piracy has shifted away from file-sharing platforms to streaming sites. A recent report by piracy-tracking firm MUSO found that there were 57.8 billion visits to 14,000 of the largest piracy websites and that 74 percent of these visits were to streaming sites.[6]

Even when copyright skeptics and opponents acknowledge the extent of piracy, many dismiss its importance, claiming that it doesn't detract from legitimate sales. However, a growing body of research proves that piracy has a negative impact on legitimate sales. A recent meta-analysis of academic literature examining the effects of online piracy shows that over half of rigorous, empirical studies conclude that piracy has a clear, statistically significant, negative impact on profits for content creators.[7] Another recent survey of the literature concludes that the vast majority (25 of 29 empirical papers) affirm that piracy harms content creators.[8] For example, the Carnegie Mellon University (CMU) study at the center of this report provides empirical evidence that consumption of pirated material detracts from the consumption of legal (ad-supported or subscription) services. In short, economists are getting better at developing the data, tools, and quasi-experimental structures to get a better measure of how much damage online piracy inflicts.

A 2016 study by the European Union's Intellectual Property Office highlights the size and scale of the cost: It estimated that the European music industry lost €170 million in sales revenue in 2014 as a consequence of digital piracy. This equals a loss of 5.2 percent of its total annual sales (both physical and digital) to piracy. When indirect economic impacts are included, digital piracy is estimated to lead to €336 million in lost sales in the European Union, which leads to an estimated 2,155 lost jobs.[9] This has real economic consequences,

as approximately 39 percent of total economic activity and 26 percent of all employment in the European Union is in intellectual property-intensive industries, with another 9 percent of jobs supported by the economic activity of these industries.[10]

Figure 1: Screenshot of a Torrent Site Hosting Illegal Copies of the Latest Movies



Even if they acknowledge that piracy comes at the cost of legal sales, some copyright critics will rationalize this loss by saying that it only hurts the profits of content firms, implying that if the choice is between theft that rewards consumers with free content versus legality that helps corporations, that the former is preferred. But it is important to realize that piracy reduces jobs, exports, and overall competitiveness in addition to standards of living

for a nation and its citizens. More directly, online piracy harms the artists and creators, both the famous and the struggling, who create content, as well as the technicians—sound engineers, editors, set designers, software and game designers—who produce it and those who support its marketing, distribution, and end sales.

One of the key policy issues around digital piracy is the importance of distinguishing between accidental and intentional piracy. Some rightly worry that antipiracy laws can go too far, sweeping in the former when they should be more focused on the latter. There are risks that poorly designed laws could unintentionally harm sites that are largely focused on legal material and that diligently work to limit infringing material. But we also know that doing nothing or little unintentional cases contributes to further piracy. Finding this balance does not mean abandoning efforts to go after intentional piracy.

The majority of piracy websites are in it for one reason: to make money. Modern digital piracy is a multibillion-dollar international business. (Only a minority of sites are supported by ideologues who believe that piracy is a social good.) For example, the owners of The Pirate Bay were earning $3 million a year, according to Swedish prosecutors.[11] More recently, U.S. law enforcement stated that one of the world's most popular piracy sites—KickassTorrents—was making $16 million annually in advertising.[12]

Business models differ, but the majority of piracy sites make money via advertising, or to a lesser degree, through subscriptions that provide premium access to content without advertising. The Digital Citizens Alliance's *Good Money Still Going Bad: Digital Thieves and the Hijacking of the Online Ad Business* report showed that 589 of the largest piracy sites generated more than $200 million in advertising-driven revenues in 2014.[13] Another report showed that 80 percent of the top piracy websites (550 of 622) in Europe carried advertising, showing how easy it is for piracy sites to profit from online advertising and how profit-driven these sites are.[14]

Piracy sites take advantage of the fact that the online economy has become more complex and easier to exploit. There are many intermediaries that aggregate ad space—known as an ad exchange—from a range of websites (both legitimate and illegitimate) for advertisers to use. This makes it easy for websites hosting illegal content to gain advertising revenue, including from legitimate brands and businesses, which may be several steps and organizations removed from the host site.

BOX A: TYPES OF DIGITAL PIRACY

Peer-to-Peer (P2P) File Sharing: This is a decentralized file-sharing system that is used extensively for the illegal distribution of copyrighted material. There are many legitimate uses for P2P technology, but the principal use has been to facilitate digital piracy around the world, via "torrents." A "torrent" is basically a file extension for torrent software programs to match one user to another "peer" in the network that contains part of the requested file. The file can be segmented among many users, making up a "swarm" of hosts that upload/download files from each other. A check of global traffic shows a number of torrent sites were among the most popular in the world: In early June 2016, KickAssTorrents was ranked 71st and Torrentz 192nd. The most notable example is BitTorrent. It is commonplace for these services to use searchable indexes of available material. More recent services, such as Popcorn Time and Cactus Player, deliver illegal content via peer-to-peer software, without the use of websites, yet with a Netflix-like user interface.

Streaming: Video and music streaming allows users to access content, such as music and movies, via a stream that can be web-based (similar to YouTube) or via standalone platforms (such as Microsoft Windows Media Player). Some services offer both (similar to Spotify). Illegal providers use the same technology to deliver illegal streams of sporting events, music, movies, and television shows. As streaming has become the preferred means of consuming content through legitimate sites, piracy sites have adapted the same technology to chase the audience.

Cyberlockers/Cloud Storage: Cyberlockers allow people involved in digital piracy to upload files to an online storage facility—the cloud. It requires little technical expertise as it can involve a simple web-based upload/download process. A web link to the stored file is created after a file is uploaded, which can be shared with other users. These piracy sites index the files hosted on the cloud storage sites to allow easy search and identification of specific content. Piracy operators often provide financial rewards for users that upload popular content. Users can pay for increased download performance from piracy sites.

WEBSITE BLOCKING

Policymakers should not consider website blocking in isolation; it is just one of many tools that countries can use to fight digital piracy. There is no single solution to creating a digital environment that supports and protects intellectual property, but there are a range of possible policies. In the fight against digital piracy, there are three possible targets: the consumer, the producer, and the middleman. In the United States the content industry initially attempted to prosecute consumers who engaged in rampant piracy, particularly repeat uploaders of illegal copies. But defenders of weak copyright attacked such efforts as unfair to average citizens, characterizing the efforts as disproportionate, ineffective, and judicial overreach; and as a result the industry largely abandoned the effort.[15] Second, copyright holders and government can go after producers of digital piracy. For domestically hosted content in the United States, copyright holders rely on remedies in the Digital

Millennium Copyright Act (DMCA), which has a "notice and takedown" process for rights holders to get website operators to remove infringing material. Copyright holders also (successfully) initiated court cases against several of the early peer-to-peer file-sharing networks, such as Napster and Grokster.[16]

There are a few ways that governments and content creators can fight international digital piracy. The first of these is straightforward and is already well underway: enact policies that increase the number of legal service providers in order to make it easier and cheaper for users to get legal media content online instead of using piracy sites. Another, which is also ongoing and obvious, is for law enforcement to specifically target website owners who operate digital piracy sites, such as Kim Dotcom (the owner of the major piracy site Megaupload.com, who was arrested in New Zealand in 2012) or the operator behind Kickass Torrents (who was arrested in Poland in June 2016).[17]

Fighting digital piracy gets much harder at the international level. That is because many countries that are home to digital piracy sites have governments that will not or cannot shut them down, whether because there are weak or nonexistent intellectual property protections or for geopolitical reasons. From a multilateral legal perspective, it is very difficult for the United States or others to bring cases against foreign digital piracy sites. To succeed, the United States requires the cooperation of the foreign government where the site is hosted, and despite the fact that virtually every nation that acts as a haven for pirate sites is in the World Trade Organization (WTO) and has signed on to the multilateral agreement protecting intellectual property—the Trade-related Aspects of Intellectual Property Rights (TRIPS) agreement—many nations, such as Russia and China, refuse to address digital piracy in their own jurisdictions. So, absent changes to the WTO, or a change in attitude of governments of scofflaw nations, governments will need to work with Internet intermediaries as the main solution.

There are several ways in which rights holders have worked with intermediaries in various countries. First, stakeholders involved in e-commerce have voluntarily agreed to work together to address aspects of the digital piracy ecosystem. For example, in the United States brand owners, advertising intermediaries, and content creators have agreed to work together to cut off the ad revenues that make digital piracy so profitable by ensuring that pirates are not profiting from ads for legal goods and services.[18] Another U.S. example is where rights holders and domain name registries have worked together to craft terms of service that prevent websites from illegally disseminating copyrighted content.[19] Other potential areas for collaboration between stakeholders involve cutting off piracy sites from online payment sources, such as PayPal, to ensure that such sites can't profit from illegal content (such as via subscriptions or ad revenue). Another is for search engines and social media platforms to reduce the visibility and availability of illegal content that often ranks highly in generic results in search engines or on hosted social media pages.

Second, they work specifically with ISPs. ISPs and content creators can work together to create a system that targets users who have illegally downloaded copyright-protected

content, sends them educational material about where to find legitimate sources, and informs them that the stakeholders know they are in violation of copyright laws.[20] It is a graduated system for repeat offenders, which can ultimately result in users having their Internet connection slowed or cut off entirely. Another option is for content creators and governments to enact voluntary or mandatory systems that require ISPs to block access to foreign sites that facilitate large-scale copyright infringement. Website blocking is seen as a logical next step since service providers hosting infringing material are often located in another jurisdiction and law enforcement cannot get cooperation to remove that material from the Internet.

The Mechanics of Website Blocking

This section explains what website blocking is, how website blocking can only ever be one policy in fighting digital piracy, the types of website blocking mechanisms, the costs of website blocking, and how website blocking is used in many countries for a variety of legitimate public policy goals.

