

How Voluntary Agreements Among Key Stakeholders Help Combat Digital Piracy

NIGEL CORY | FEBRUARY 2020

Working together, firms from different parts of the digital economy can disrupt the supply side of the digital piracy equation to make it harder and costlier for illicit operators to function.

KEY TAKEAWAYS

- There is no single, easy solution to the scourge of digital piracy. But voluntary agreements between copyright holders and payment processors, advertising networks, domain name registrars, search engines, and others can and should play a key role.
- These voluntary agreements target key facilitating services and processes that enable piracy sites to profit from facilitating access to illegal content as if they were legitimate businesses—which they most definitely are not.
- Digital-piracy-focused voluntary agreements are increasingly common around the world. They differ by country and issue, but empirical evidence shows they can meaningfully effect consumer behavior, reduce piracy, and increase legal sales.
- The United States, Europe, and others should support further research and discussion of how voluntary agreements can be a standard part of every country's digital piracy toolkit.
- Governments should proactively encourage more voluntary agreements alongside other anti-piracy policies as part of a reinvigorated, pragmatic discussion about best practices to support IP in the global digital economy.

INTRODUCTION

Voluntary agreements between copyright holders and payment processors, advertising networks, domain name registrars, search engines, and others can complement legislative and other efforts to protect creators' digital intellectual property (IP) from the significant negative impact of piracy. Experience from the United States, Europe, and elsewhere shows how firms from different parts of the digital economy can work together both to support the marketplace for legal content and to reduce the availability of illegal content. There is no easy, single solution to address the scourge of illegal digital piracy, but voluntary agreements can and should play a key role.

Digital-piracy-focused voluntary agreements are increasingly common around the world. They differ by country and issue, but all share the common focus on groups of firms coming together to reduce digital piracy—a goal all responsible stakeholders should share. The empirical evidence shows these types of firm and government interventions can have a meaningful effect on consumer behavior, while also reducing piracy and increasing legal sales.¹ These voluntary agreements don't directly address IP rights enforcement online (such as getting web pages containing infringing material blocked or removed), but rather target key facilitating services and processes that otherwise enable large-scale, commercially driven piracy sites to function as if they were legitimate businesses—which they most definitely are not.

In this way, voluntary agreements target supply-side factors that make life harder and costlier for piracy operators that otherwise would be left unimpeded to profit from facilitating access to illegal content. It should be in the interest of all actors interested in an innovative and prosperous digital economy to have measures in place to stop their goods and services from being used to monetize illegal actions. At the heart of these efforts is the collective recognition by all players that digital piracy services are a social and economic harm to the broader creative and digital economy on which they all rely, and they'd all be better off working to make it harder—if not impossible—for them to function.

Despite what some might claim, digital content piracy remains a significant threat to creative individuals and firms that depend on copyright protection. The point should be obvious that enabling free (and illegal) consumption would cut into paid (and legal) consumption. Yet some need evidence. A 2017 scholarly study on copyright enforcement analyzed 26 peer-reviewed journal articles studying the economic harm caused by piracy, and found that 23 of them concluded piracy causes significant harm to legal sales.² The report quotes Joel Waldfoegel of the University of Minnesota, who observed at a 2015 meeting of the World Intellectual Property Organization (WIPO), “[T]he dust has settled in that literature... and most people believe that, indeed, unpaid consumption reduces the ability of sellers to generate revenues.”³ The director general of WIPO agreed:

What is clear [in regard to digital piracy], however, is that the impact of illegal downloading is significant and negative.... By dint of technology, we already have a seamless global digital marketplace, but it is an illegal one.⁴

The world's leading creative countries still have a long way to go before they can say they've significantly reduced digital piracy, but many are finally taking steps in the right direction toward this goal. In some instances, governments act as an honest broker to facilitate collaboration between the various stakeholders—whether rightsholders or Internet platforms—by suggesting

that if they don't come to mutually acceptable agreements to curb piracy, legislation could follow, which may be in a form more prescriptive and onerous than some would otherwise prefer.