Website blocking is simply the technical mechanism Internet service providers use to stop access to prohibited sites.

There are three key methods for website blocking: Internet Protocol (IP) address blocking, Domain Name Server (DNS) blocking, and Uniform Resource Locator (URL) blocking. While there may be ways for users and piracy site operators to circumvent these methods, it is important to remember that the aim of website blocking, like other online enforcement methods, is not to eliminate online piracy altogether, but to change consumers' behavior by raising the cost—in terms of time and willingness to find alternatives sites and circumvention tools—to make the legal sources of content more appealing.

Internet Protocol (IP) Address Blocking

Every computer has an IP address, similar to a street address or telephone number. When a user connects to the Internet, every packet of data sent or received over the Internet (e.g., for emails or to view websites) carries this IP address as does every destination on the Internet. Since ISPs act as central clearing houses for users' access to the Internet, they can modify their network settings equipment to discard user requests to access IP addresses for blocked sites. The costs of this process are low as the list of IP address is maintained centrally by the ISP.[21] Many ISPs and Internet backbone operators already use this process for security reasons (to fight malware) and to fight spam.[22]

There are a few ways that IP blocking can be circumvented, but these are cumbersome, and most Internet users do not have the sophisticated technical skills (and motivation) to sidestep blocking. Website operators can circumvent IP blocking by obtaining new IP addresses and reconfiguring their domain names so that users go to these new IP addresses, but this is also cumbersome, especially if it has to be done repeatedly.[23] Users can circumvent IP address blocks by using software (such as an encrypted virtual private network) to relay their Internet connection via a server that is with a different ISP or via a different Internet backbone operator that is not affected by the block, but most users are not this sophisticated.

A disadvantage of IP blocking is that IP addresses can be quickly changed. IP blocking can also impact non-infringing websites, as a single IP address can host multiple websites.[24] However, the focus of copyright enforcement and website blocking is on sites that facilitate large-scale copyright infringement—such as those that have many full-length movies, TV shows, and songs—so even if the IP address used by a piracy site hosts non-infringing pages or files, the legitimate content that is blocked is small, and not reason enough to avoid shutting down the website. If The Pirate Bay or KickAssTorrents facilitated access to a small amount of content that had a creative commons license, and was therefore able to be shared, this would not change the fact that it is a piracy site worth shutting down.

Domain Name System (DNS) Blocking

DNS blocking targets the process that converts website domain names into a corresponding IP address, which is then used to communicate with other servers. The DNS system effectively serves as the phone book of the Internet and is used by virtually every piece of software or hardware on the Internet, from web browsers and email applications to game consoles and streaming video devices.

An ISP can block an entire domain by making configuration changes at its DNS server. When a user asks to access a particular website, such as www.maindomain.com, the DNS server of the customer's ISP recognizes the domain as a blocked site, does not allow it to be translated into an IP address, and responds to the user that the domain does not exist or redirects to an informational webpage. DNS blocking is quick to implement, as existing systems can be easily adapted, and would only require a modest incremental investment for ISPs.[25] Critics claim that DNS blocking, like IP blocking, will cause "collateral damage" due to the risk of over-blocking, as a single domain can host many websites through website extensions.[26] However, this risk can be addressed by implementing DNS blocking at the subdomain level (e.g. www.piracysite.maindomain.com instead of www.maindomain.com). Furthermore, like IP blocking, if the main domain hosts a site that has the primary purpose of facilitating illegal access to copyrighted material, then it is a legitimate target for online enforcement.

A website operator that hosts copyright infringing material would only be able to circumvent the DNS block by using another domain name, but like IP blocking, this becomes cumbersome. Users are able to circumvent this process by using another domain name server (e.g., users could use a virtual private network to connect to an alternative DNS server not subject to the blocking orders). However, like IP blocking, it would be a mistake to assume that the average Internet user has the above-average technical skills necessary to do this. Many, if not most, consumers have low levels of computer literacy and certainly are not sophisticated enough to understand how to manipulate the DNS settings in the network configuration of their computers, mobile phones, and other Internet-connected devices. Furthermore, users who switch DNS servers can expose themselves to many security risks if they cannot trust the responses from these servers. For example, while the alternate servers may reliably return the correct IP address for a Russian file-sharing site,

they might not return the correct address for Bank of America.[27] How many users are willing to risk their identity and financial information just to download a few songs?

Finally, circumvention software (such as encrypted virtual private networks) probably will not be adopted by many, as studies show that few users use these types of tools in countries where the government restricts access to certain websites. For example, a study by the Berkman Center for Internet and Society at Harvard University found that "no more than 3 percent of Internet users in countries that in engage in substantial filtering use circumvention tools. The actual number is likely considerably less."[28]

Uniform Resource Locator (URL) Blocking

URL blocking requires the ISP to examine both the headers of IP packets (which contain the source and destination IP addresses) and the contents of the IP packet. This is done through "shallow" or "deep" packet inspection (DPI) that examines the contents of the packet in transit, rather than simply the IP address of the source and destination devices. Shallow packet inspection is focused on IP addresses and technical specifications, such as port and protocol combinations. Deep packet inspection examines the packet for specific characteristics or values. When a packet matching the blocked site IP address, destination host, or even a particular keyword passes through a DPI device, the network connection can be terminated. These inspections can be performed by the ISP's router or a proxy that all traffic is forced through in order to access the Internet (such proxy servers are common in schools and businesses, as they cache content, block inappropriate sites, and provide some security).

This process can block specific websites (e.g., www.itif.org) or website addresses (e.g., www.itif.org/events/upcoming). Given this capability, URL blocking is the most precise method, thereby avoiding over-blocking.[29] URL blocking combines the advantages of both DNS and IP blocking.[30] To be effective, URL blocking needs to be designed so that it only targets specific types of network traffic, whether this is related to sites that actively facilitate terrorism, child pornography, or copyright infringement.

Network Functions Virtualization and Software-Defined Networks Can Make Blocking Cheaper, Easier, and More Effective

Software-Defined Networks (SDN) and Network Functions Virtualization (NFV) will fundamentally change how telecommunications carriers manage network operations and enable flexible new tools to block websites.[31] These technologies, already used in many data centers, will eventually become key components of virtually all wide-area carrier networks for the simple reason that they offer powerful new tools and significant cost savings.[32] These advantages are spurring surprisingly quick adoption of these techniques by industry. For example, AT&T plans for 30 percent of its network to use SDN and NFV by the end of 2016 and 75 percent by 2020.[33]

SDN separates the control of the network from the forwarding of information, offering network operators global control over switches and routers through software separate from the underlying hardware. This in turn allows networking applications, such as DNS,

firewalling, and intrusion detection, to run in virtual systems installed on generic hardware whereas traditional network infrastructure relied on dedicated, fixed-function networking hardware. Combined, SDN and NFV allow greater network flexibility, easier introduction of new services, improved network manageability, and reduced costs.[34] In line with this, these changes in network management will make it much easier and cheaper to implement website-blocking mechanisms. For example, blocking could be achieved on the fly through software updates rather than individualized hardware configurations.

The Costs of Website Blocking

Many countries have turned to website blocking to apply existing and new legislation to a range of legitimate public policy goals that involve the Internet.

The costs of website blocking vary according to the type of blocks used and the country implementing them. More intensive processes, such as deep packet inspections, cost more. All website-blocking processes involve technical support costs for administering the blocking process within an ISP's network and in fielding calls from users about why they cannot access certain sites. There are hosting costs for the landing page that users trying to access blocked sites are redirected toward, as required in many countries. Cost estimates for initial website blocking injunctions are likely to be high, given the legal costs involved in landmark court cases that a legal process for rights holders to use. However, once a website-blocking process is up and running, parts of it can be automated in order to minimize costs. For example, a centrally maintained register (with digitally signed lists of IP addresses) could be used by all ISPs in a country to update their settings to ensure that all necessary sites are blocked.

The United Kingdom's communications regulator, Ofcom, ranked the costs of different blocking techniques:

- IP address blocking: low cost;
- DNS blocking: marginal incremental cost;
- Shallow packet inspection: low cost if implemented only on routers, costly if implemented on firewall devices;
- Deep packet inspection: relatively costly given the inspection of network traffic; and
- URL blocking: potentially costly given hardware and software configurations, but this will change as ISPs move to software-defined networks.[35]

Detailed information on the specific costs of the various approaches and systems is unavailable, partly because this is still a relatively new policy area. In the United Kingdom, legal documents filed by lawyers representing rights holders estimated that the cost can be as high as $18,900 per new website blocked for each ISP.[36] UK ISPs have not publicly stated what the ongoing costs of website blocking are: What figures exist vary from a few hundred to a few thousand dollars.[37] The cost to block the first website in the United Kingdom, for NewzBin2, was $7,100 for the main domain and $142 for each subsequent site (if the website operator tried to move to another site).[38] Without providing a detailed breakdown, an Australian government estimate gave the cost per ISP to enact website blocking as $95,000 annually.[39] Estimates by Australian ISPs also vary—from $36 per domain name (TPG Internet), to $183 per site and $29 per DNS (M2 Communications),

to $7,350 in labor costs for setting up initial compliance, $2,200 for a landing page, and $18 per additional site (Telstra).[40]

Website Blocking Is Used as a Legitimate Tool by Many Countries

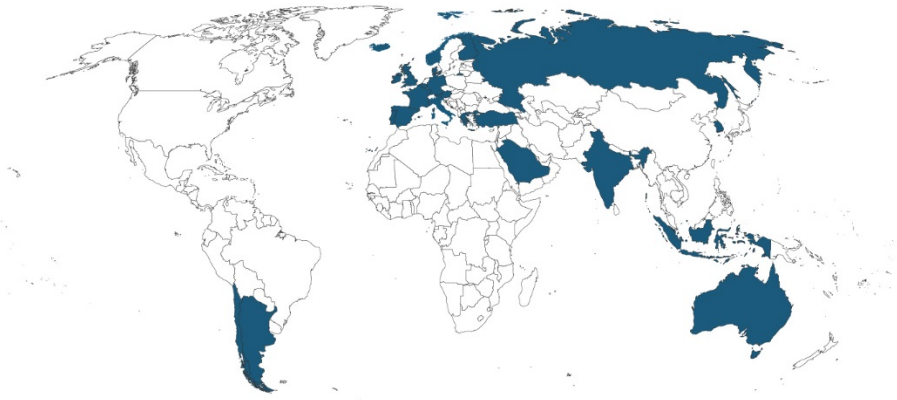
Many countries have turned to website blocking to apply existing and new legislation to a range of legitimate public policy goals that involve the Internet. Examples of the types of websites that are blocked:

- Child pornography (many countries)
- Malware (e.g. Australia)[41]
- Investment fraud (e.g. Australia)[42]
- Online gambling (e.g. Singapore and Quebec, Canada)[43]
- Pornography (e.g. India and others)[44]
- Prostitution (e.g. India)[45]
- Terrorism (the United Kingdom, Australia, France, and India)[46]
- Copyright-infringing content (at least 25 nations)

As an example, website blocking is used extensively to block child pornography websites. International Criminal Police Organization (INTERPOL)'s 190 members voted unanimously to promote the use of all technical tools, including website blocking, to fight child pornography. INTERPOL maintains a list of domains containing websites that disseminate the most severe child abuse material worldwide as part of a "worst of" list.[47] INTERPOL provides domains, not URLs, for blocking. As INTERPOL explains, blocking does not by itself remove the offending content, but it does dramatically reduce the amount that is accessible and available to most users. In this case, website blocking is used in conjunction with other measures.

For online copyright infringement, there are at least 25 countries that allow website blocking (see Figure 2 below). The first website blocked for copyright infringement was AllofMP3 in Denmark in 2006. (For further details on website blocking in the United Kingdom see Appendix A, for Australia see Appendix C, for the European Union see Appendix D, and for the United States see Appendix E.) A Motion Picture Association of America report from September 2015 stated that European ISPs block more than 500 websites—238 in Italy, 135 in the United Kingdom, 41 in Denmark, 24 in Spain, 18 in France, 15 in Portugal, 13 in Belgium, 7 in Norway, and smaller totals for other countries.[48] The actual figure is likely much higher, as some countries, such as the United Kingdom, do not release specific details on which websites are being blocked, in order to not alert website operators. Furthermore, countries have recently added more sites: Portugal added over 240 between December 2015 and April 2016.[49]

Figure 2: Countries That Allow Website Blocking for Copyright Infringing Content



Australia, Argentina, Austria, Belgium, Chile, Denmark, Finland, France, Germany, Greece, Iceland, India, Indonesia, Ireland, Italy, Malaysia, Norway, Portugal, Russia, Saudi Arabia, Singapore, South Korea, Spain, Turkey, and the United Kingdom.

SITE BLOCKING CAN HELP FIGHT ONLINE PIRACY

At least 25 countries use website blocking to stop access to websites that facilitate copyright infringement online.

Some proponents of weak copyright argue that site blocking does no good, as content thieves will just find other sites to go to. In practice, this appears to be wrong. A new Carnegie Mellon University (CMU) study shows that the latest expansion of website blocking in the United Kingdom has been effective in fighting digital piracy. This study, released in April 2016, uses consumer data to analyze the impact of a court order for ISPs to block 53 websites in the United Kingdom in November 2014. This study shows that website blocking, when done on a large enough scale, can shift consumers from accessing copyright infringing material to consuming legal content online.

The United Kingdom has had the legislative ability—in the form of an amendment to the Copyright, Designs, and Patent Act law—to allow website blocking since 2003, but it was not used until a landmark court case in 2011 (see Appendix A). This case set a legal precedent for rights holders to force ISPs to block websites that facilitate copyright infringement.[50] Subsequent court decisions have since clarified the steps involved in these cases and streamlined the process for rights holders to get websites added to a list of blocked sites, which now likely numbers in the hundreds.

The court-ordered injunctions are aimed at websites whose purpose is clear—to facilitate large-scale copyright infringement. The onus is on rights holders to prove to the court that each website they want blocked (each case involves a number of websites) are indeed facilitating widespread copyright infringement. If rights holders are successful, the court issues an injunction that forces all ISPs in the UK to block the primary offending website and any other website that the operator shifts to in an attempt to circumvent the block (e.g. www.digitalpiracy.com to www.digitalpiracy2.com). In this regard, the court order is

dynamic. The specific list of blocked websites is not officially published in order to facilitate implementation, but UK ISP TalkTalk listed 1,357 file-sharing sites (as of August 2016) it was blocking for copyright infringement.[51]

The CMU study empirically tests an intuitive understanding about online copyright enforcement—if enough piracy sites are blocked, then people will shift to legal sources, especially given the growing number of such services. The study analyzes consumer-level data over a few months (both pre-block and post-block) to look at how blocking 53 websites changed user behavior in terms of their consumption of illegal and legal content. Website blocking forces consumers in the United Kingdom, and other countries that use website blocking, to make a choice: find ways to circumvent the blocks, find other sites to access pirated content, increase their use of legal channels, or decrease their consumption of the media in question.

The results reinforce a central intuitive point—that making legal content more attractive can turn some pirates into legal consumers, but that it is more effective when accompanied by enforcement.

This is the second CMU study that analyzes the evolution of website blocking orders in the United Kingdom from a single site to dozens/hundreds. The first part of the initial study focused on the blocking of a single (albeit notorious and popular) site—The Pirate Bay—in the United Kingdom in May 2012. Before the block, The Pirate Bay had an estimated 3.7 million users in the United Kingdom and made approximately $3 million in advertising a month by providing millions of illegal copies of music, movies, and other types of content to its users.[52] The study found that blocking The Pirate Bay on its own had only a small impact on total piracy and no impact on consumer uptake of paid legal streaming services—former users switched to "proxy" sites that mirrored the contents of The Pirate Bay, circumvented the blocks with virtual private networks, or dispersed to other piracy sites.[53]

The second part of this first study looks at a broader blocking of piracy websites. The study estimated that the blocking of 19 major piracy websites in the United Kingdom between October and November 2013 caused a significant increase in usage of paid legal streaming sites—by an average of 12 percent, which increased to 23.6 percent for the heaviest users of these piracy sites.[54] The authors also concluded that piracy does indeed displace usage of legal paid streaming sites, despite the relative convenience and low cost of such sites. Finally, these results reinforced a central intuitive point—that making legal content more attractive can turn some pirates into legal consumers, but that it is more effective when accompanied by enforcement.[55]

The latest CMU study analyzed the impact that blocking 53 piracy websites in the United Kingdom in November 2014 had on the behavior of 58,809 users, comparing user visits three months before the blocks against user visits in the three months after the blocks (see Appendix B for the study's descriptive statistics).[56] In both studies, the British Phonographic Industry (the trade association that represents the British record industry) was responsible for compiling and submitting to the court the list of websites for blocking.[57] The court orders covered the six biggest ISPs, who collectively provide Internet services to over 90 percent of the United Kingdom.[58]

The study found that this round of website blocking caused a 90 percent drop in visits to blocked sites and did not cause former users to increase visits to unblocked piracy websites.

The study does not focus on individual users, but segregates users into 10 groups based on the number of times they used the piracy sites during August, September, and October 2014. Compared to the first study, this latest study expanded the window of time to compare pre- and post-block user behavior from two to three months. The control group includes users who did not visit the blocked sites, while the 10th segment includes heavy users, who visited the blocked sites over 35 times in September 2014. The study observes the aggregate number of visits and time spent in different categories of sites during each month: visits to blocked sites, visits to unblocked piracy sites, visits to virtual private networks sites, visits to legal ad-supported video sites (e.g., BBC's iPlayer and the UK Channel 5's "Demand 5" streaming site), and visits to legal subscription sites (e.g., Amazon Prime and Netflix). The study then used regression analysis to estimate the impact of the blocks (see Appendix B).

The results clearly showed that the website blocks were effective in changing consumer behavior. (Also see Appendix B.) To estimate the impact of the blocks, the study determined the difference between the observed activity by users after the blocks were enacted and the estimated counterfactual (as if the blocks had not been enacted) for these users' visits to piracy, ad-supported video, and subscription-based websites. The study found that:

- The blocking of these websites was effective, causing a 90 percent drop in visits to the blocked sites by users in the study sample (from 86,735 visits to blocked sites to 10,474), while causing no increase in usage of unblocked piracy websites.[59]

- The blocking of these websites had a significant impact on piracy, leading to a 22 percent decrease in total piracy for all users affected by the blocks (relative to the counterfactual estimate for how much they would have pirated if not for the blocks). The study is able to analyze the broader piracy universe as the 53 sites that were blocked were only a portion of the total piracy sites tracked in the study.[60]

- These blocks changed consumer behavior. The study estimated that the blocks caused a 10 percent increase in user visits to legal ad-supported streaming sites such as the United Kingdom's BBC and Channel 5.[61] It also caused an estimated 6 percent increase in visits by users in the study to paid legal subscription-based streaming sites such as Netflix. This contrasts with the 12 percent increase in visits to subscription-based sites in the study of the 2013 blocks.[62] The latest figure may be lower due to increased price sensitivity of the remaining pirates in 2014 or due to the lower popularity of the 53 sites in 2014 compared with the 19 sites blocked in 2013.