Various stakeholders in the digital economy often face a choice: do an effective job regulating themselves as part of a collective effort toward achieving a shared goal, or face government regulation. This is a decision many firms and policymakers are now debating across a range of digital economy issues, including digital piracy. If companies work well voluntarily, the pressure to introduce legislation to impose mandatory measures will recede. Voluntary agreements can influence public policymakers' perceptions, as they can be seen (as they should be) as a good-faith effort to address a pressing issue. Voluntary agreements can also set industry best practices that can become norms, in part, as they differentiate firms and stakeholders working together toward a common, mutually shared goal with those not taking part in these efforts.

Digital piracy services are a social and economic harm to the broader creative and digital economy on which they rely. All players would be better off working to make it harder—if not impossible—for them to function.

Many stakeholders also realize voluntary agreements are, as they need to be, more adaptable than legislation, given the many different stakeholders and business models involved, both of which will inevitably change with technology. Likewise, for policymakers interested in pragmatic options to improve their digital economies, voluntary agreements are attractive, as legislative procedures take a lot more time and ultimately may not be best to address certain issues given the ever-changing nature of piracy. It may also be necessary for government to regulate in this space. But robust voluntary cooperative efforts can address many parts of the digital piracy problem.

This report provides an update regarding voluntary agreements around the world to highlight the role these initiatives play in reducing digital piracy. In this way, these existing agreements can act as a model for policymakers and firms in countries that have not yet sought to encourage this type of cooperation. Alternatively, these agreements could be adapted to work on digital piracy issues that do not yet have industry-based collaboration but would benefit from such a mechanism.

This report offers the following recommendations:

- Governments should support voluntary agreements as one of the policy tools they use to fight digital piracy.
- The United States, the EU and its member states, and other countries should support further research and discussion around how voluntary agreements should be a standard part of every country's digital piracy toolkit. As part of this, the Organization for Economic Cooperation and Development (OECD) should develop the core principles and processes necessary to create a template for voluntary agreements and include voluntary agreements as part of its standard digital economy policy recommendations.

- Australia, the EU, United Kingdom, United States, and others should actively encourage other countries to use voluntary agreements (which at the moment they don't), and other anti-piracy policies, as part of a holistic approach to protect and support the creation of legal content in their respective countries. Ultimately, this needs to be part of a broader, energized effort to support the development of a global digital economy based on legal (and not illegal) content.

VOLUNTARY AGREEMENTS IN THE UNITED STATES

The U.S. government has facilitated discussions between rightsholders and other players in the Internet ecosystem to establish voluntary agreements to address different aspects of digital piracy, including with regard to domain name registrations, payment processors, advertising, and others.⁵ During the Obama administration, the U.S. Department of Commerce's Internet Policy Taskforce encouraged stakeholders to take part in existing initiatives and develop new ones in other sectors.⁶ Building on this, the Trump administration is engaging and working with stakeholders as one component of its four-part strategic approach to IP enforcement.⁷ At the heart of this effort is the Intellectual Property Enforcement Coordinator.⁸ Most recently, the U.S. Department of Commerce has considered the role of voluntary agreements as part of an inquiry it is holding into counterfeit and pirated goods.⁹

This U.S. government's effort to support voluntary agreements complements key provisions of the 1998 Digital Millennium Copyright Act (DMCA). In the DMCA—a foundational law for the U.S. digital economy—Congress acknowledged the importance of voluntary agreements in addressing technological developments, conditioning Internet safe harbors on accommodating “standard technical measures” that have been “developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process.” The U.S. Congress recognized that “technology is likely to be the solution to many of the issues facing copyright owners and service providers in this digital age,” and “strongly urge[d] all of the affected parties expeditiously to commence voluntary, interindustry discussions to agree upon and implement the best technological solutions available to achieve these goals.”¹⁰ In other words, Congress premised the safe harbor provisions of the DMCA on an expectation Internet companies would work in good faith with other parties to actively limit digital piracy.

The following sections outline some—but not all—voluntary agreements used in the United States.

Cooperation to Prevent Piracy Operators From Abusing Domain Name Registries

Rightsholders and domain name registrars (organizations that create, manage, and sell top-level domain names) have set up or considered several voluntary agreements called “Trusted Notifier” programs. These agreements streamline how domain name registrars respond to notices from rightsholders about cases wherein large-scale piracy sites have registered domains they manage, which contravene the domain name registry operator's anti-abuse and acceptable-use guidelines.