- Relatively few users circumvented the website blocks. The study estimates that access to VPN sites increased 30 percent after the blocks, but this is likely off a relatively small base. The descriptive statistics show usage of VPN services is small relative to visits to other sites. For example, users in the study made 86,735 visits

to the piracy sites before they were blocked, but only 1,688 to VPN sites (see descriptive statistics in Appendix B).

- The blocks had the biggest impact on the heaviest users of piracy sites. The study estimates that the blocks caused the heaviest piracy users in the study sample to reduce their use of pirated material by 28 percent, while leading to a respective 48.1 percent and 36.9 percent increase in their purchases of legal ad-supported and subscription services.

Some of the differences between the CMU studies into the two rounds of website blocking orders—the first from 2013 and the second from 2014—in the United Kingdom are worth highlighting:

The study shows that a greater number and variety of legal sources make it easier to use website blocks to push people away from piracy.

- **A greater number and variety of legal sources make it easier to use website blocks to push people away from piracy.** It makes intuitive sense that greater availability and competition in legal content sites makes it easier to persuade people to use legal sources. The difference in the impact that blocks had may be partly due to changes in the users involved in online piracy as legal distribution channels, such as Netflix, became more prevalent between 2013 and 2014. Many users who were less committed to piracy may have already switched to legal sites after the 2013 round of website blocks, thereby lowering the potential impact of the 2014 expansion. While the 2013 study did not cover ad-supported legal services, the larger shift to these services in 2014 may reflect that piracy users may be more price sensitive (since ad-supported services are free) and therefore more likely to change to these services after piracy websites are blocked.

- **The biggest gains come from blocking the most popular sites.** Piracy users were more heavily concentrated around a small number of piracy sites when the first round of piracy websites were blocked in 2013, meaning that users of piracy websites were dispersed among a greater number of sites when the second set of websites was blocked in 2014. This highlights the need for a continuously updated list of targeted websites as remaining users try to shift to other sites. Making sure the most popular piracy websites—at any given time—are inaccessible will maximize the impact of website blocking.

- **Blocking has the biggest impact on heavy users of pirated material.** The remaining users that consumed pirated material in 2014 may have been the "hard core." Those consumers that were less committed to piracy may have already been shifted to legal content (due to the availability of legal sources and the impact of prior blocks), leaving only the most committed users of piracy sites, as these consumers have a higher "willingness to pay" in terms of search costs—and are therefore harder to shift. These users may also be more technically savvy in searching for and finding reliable alternative sources of pirated material. However, the latest study shows that widespread website blocking can shift at least some of these hard-core piracy users to consume greater amounts of legal content, even if they still access illegal content, albeit at lower levels.

In summary, the study shows that while website blocking will not solve online piracy—no single tool, law, or practice will—it does reduce it while increasing the consumption of legal content. It then falls to other policies to target different parts of the piracy process and environment, which the United Kingdom does through a graduated response system for ISPs to notify users of reported infringement, funding for education campaigns about accessing legal and illegal content, and a specialized Police Intellectual Property Crime Unit to investigate and tackle copyright infringement. All these measures, when combined with ongoing service and technology innovations, help tip the balance back toward the digital creators that rely on intellectual property to support and protect their creations and away from the rampant piracy that undermines their creativity.

OBJECTIONS TO WEBSITE BLOCKING

Internet exceptionalists, such as the Electronic Frontier Foundation, argue that rules that apply offline should not apply online.

Copyright minimalists have long discounted the need for and effectiveness of virtually all polices designed to reduce piracy. It is no surprise that they object to website blocking. This section details and rebuts the most common criticisms to website blocking of digital piracy. In 2011, U.S.-based opponents of website blocking used many of these arguments when Congress contemplated legislation that would have allowed website blocking in the United States (see Appendix E).

Normal Rules Do Not Apply to the Internet

Internet exceptionalists, such as the Electronic Frontier Foundation, are defined by a belief that because the Internet is exceptional, most rules that apply offline should not apply online.[63] For these groups, the Internet is first and foremost about individual freedom, not about collective responsibility. Their view is that the Internet's chief function is to liberate individuals from control by, or dependence on, government and corporations. They see the Internet as a special place not anchored to physical geography that stands above and beyond the reach of rules that govern the offline world.

Yet, in reality and for most of the rest of us, the Internet is no different than the offline world, where people have rights and responsibilities and where laws against certain behaviors exist. There is no logical reason why a crime in the physical world is not a crime in the digital world. To be sure, there is need for balance in these policies, to avoid unnecessary costs or impacts on other interests and rights, but this applies online as well as offline.

Opponents of website blocking often respond that blocking is antithetical to efforts to preserve a "free and open" Internet. While this is a rightly and broadly supported goal, at least in most democratic nations, it does not mean that every website should be freely accessible.[64] But just as supporting bans on the importation of ivory or cross-border human trafficking does not make one a protectionist, supporting website blocking for sites dedicated to piracy does not make one an opponent of a free and open Internet. Clearly, society should want as little as possible to be blocked or taken off the Internet, but that does not mean that we should oppose attempts to block online materials that are clearly illegal.

Blocking Will "Break the Internet"

Critics claim that website blocking, particularly DNS filtering, will "break the Internet" by undermining "basic Internet infrastructure."[65] In the United States these claims were made by opponents to proposed legislation that would have allowed website blocking in 2011. (See Appendix E.) The irony is that just months before leading opponents stated their opposition to website blocking, a key opponent said it was okay to block domains that spread malware and that this could be done without harming the Internet itself. But somehow doing the blocking for copyright infringement was completely different.[66] Never mind the fact that there is significant overlap between digital piracy sites and malware sites.[67]

Yet, the growing use of website blocking since then shows that these claims were not based in reality and that website blocking did not "break the Internet," nor lead to a multitude of other predicted dire outcomes, such as the widespread circumvention of blocking orders, the fragmentation of the global DNS namespace for the Internet, an alternative DNS system for the Internet, nor contribute to a breakdown in user trust and an exodus of users from the Internet.[68] The reality is that the people in these countries with blocking orders still have a working Internet and use the Internet in much the same way as the rest of us.

Blocking Will Be Ineffective

Critics claim that website blocking would be ineffective, as there are too many sites online that facilitate copyrighted content.[69] For example, if consumers want to download a pirated copy of the latest movie and they know three sites from which they can obtain a copy, blocking access to only one of these sites will not change their behavior. However, if all three are blocked, the consumer has a choice of paying a cost—a search cost or a learning cost—to discover new reliable illegal sources or paying the legal price and obtaining a legal source.

This goes to the heart of what the CMU study found in the United Kingdom: If website blocking is done sufficiently broadly, it can lead to significant changes in consumer behavior. For low-level piracy users with a low willingness to pay, a broad range of website blocks is a sufficient for many to switch to legal sources. Even for high-level piracy users, who are likely to be more technically savvy in finding alternative piracy sites, widespread website blocking leads to a substantial rise in the consumption of legal content. As a presiding U.K. judge, Justice Arnold, stated in comments on the efficacy of website-blocking orders in a recent case—although experienced and determined users would be able to circumvent the blocking measures, blocking websites has proved to be reasonably effective in reducing use of those websites in the United Kingdom.[70]

Critics claim that website blocking is an exercise in futility as website operators shift sites—the so-called "whack-a-mole" effect—but the United Kingdom's approach shows that this can be countered through a dynamic blocking order. ISPs are required to block the website named in the initial court order, and when notified in writing, any other IP address or URL whose sole or predominant purpose is to facilitate access to the named website.

The CMU study also shows what other studies on the effectiveness of online enforcement have made clear—that the impact depends on public awareness and consistent and credible enforcement and implementation. Government interventions targeting online infringement can reduce piracy, especially when done in cooperation with firms to promote legal content, but when enforcement activity loses credibility, piracy and sales of legal content revert to original levels.[71] For example, the 32 percent decrease in piracy caused by Sweden's IPRED law (which made it easier for rights holders to detect and identify file sharers) returned to previous levels after six months as the public realized it was not going to be enforced.[72] Likewise, if a legitimate firm offers its content in a timely and convenient fashion, but the government does nothing to enforce copyright, then the firm is effectively competing against a "free" pirated version.[73]

The key takeaway the CMU study found in the United Kingdom is that if website blocking is done sufficiently broadly, it can lead to significant changes in consumer behavior.

Blocking Is a Form of Filtering and Censorship

Critics claim that website blocking will set a negative precedent if used by democratic countries and will weaken the moral authority of democratic nations to criticize totalitarian governments for limiting Internet access unrelated to intellectual property. They claim that these governments would point to democratic nations' use of website blocking to justify their Internet censorship.

But the U.S government has not abandoned its long practice of banning the use of U.S. mail to send illegal products because it fears giving an excuse to foreign governments to censor their mail. Likewise, the U.S government has not changed laws that limit the ability of newspapers to publish information that is libelous because it fears it will give comfort to nondemocratic nations that want to control information access. Likewise, the U.S. government has not abandoned laws requiring child pornography to be blocked because it thinks it gives carte blanche approval to dictatorships that want to block dissenting websites. Governments' response to rioters who engage in wholesale property destruction and violence isn't based on the fear that they encourage totalitarian governments to use police to suppress citizens. In short, there is no comparison between a country that uses detailed and transparent legal means, supported by an independent legal system to administer such rules, to enforce intellectual property online and a country censoring political speech online.

Some opponents of website blocking have seized upon reports of governments misusing intellectual property enforcement measures for unrelated means, such as the Russian police raid on advocacy groups and opposition newspapers in the name of searching for pirated software.[74] However, such cases are rare and would not stand up to the type of scrutiny that is involved in the hundreds of cases where website blocking has been used to fight online piracy in recent years. Online intellectual property enforcement is far from alone in being a public policy that could be misused in order to pursue unrelated and illegitimate objectives. In each case, what matters is the actual intent and the integrity of the process involved in administrating these policies.

Blocking Will Be Expensive for ISPs and Other Intermediaries

Opponents of website blocking, including some ISPs, believe that the costs of website blocking are high enough to make the practice untenable. Internet exceptionalists fill the void created by the lack of detailed information about website blocking costs to paint the policy as unfeasible and unfair to both ISPs and consumers. However, these claims should not be taken at face value. The fact that we have not heard any uproar over the costs of website blocking of sites that actively facilitate child pornography or terrorism shows that enacting these blocks is not prohibitively expensive. In line with this, UK courts noted that ISPs have already made much of the necessary investment in relevant technology, processes, and staff in response to other law enforcement requirements.

As discussed above, website blocking costs look reasonable, especially when compared against total ISP operating revenue and investments. The UK government and judges presiding over website-blocking cases have stated that IP address-blocking would require ISPs to make additional investment in network hardware, but that these costs were not substantial, in many cases had already been made (to abide by other law enforcement decrees), and therefore would not present a barrier to IP blocking. Furthermore, in a similar process to what is required for website blocking, some DNS software vendors already offer customers an add-on to DNS systems that blocks malicious domains.[75]

Blocking Will Be Abused by Content Rights Holders

Critics claim that any measure to fight digital piracy will be abused by rights holders and that even the potential for such abuse is reason enough not to pursue online enforcement in the first place. This is why legislation and court orders in Australia, the United Kingdom, and elsewhere have built-in safeguards to ensure that only rights holders with high-quality cases—those involving websites that are dedicated to copyright infringement—are granted an injunction.

Safeguards are a common feature of legislation allowing website blocking. For example, in the United Kingdom, the courts have considered and set out criteria for rights holders to clear before they can apply for a website-blocking injunction, such as whether blocking is a proportional response, the availability of alternate measures, the cost of the website-blocking order, and the impact the block will have on the individual as well as the broader public. Furthermore, if website owners feel that they've been unfairly targeted, they can apply to discharge or vary a court injunction.[76] In Australia, the legislation that allows website blocking specifically mentions that it cannot be applied to websites that are mainly operated for a legitimate purpose, but contain a small amount of infringing content (see Appendix C for further details). Furthermore, rights holders have to inform the website owner of the injunction application to give them a chance to respond.[77] In Portugal, the system explicitly requires a minimum of 500 works that allegedly infringe or that two-thirds of the content on a site must be infringing copyright.[78] These are quite normal and reasonable safeguards that are used to ensure that cases are legitimate, necessary, and open to revision or overturning.

CONCLUSION

As with any law-enforcement initiative, efforts to reduce digital piracy involve balancing costs and benefits. For example, while street crime could be reduced by doubling the number of police officers, communities seek an equilibrium where the marginal cost of an additional police office does not outweigh the benefits from a corresponding reduction in crime. Regarding digital piracy, it is hard to argue that this equilibrium has been reached—there remains a lot of societal benefit to be gained through better efforts to stop digital piracy. The extent of digital piracy is so large, and the costs of additional enforcement are so reasonable, that it is clearly in the public interest to take more aggressive steps to fight digital piracy.

Countries that use website blocking have built in intentionally high thresholds to ensure it is only used appropriately.

There is a reason why website blocking is being used in a growing number of countries: It can be a reasonable and useful tool to reduce piracy and encourage consumption of legal content. For it to be effective and workable, it needs to be predictable, transparent, accountable, low-cost, and quick to implement. To be sure, website blocking is no silver bullet in the fight against digital piracy, but it should at least be one of the lead bullets, alongside other measures such as partnering with Internet ad companies, notice-and-takedown processes for websites hosting infringing material, domain seizures, and other efforts to prosecute owners of pirate sites.

Many opponents focus on the fact there are technical ways to circumvent website- blocking orders. However, the CMU study and others show that these users make up a relatively small proportion of total Internet users—certainly not enough to render website-blocking orders ineffective. Some critics would say that if blocking a website is not effective all of the time, then it should not be used at all. This is the same weak argument used against virtually every type of countermeasure. Why bother locking a door, when it is possible for sophisticated thieves to pick the lock? The answer, clearly, is that most thieves are not that sophisticated.

Complex problems with no single solution benefit from multilayered solutions. The standard for effectiveness should not be, as some opponents claim, elimination of all piracy. Reduction is an important goal, and on this point, the CMU study shows that website blocking can certainly help achieve this goal.

APPENDIX A: WEBSITE BLOCKING IN THE UNITED KINGDOM

In the United Kingdom, a landmark court case in 2011 created the legal precedent that has allowed rights holders to ask for court injunctions to block websites that infringe copyright.[79] This is despite the fact that the law allowing website blocking in the United Kingdom has been available since 2003 (when section 97A was added to the Copyright, Designs, and Patent Act (CDPA) 1988 as part of the European Copyright Directive 2003). The exact number of websites blocked in the United Kingdom is unknown, as these are kept secret in order to ensure the block is as effective as possible.

For a court to issue an injunction, it must be shown that: the ISPs were service providers, the users or operators of the target websites infringed copyright and used the services of the ISPs to do so, and the ISPs had actual knowledge of this.[80] The court can also consider whether the block is proportionate—whether the likely cost burden on the ISPs is justified by the efficacy of the blocking measures and the consequent benefit to the rights holders.[81] In assessing proportionality, the court considers the availability of alternative measures; the efficacy, costs, and dissuasiveness of the measure; and the impact on lawful users of the Internet.[82] In terms of proportionality, the presiding judge in one of these initial cases considered the alternatives, but held that those measures were unlikely to be sufficient in stopping the infringement, and that website blocking can be considered a primary tool for rights holders to use. Furthermore, the judge found that on balance the evidence showed that blocking measures can be very effective.[83]

The United Kingdom is adapting its online piracy efforts to the various services and technologies used to facilitate copyright infringement. For example, BitTorrent websites and streaming websites have been held to infringe copyright by communication to the public even though the infringing copy did not come directly from those websites, but because the websites contained catalogued and indexed connections to the sources of those copies.[84] More recently, courts have dealt with cases involving software that facilitates access, while not actually transmitting infringing material to the public, such as Popcorn Time. Popcorn Time is an open source application that uses BitTorrent technology and can be downloaded from a website that allows users to browse, search, and locate illegal copies of films and television programs. United Kingdom courts have found that the operators of the website which offered Popcorn Time, while they did not transmit or retransmit infringing content, did facilitate the making available of infringing content by providing the tool to do so and therefore should be blocked.[85]

APPENDIX B: STUDY DETAILS AND RESULTS

Table 1: Descriptive Statistics

Consumer Segment	Users in Segment	Avg. Visits to Blocked Sites Per User	Total Piracy Visits	Legal Ad-Supported Visits	Legal Subscription Visits	VPN Visits
0	**53,273**	**0.0**	138,257	61,967	57,475	4,854
1	**1,737**	**1.0**	31,553	6,610	7,692	390
2	**801**	**2.0**	18,027	2,346	3,322	147
3	**451**	**3.0**	15,073	2,286	1,871	166
4	**319**	**4.0**	11,665	1,119	1,301	18
5	**426**	**5.4**	15,802	1,590	1,978	229
6	**478**	**8.3**	23,118	2,389	2,666	71
7	**396**	**13.2**	28,988	1,999	3,446	524
8	**502**	**23.8**	56,917	3,448	3,018	115
9	**426**	**78.6**	140,423	3,178	2,496	28

Table 2: Regression Effects

To determine the impact of the website blocks, the study uses a difference-in-difference regression model (below). The *After* dummy variable controls for the difference between the pre-block period and the post-block period. The *Treatintensity* variable indicates the number of visits that the average user in each group made to the 53 blocked sites during August and September 2014. Variable μ is a vector of group fixed effects.

$$LnVisits = \beta_0 + \beta_1 After + \beta_2 TreatIntensity * After + \mu + \varepsilon$$

	Unblocked Piracy	VPNs	Legal Ad-Supported	Legal Subscription
After Block	-1.053* (0.001)	-1.500* (0.004)	-0.586* (0.000)	-0.619* (0.000)
Treat Intensity x After Block	-0.002 (0.38)	0.030*** (0.066)	0.005** (0.050)	0.004 (0.251)
Constant	10.178* (0.000)	5.148* (0.000)	8.131* (0.060)	8.217* (0.000)
Observations	20	20	20	20
Consumer Groups	10	10	10	10
R-squared	0.979	0.851	0.99	0.97

Parentheses show p-values. Based on a t distribution with 8 degrees of freedom.

***= significant at 10 percent; **=significant at 5 percent; *=significant at 1 percent

A few key points:

- The variable of interest is $\beta_{2,}$ as it shows the causal impact of the block on visits to sites. Its coefficient is small, negative, and statistically significant for unblocked piracy sites, indicating that the blocks did not cause former users of blocked sites to increase their consumption at other illegal sites.

- Some users of the blocked sites did employ technical workarounds, as shown by the coefficient for visits to VPN sites (which is positive and significant at the 90 percent confidence level). It estimates that for every 10 additional visits to blocked sites before the blocks, a consumer increased visits to VPN sites after the blocks by an additional 30 percent. However, Table 1 shows that VPN site visits before the blocks were small relative to other sites.

- There was a positive and statistically significant increase in usage of ad-supported sites. A 10 visit increase in pre-block visits to blocked sites is correlated with a 5 percent increase in visits to legal ad-supported sites.

Table 3: Estimated Causal Change in Piracy and Legal Viewing

Pre-block Visits/Users of Blocked Sites	Causal Decrease in Total Piracy	Causal Increase in Ad-Supported Services	Causal Increase in Subscription Viewing
0.0	0.0%	0.0%	0.0%
1.0	7.6%	0.5%	0.4%
2.0	11.4%	1.0%	0.8%
3.0	11.1%	1.5%	1.2%
4.0	13.5%	2.0%	1.6%
5.4	17.0%	2.7%	2.2%
8.3	20.2%	4.2%	3.4%
13.2	22.8%	6.8%	5.4%
23.8	25.3%	12.6%	10.0%
78.6	28.0%	48.1%	36.9%

APPENDIX C: WEBSITE BLOCKING IN AUSTRLAIA

Australia has two laws that allow website blocking: The Copyright Amendment of 2015 and the Telecommunications Act of 1997.

On June 22, 2015, the Australian government enacted the Copyright Amendment (Online Infringement) Act 2015, which added a new injunction power into the Copyright Act 1968 that could be used to block websites. Section 115A of the amendment gives the federal court of Australia the power to order an injunction to require an ISP to block access to "online locations" located outside Australia whose "primary purpose" is infringing or facilitating copyright infringement. "Online location" was used as an intentionally broad term that includes, but is not limited to, websites and would also accommodate future technologies. The "primary purpose" test was designed as an intentionally high threshold, intended to exclude websites that are mainly operated for a legitimate purpose, but contain a small percentage of infringing content.[86] In granting an injunction, the court may take into account a range of factors, including the flagrancy of the infringement, whether the website is blocked in another jurisdiction, whether blocking is a proportionate response, the public interest, and the impact on any class of person affected by the injunction.[87]

Unresolved issues around implementation of this amendment include: who would bear the costs of the website-blocking injunction; whether blocked websites would be redirected to a single "landing page" or many such pages, and who would host such landing pages; who would contribute to the cost of hosting those landing pages; and how long blocks are in place. The judge presiding over the first application for an injunction has asked ISPs to provide cost estimates before deciding whether to issue an injunction.[88]

Australia also allows website blocking for sites involved in investment and financial fraud and malware and phishing sites under section 313(3) of Australia's Telecommunications Act 1997. This Act specifies that blocks occur through URLs rather than IP addresses.[89]

APPENDIX D: WEBSITE BLOCKING IN THE EUROPEAN UNION

While there is no European Union-wide approach to website blocking, there is a common legislative platform that allows individual member countries to enact such measures.

The European Union's E-Commerce Directive of 2000 provides liability exemption for a range of Internet service providers—known as "safe harbor"—in that they are not liable for information transmitted over their network, such as pirated material. However, this exemption does not excuse them from efforts to fight digital piracy, such as website blocking. The exemption does "not affect the possibility for a court or administrative authority … of requiring the service provider to terminate or prevent an infringement," in particular, an injunction that orders the "disabling of access to [illegal information]."[90]

The European Union allows each member country's courts to order ISPs to fight online copyright infringement, including through court orders for website blocking. In 2011, the European Court of Justice decided on a case that established the legal basis allowing national courts to order ISPs whose services are being used by a third party for copyright infringement "to take measures aimed not only at bringing to an end to infringements already committed against intellectual property rights using their information society services, but also at preventing further infringement."[91]

DNS and IP blocking are legitimate website-blocking options in the European Union.[92] However, URL blocking is likely to be problematic, as it requires the examination of all data packets to see if they are part of a request to a blocked URL and therefore could be considered a "general monitoring" obligation on ISPs, which the Court of Justice of the European Union has expressly forbidden (as it contravenes the EU E-Commerce Directive). For example, in a case involving peer-to-peer networks, the European Court of Justice held that an injunction that requires an ISP to install a filtering system that would "actively monitor all the data relating to each of its customers" would amount to general monitoring, and therefore be in breach of the E-Commerce Directive. [93]

APPENDIX E: WEBSITE BLOCKING IN THE UNITED STATES

Website blocking has a checkered history in the United States. In 2011, two pieces of legislation were introduced in Congress that contained provisions that would allow the Attorney General to apply for website-blocking injunctions. The Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 (known as PIPA or Protect IP Act) was introduced in the Senate in May 2011, but never progressed. The Stop Online Piracy Act (SOPA) was introduced in the House of Representatives in October 2011, but also did not progress.

While not technically blocking, the U.S. National Intellectual Property Rights Coordination Center is able to seize and destroy websites that are involved in copyright and trademark infringement.[94] The Prioritizing Resources and Organization for Intellectual Property Act of 2008 (PRO-IP Act) provides for civil forfeiture of property that is used to facilitate, or constitutes the proceeds of, certain intellectual property crimes, including copyright. Federal agents submit a sworn affidavit to a federal magistrate, and if the magistrate finds there is probable cause that the property is connected to the commission of criminal copyright infringement or trademark counterfeiting, the magistrate issues a seizure warrant, which the government uses to initiate forfeiture proceedings.[95] Users trying to access seized sites are redirected to a page showing a seizure notice.

This law forms the basis for "Operation in Our Sites," which is an ongoing law-enforcement effort to target piracy websites. Since it began in June 2010, it has seized thousands of domain names.[96] For example, on February 2, 2011, the U.S. Immigration and Customs Enforcement Agency used a federal court order to seize 10 websites that illegally streamed copyrighted sporting and pay-per-view events.[97] However, this power is limited to domains that use top-level domains of registries located in the U.S. (i.e. .com, .net, and .org).

A case before the courts may determine whether the United States International Trade Commission (USITC) can order the blocking of transmissions and websites that facilitate online copyright infringement. The USITC has the authority to investigate patent and copyright infringement complaints filed by U.S. companies and block the import of infringing goods. Past USITC cases have focused on physical goods, but a case currently before the USITC involving two companies—Clear Correct and Invisalign—looks at whether the agency can block the transmission of infringing digital goods (in this case 3D maps of patients' teeth). The question before the courts now is whether the USITC can block digital goods, in addition to physical goods, from being imported into the United States. If the courts decide that the USITC can order the blocking of this material, then it potentially could be used to order the blocking of digital piracy in other areas.

ENDNOTES

1. Brett Danaher, Michael D. Smith, and Rahul Telang, "Website Blocking Revisited: The Effect of the UK November 2014 Blocks on Consumer Behavior" (paper, Carnegie Mellon University, Pittsburg, April 18, 2016), http://ssrn.com/abstract=2766795http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2766795.
2. "PROTECT IP/SOPA Breaks the Internet," Fight for the Future website, accessed August 8, 2016, https://www.fightforthefuture.org/pipa/.
3. Todd Cunningham, "How Hollywood Is Using the Streaming Boom to Beat Back Digital Pirates," *The Wrap,* January 27, 2016, http://www.thewrap.com/how-hollywood-is-using-the-streaming-boom-to-beat-back-digital-pirates/.
4. Michael Ho, Joyce Hung, and Michael Masnick, "The Carrot or the Stick" (The Copia Institute, October 2015), https://copia.is/wp-content/uploads/2015/10/COPIA-The-Carrot-Or-The-Stick.pdf.
5. David Price, "Sizing the Piracy Universe" (industry report, Netnames, London, September 2013), https://www.netnames.com/assets/shared/whitepaper/pdf/netnames-sizing-piracy-universe-FULLreport-sept2013.pdf.
6. Ernesto Van der Sar, "Streaming Sites Dominate Movie and TV-Show Piracy," *TorrentFreak*, July 27, 2016, https://torrentfreak.com/streaming-sites-dominate-movie-and-tv-show-piracy-160727/.
7. The final sample of 26 published articles and 18 working papers yields 71 general conclusions about piracy's effect on sales (some studies analyzed more than one type of good, or considered different samples) and 426 estimates that could be studied through a meta-regression. While a majority of the studies concerns the United States, the 44 analyzed research papers comprise studies for Australia, Canada, China, France, Germany, Japan, and Sweden, along with several cross-country studies. The meta-analysis finds that 54 percent of papers examining the film industry and 60 percent of papers examining the music industry have a clear, statistically significant, negative impact on profits for content creators in this sector. See page 5 of Hardy et al. to get a detailed breakdown of the papers included in the meta-regression and why they were chosen. Wojciech Hardy, Michal Krawczyk, and Joanna Tyrowicz, "Friends or Foes? A Meta-Analysis of the Link Between "Online Piracy" and Sales of Cultural Goods" (working paper no. 23/2015 (171), University of Warsaw, Warsaw, 2015), http://www.wne.uw.edu.pl/files/9214/3741/1680/WNE_WP171.pdf; Adams Nager, "The True Damages of Online Piracy? It's Hard to Measure," *Innovation Files*, August 31, 2015, http://www.innovationfiles.org/the-true-damages-of-online-piracy-its-hard-to-measure/.
8. Michael D. Smith and Rahul Telang, "Assessing the Academic Literature Regarding the Impact of Media Piracy on Sales" (paper, Carnegie Mellon University, Pittsburg, August 19, 2012), http://dx.doi.org/10.2139/ssrn.2132153.
9. Nathan Wajsman, Carolina Burgos, and Christopher Davies, "The Economic Cost of IPR Infringement in the Recorded Music Industry" (Alicante, Spain: European Union Intellectual Property Office, May 2016), https://euipo.europa.eu/ohimportal/en/web/observatory/ipr_infringement_music.
10. Ibid.
11. Ernesto Van der Sar, "Pirate Bay Admins Charged with Assisting Copyright Infringement," *Torrent Freak*, January 31, 2008, https://torrentfreak.com/pirate-bay-team-charged-080131/.
12. "Criminal Complaint United States of America vs. Artem Vaulin," AO 91, (Rev. 11/11) Criminal Complaint, U.S. Department of Justice, accessed August 6, 2016, https://www.justice.gov/usao-ndil/file/877591/download.
13. "Good Money Still Going Bad: Digital Thieves and the Hijacking of the Online Ad Business" (Digital Citizens Alliance, May 2015), http://illusionofmore.com/wp-content/uploads/2015/05/latest-DigitalCitizensAlliance5.pdf.
14. "The Revenue Sources for Websites Making Available Copyright Content Without Consent in the EU" (Incopro, March 2015), http://www.incopro.co.uk/wp-content/uploads/2015/05/Revenue-Sources-for-Copyright-Infringing-Sites-in-EU-March-2015.pdf.
15. Frank la Rue, "Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression" (Geneva: United Nations Human Rights Council A/HRC/17/27, May 16, 2011), http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf; Josh Taylor, "Three Strikes Doesn't Deter Copyright Infringement," *ZDNet*, September 10, 2013, http://www.zdnet.com/article/three-strikes-doesnt-deter-copyright-infringement/.
16. David Corwin, "Contributory Copyright Liability in Napster versus Grokster: A Distinction Without a Difference," Loyola of Los Angeles Entertainment Law Review, 605, (2004), http://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=1479&context=elr.

17. "Release for Victim Notification: United States vs. Kim Dotcom, et al," The United States Attorney's Office, Eastern District of Virginia, accessed July 18, 2016, https://www.justice.gov/usao-edva/release-victim-notification; "Owner of Most-Visited Illegal File-Sharing Website Charged with Criminal Copyright Infringement," The United States Attorney's Office, Eastern District of Virginia, July 20, 2016, https://www.justice.gov/usao-ndil/pr/owner-most-visited-illegal-file-sharing-website-charged-criminal-copyright-infringement.
18. "Anti-Piracy Program FAQ," tag: Trustworthy Accountability Group, accessed July 4, 2016, https://tagtoday.net/piracyfaq/.
19. Daniel Castro and Nigel Cory, "Industry Cooperation Takes Another Step in Fighting Online Piracy," *The Hill*, March 3, 2016, http://64.147.104.30/blogs/pundits-blog/technology/271587-industry-cooperation-takes-another-step-in-fighting-online.
20. "What Is a Copyright Alert?" Center for Copyright Information, accessed June 14, 2016, http://www.copyrightinformation.org/the-copyright-alert-system/what-is-a-copyright-alert/.
21. Lukas Feiler, "Website Blocking Injunctions under EU and US Copyright Law: Slow Death of the Global Internet or Emergence of the Rule of National Copyright Law" (working paper no. 13, Transatlantic Technology Law Forum (TTLF), Stanford University Law School and University of Vienna School of Law, 2012), http://law.stanford.edu/wp-content/uploads/sites/default/files/publication/203758/doc/slspublic/feiler_wp13.pdf.
22. Ibid.
23. Ofcom, "'Site Blocking' to Reduce Online Copyright Infringement: A Review of Sections 17 and 18 of the Digital Economy Act" (London: Ofcom, May 27, 2010), http://stakeholders.ofcom.org.uk/binaries/internet/site-blocking.pdf.
24. Benjamin Edelman, "Web Sites Sharing IP Addresses: Prevalence and Significance," Berkman Center for Internet and Society, Harvard Law School, last modified September 12, 2003, https://cyber.law.harvard.edu/archived_content/people/edelman/ip-sharing/.
25. Ofcom, "Site Blocking."
26. Internet Society, "Internet Society Perspectives on Domain Name System (DNS) Filtering" (Internet Society, May 30, 2012), 202, http://www.internetsociety.org/internet-society-perspectives-domain-name-system-dns-filtering-0; Steve Crocker et al., "Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill" (technical white paper, May 2011), https://stupid.domain.name/files/2011/05/PROTECT-IP-Technical-Whitepaper-Final.pdf.
27. Paul Vixie, "DNS Changer," *Circle ID*, March 27, 2012, http://www.circleid.com/posts/20120327_dns_changer/; U.S. Attorney's Office, Federal Bureau of Investigations, "Manhattan U.S. Attorney Charges Seven Individuals for Engineering Sophisticated Internet Fraud Scheme That Infected Millions of Computers Worldwide and Manipulated Internet Advertising Business," new release, November 9, 2011, https://archives.fbi.gov/archives/newyork/press-releases/2011/manhattan-u.s.-attorney-charges-seven-individuals-for-engineering-sophisticated-internet-fraud-scheme-that-infected-millions-of-computers-worldwide-and-manipulated-internet-advertising-business.
28. Hal Roberts et al., "2010 Circumvention Tool Usage Report" (report, The Berkman Center for Internet & Society, Harvard Law School, Cambridge, MA, October 2011), https://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/2010_Circumvention_Tool_Usage_Report.pdf.
29. Ofcom, "Site Blocking."
30. Feiler, "Website Blocking Injunctions Copyright Law."
31. Fujitsu, "Technical Report: Carrier Software Defined Networking" (technical report for Ofcom, Fujitsu, Tokyo, March 2014), http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/SDN_Report.pdf.
32. For example, Arthur Little and Bell Labs estimate operating expense savings of 30 to 50 percent. Arthur D. Little, "Reshaping the Future with NFV and SDN" (report, Bell Labs, Murray Hill, NJ, May 2015), 9, http://www.adlittle.com/downloads/tx_adlreports/ADL_BellLabs_2015_Reshapingthefuture.pdf.
33. Sean Michael Kerner, "AT&T to Virtualize 75 Percent of Its Network by 2020," *Enterprise Networking Planet*, March 15, 2016, http://www.enterprisenetworkingplanet.com/netsp/att-pledges-to-virtualize-75-percent-of-its-network-by-2020.html.
34. "Data Plane Performance: A Key Enabler of SDN," 6Wind, accessed August 11, 2016, http://www.6wind.com/software-defined-networking/6windgate-sdn/.

35. Ofcom, "Site Blocking."
36. "Cartier International AG and Others vs. British Sky Broadcasting Ltd and Others, [2014] EWHC 3354," England and Wales High Court Chancery Division, British and Irish Legal Information Institute, October 17, 2014, http://www.bailii.org/ew/cases/EWHC/Ch/2003/3354.html.
37. It is unclear whether this cost estimate is per ISP or for all ISPs in the United Kingdom. A cost breakdown is not possible as the application is confidential. Mark Jackson, "The Cost of Getting UK ISPs to Block a Website via Court Order," *ISPreview*, October 22, 2014, http://www.ispreview.co.uk/index.php/2014/10/cost-getting-uk-isps-block-website-via-court-order.html.
38. Mark Sweney, "BT Ordered to Block Newzbin2 Filesharing Site Within 14 Days," *The Guardian*, October 26, 2011, https://www.theguardian.com/technology/2011/oct/26/bt-block-newzbin2-filesharing-site.
39. Copyright Amendment (Online Infringement) Bill 2015, Parliament of Australia, (2015), http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr5446_ems_1599ec23-c036-4dee-9562-a8a2e4d3d6fe%22.
40. Corinne Reichert, "Telcos Argue Costs of Compliance and Workarounds Process in Piracy Website Blocking," *ZDNet*, June 24, 2016, http://www.zdnet.com/article/telcos-argue-costs-of-compliance-and-process-for-workarounds-in-piracy-website-blocking/.
41. Claire Reilly, "AFP Using Site Blocking Laws to Target Malware," *CNET*, October 22, 2014, http://www.cnet.com/au/news/afp-using-site-blocking-laws-to-target-malware/.
42. Josh Taylor, "FOI Reveals ASIC's IP-Blocking Requests," *ZDNet*, July 1, 2013, http://www.zdnet.com/article/foi-reveals-asics-ip-blocking-requests/.
43. "Approach to Regulating Content on the Internet," Media Development Authority Singapore, August 11, 2016, http://www.mda.gov.sg/RegulationsAndLicensing/ContentStandardsAndClassification/Pages/Internet.aspx.
44. "Banned: Complete List of 857 Porn Websites Blocked in India," *Deccan Chronicle*, updated January 10, 2016, http://www.deccanchronicle.com/150803/nation-current-affairs/article/porn-ban-complete-list-857-porn-websites-blocked-india.
45. "174 Escort Services Websites to Be Blocked: State to Bombay High Court," *dna India*, April 21, 2016, http://www.dnaindia.com/mumbai/report-174-escort-services-website-to-be-blocked-state-to-bombay-high-court-2204387.
46. For example, in 2015, France introduced a law that allows government agencies to order the blocking of websites that advocate acts of terrorism or contain images of child abuse. The legislation was brought in by revisions to the Loppsi Act, and an anti-terror bill passed by the French senate in 2914, but can now be used by the general directorate of the French police's cybercrime unit to force French internet service providers to block sites within 24 hours, without a court order. In the United Kingdom the government and ISPs have agreed to implement a system of blocks, similar to that used to keep child abuse material off the internet, for websites espousing terrorism related extremist views. Samuel Gibbs, "French law blocking terrorist and child abuse sites comes into effect," *The Guardian*, February 9, 2015, https://www.theguardian.com/technology/2015/feb/09/french-law-blocking-terrorist-and-child-abuse-sites-comes-into-effect. the United Kingdom.
47. "Access Blocking," INTERPOL, accessed August 11, 2016, http://www.interpol.int/Crime-areas/Crimes-against-children/Access-blocking/The-INTERPOL-%22Worst-of%22-list.
48. Andy, "MPA Reveals 500+ Instances of Pirate Site Blocking in Europe," *Torrent Freak*, September 18, 2015, https://torrentfreak.com/mpa-reveals-500-instances-of-pirate-site-blocking-in-europe-150918/
49. Andy, "Portugal Blocks 330 Pirate Sites in Just Six Months," *Torrent Freak*, April 30, 2016, https://torrentfreak.com/portugal-blocks-330-pirate-sites-in-just-six-months-160430/.
50. "List of Court Orders," Virgin Media, accessed August 3, 2016, http://www.virginmediabusiness.co.uk/help/s/article/List-of-Court-Orders. This is an indicative list of court orders that require Virgin media, one of the UK's major ISPs, to block websites.
51. "Access Restricted to Certain File Sharing Websites," TalkTalk, accessed August 11, 2016, http://help2.talktalk.co.uk/access-restricted-certain-file-sharing-websites.
52. Josh Halliday, "British ISPs Will Block The Pirate Bay Within Weeks," *The Guardian*, April 30, 2012, https://www.theguardian.com/technology/2012/apr/30/british-isps-block-pirate-bay.

53. Brett Danaher, Michael D. Smith, and Rahul Telang, "The Effect of Piracy Website Blocking on Consumer Behavior" (research paper, Carnegie Mellon University's Initiative for Digital Entertainment Analytics, Pittsburg, November 2015), http://dx.doi.org/10.2139/ssrn.2612063.
54. There were actually 21 sites blocked, but the study excluded piracy sites which were solely focused on providing access to music.
55. Danaher, Smith, and Telang, "Effect of Piracy Website Blocking."
56. Danaher, Smith, and Telang, "Website Blocking Revisited."
57. Mark Sweney, "Record Labels Win ISP Blocks on 21 Filesharing Sites," *The Guardian*, October 29, 2013, https://www.theguardian.com/business/2013/oct/29/record-labels-isp-piracy-block-music-filesharing.
58. "Facts and Figures," Ofcom, accessed August 11, 2016, http://media.ofcom.org.uk/facts/.
59. The result was not 100 percent as some ISPs may have delayed enacting the blocks (into December), usage of virtual private networks to circumvent the blocks, and the order does not target some of the smaller ISPs.
60. The causal change in total piracy was computed differently. The study assumes that the drop was a result of the blocks. Noting that the regression showed no causal increase in usage of unblocked piracy sites, the study calculated for each segment the total piracy before the blocks and assumed in the post-block period that, if nothing else changed except for the blocks, it would have been the same number less 90 percent, based on the study results. From this, the study calculated the causal change in piracy in each segment.
61. The analysis of the results for access to ad-support and subscription video services was based on an analysis of coefficients from a regression analysis and showed that the estimate for the change in access to ad-supported video site was measured with 95 percent confidence, while the estimate for access to subscription services was measured with 75 percent confidence.
62. The study into the website blocks of 2013 did not have data on visits to ad-supported legal content sites.
63. Daniel Castro, "A Declaration of the Interdependence of Cyberspace," *Computerworld*, February 8, 2013, http://www.computerworld.com/article/2494710/internet/a-declaration-of-the-interdependence-of-cyberspace.html.
64. Rob Atkinson, "The Internet Is Not (Fully) Open, Nor Should It Be," *Innovation Files*, August 13, 2015, http://www.innovationfiles.org/the-internet-is-not-fully-open-nor-should-it-be/.
65. Richard Esguerra, "Censorship of the Internet Takes Center Stage in 'Online Infringement' Bill," *Electronic Frontier Foundation*, September 21, 2010, https://www.eff.org/deeplinks/2010/09/censorship-internet-takes-center-stage-online; Kathryn Kleiman, "Letter to Senate Judiciary Committee," Electronic Frontier Foundation website, November 15, 2010, https://www.eff.org/files/filenode/coica_files/coica_blocking_breaks_dnssec_-_.org_memo.pdf.
66. Richard Bennett, "DNS Integrity in the Real World," *Innovation Files*, March 30, 2012, http://www.innovationfiles.org/dns-integrity-in-the-real-world/.
67. Digital Citizens Alliance, "Enabling Malware: How U.S.-Based Firms are Enabling Malware Peddlers to Bait Consumers and Steal Their Personal Information" (Digital Citizens Alliance, July 2016), https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/0057c1cf-28f6-406d-9cab-03ad60fb50e4.pdf.
68. Daniel Castro, "PIPA/SOPA: Responding to Critics and Finding a Path Forward" (Information Technology and Innovation Foundation, December 2011), http://www.itif.org/files/2011-pipa-sopa-respond-critics.pdf.
69. Martin Husovec, "Injunctions Against Innocent Third Parties: Case of Website Blocking" (Max Planck Institute for Intellectual Property and Competition, April 27, 2013), http://dx.doi.org/10.2139/ssrn.2257232.
70. Cate Nagy and Anna Spies, "Website-Blocking Injunctions to Combat the Increasing Risk of Online Copyright Infringement," King & Wood Mallesons, January 13, 2016, http://www.kwm.com/en/knowledge/insights/website-blocking-injunctions-to-combat-the-increasing-risk-of-online-copyright-infringement-20151109.
71. Brett Danaher, Michael Smith, and Rahul Telang, "Copyright Enforcement in the Digital Age: Empirical Economic Evidence and Conclusions" (report, Advisory Committee on Enforcement, World Intellectual Property Organization, Geneva, November 23–25, 2015), http://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_10/wipo_ace_10_20.pdf.
72. Ibid.
73. Ibid.

74. Clifford J. Levy, "Russia Uses Microsoft to Suppress Dissent," *The New York Times*, September 11, 2010, http://www.nytimes.com/2010/09/12/world/europe/12raids.html.
75. Ofcom, "Site Blocking."; Ron Moscona, "Website Blocking Orders - A New Tool in the Fight Against Online Trade in Counterfeit Goods," *Dorsey,* October 24, 2014, https://www.dorsey.com/newsresources/publications/2014/10/website-blocking-orders--a-new-tool-in-the-fight__.
76. Nagy and Spies, "Website-Blocking Injunctions."
77. Ibid.
78. Maryant Fernández Pérez, "Portugal: 'Voluntary' Agreement Against Copyright Infringements," *EDRi,* August 12, 2015, https://edri.org/portugal-voluntary-agreement-against-copyright-infringements/.
79. In October 2011, a court in the United Kingdom ordered a major ISP, BP (which has an estimated 6 million customers), to block access to NewzBin2 as it was facilitating widespread copyright infringement. Given the easy ability for the owner to shift their services to other domain names, the judge also ordered BP to block any other IP that NewzBin2. In November 2012, the NewzBin2 shutdown.
80. "High Court Orders UK's Major Internet Service Providers to Block Access to 'Popcorn Time" Website," *Charles Russell Speechleys*, May 6, 2015, http://www.charlesrussellspeechlys.com/insights/latest-insights/tmt-new/high-court-orders-uk-s-major-internet-service-providers-to-block-access-to-popcorn-time-websites/.
81. Nagy and Spies, "Website-Blocking Injunctions."
82. "Cartier vs. British Sky Broadcasting Ltd."
83. Moscona, "Website Blocking Orders."
84. Audrey Horton, "IP & IT Bytes: Copyright: Website-Blocking Order Against Internet Service Providers," *Bird & Bird,* June 4, 2015, http://www.twobirds.com/en/news/articles/2015/global/ip-and-it-law-bytes-june/copyright-website-blocking-order-against-internet-service-providers.
85. Ibid.
86. Copyright Amendment (Online Infringement) Bill 2015.
87. Nagy and Spies, "Website-Blocking Injunctions."
88. Corrine Reichert, "Telstra Argues Against Compliance Costs for piracy website blocking," *ZDnet,* May 6, 2016, http://www.zdnet.com/article/telstra-argues-against-compliance-costs-for-piracy-website-blocking/.
89. Ibid.
90. "Directive on Electronic Commerce," EUR-Lex website, accessed August 12, 2016, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32000L0031.
91. Feiler, "Website Blocking Injunctions."
92. "Directive on Electronic Commerce."
93. Court of Justice of the European Union, "EU Law Precludes the Imposition of an Injunction by a National Court Which Requires an Internet Service Provider to Install a Filtering System with a View to Preventing the Illegal Downloading of Files," news release, November 24, 2011, http://curia.europa.eu/jcms/upload/docs/application/pdf/2011-11/cp110126en.pdf.
94. Ann Chaitovitz et al., "Responding to Online Piracy: Mapping the Legal and Policy Boundaries," *CommLaw Conspectus 20*, (2011): 1, http://scholarship.law.edu/cgi/viewcontent.cgi?article=1478&context=commlaw.
95. Karen Kopel, "Operation Seizing Our Sites: How the Federal Government Is Taking Domain Names Without Prior Notice," *Berkeley Technology Law Journal 28*, (2013): 859.
96. U.S. Immigration and Customs Enforcement, "ICE, CBS, USPIS Seize More Than 136 Million Fake NFL Merchandise During Operation Red Zone," news release, January 31, 2013, https://www.ice.gov/news/releases/ice-cbp-uspis-seize-more-136-million-fake-nfl-merchandise-during-operation-red-zone.
97. U.S. Immigration and Customs Enforcement, "New York Investigators Seize 10 Websites that Illegally Streamed Copyrighted Sporting and Pay-Per-View Events," news release, February 2, 2011, https://www.ice.gov/news/releases/new-york-investigators-seize-10-websites-illegally-streamed-copyrighted-sporting-and.

ACKNOWLEDGMENTS

The author wishes to thank the following individuals for providing input to this report: Robert Atkinson, president, ITIF; Daniel Castro, vice president, ITIF; Doug Brake, telecommunications policy analyst, ITIF; and Stephen Ezell, vice president, ITIF. Any errors or omissions are the author's alone.

ABOUT THE AUTHOR

Nigel Cory is a trade policy analyst at ITIF. He previously worked as a researcher at the Sumitro Chair for Southeast Asia Studies at the Center for Strategic and International Studies. Prior to that, he worked for eight years in Australia's Department of Foreign Affairs and Trade and also had diplomatic postings to Malaysia and Afghanistan. Cory holds a master's degree in public policy from Georgetown University and a bachelor's degree in international business and commerce from Griffith University in Brisbane, Australia.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized as one of the world's leading science and technology think tanks, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

FOR MORE INFORMATION, VISIT US AT WWW.ITIF.ORG.