On February 9, 2016, the Motion Picture Association of America (MPAA)—now known as the Motion Picture Association—announced the first of these with Donuts, the largest operator of new global top-level domain name (gTLDs) extensions such as .MOVIE, .THEATRE, .COMPANY, and over 200 other naming options.¹¹ In setting out the details for trusted notifier status, standards for referrals, and actions by the registry, the Donuts-MPAA agreement shows how

private-sector stakeholders can come together to address online piracy and create a win-win scenario for all partners.¹² For Donuts, the agreement protects its brand by ensuring its domains are legitimate and law-abiding contributors to the digital economy. For MPAA, the agreement provides a clear path toward the removal of infringing sites and material, albeit with the responsibility to fulfill several clearly defined and detailed steps it must make in presenting its case.

The president of the Internet Corporation for Assigned Names and Numbers (ICANN)—the private organization that governs the Internet’s domain name system—welcomed the agreement.¹³ Indeed, he should have, as ICANN’s lax enforcement of domain name abuses has long been a sore spot. As the Information Technology and Innovation Foundation (ITIF) outlined during a congressional hearing, ICANN has a history of poorly enforcing its policies, and has developed a pattern of putting its own interests ahead of those of the global Internet community, including not enforcing its own policies against domain name registrars that knowingly harbor or facilitate criminal activity.¹⁴

In the first year of the agreement, 12 domain names were submitted, of which 7 were suspended or deleted by the registrar, 3 were suspended by Donuts, and 1 was addressed by the hosting provider.¹⁵ In this review, countering the criticism leveled at the Trusted Notifier program from pro-piracy activists, Donuts noted:

There has been concern on the part of some in the industry about this type of arrangement—namely, that it represented a “slippery slope” toward inappropriate content control, or that hundreds of domain names would be snatched away from rightful registrants. To the contrary, however, and in line with the previously published characteristics of a trusted notifier program, a mere handful of names have been impacted, and only those that clearly were devoted to illegal activity. And to Donuts’ knowledge, in no case did the registrant contest the suspension or seek reinstatement of the domain.¹⁶

Following this, on May 13, 2016, MPAA announced a second trusted notifier agreement with Radix, another domain name registry operator, to ensure websites using domains operated by Radix are not engaged in large-scale commercial piracy.¹⁷ This is the first such agreement with an operator outside the United States. Radix has launched seven new domain extensions, including .online, .tech, .space, .website, .press, .host, and .site.¹⁸ The agreement imposes strict standards for rightsholder to use in their referrals, including that they be accompanied by evidence of clear and pervasive copyright infringement, and contain a representation that the MPAA has first attempted to contact the registrar and hosting provider for resolution.

These agreements between specific players in the domain name sector aim to proactively embed best practices in new domain name operators as an attempt to prevent piracy operators from misusing and profiting from new—and in some cases, existing—domain name operations. For example, on November 1, 2018, in its agreement with Verisign to operate the .com top-level domain, the U.S. National Telecommunication and Information Administration (NTIA) stated that it “looks forward to working with Verisign and other ICANN stakeholders in the coming year on trusted notifier programs to provide transparency and accountability in the .com top level domain.”¹⁹ Neustar Registry Services (which operates a number of TLDs, including .US, .CO,

.nyc, and .biz) informed NTIA that it had started discussions with industry groups about enacting a trusted notifier program.²⁰

The Domain Name Association (DNA), a nonprofit global business association comprising groups, businesses, and individuals involved in the provision, support, and sale of domain names is working to build on these agreements as part of a broader effort to improve registry operations as they relate to piracy. Building on the early surge in interest when new gTLDs were launched, DNA and its various partners undertook good-faith efforts to develop the Healthy Domains Initiative, which is a voluntary self-regulation scheme launched in early 2017 to tackle misuse and abuse of domain name registrations.²¹ The practices are grouped into four areas, including addressing online security abuse, complaint handling for “rogue” pharmacies, enhancing child abuse mitigation systems, and voluntary third-party handling of copyright infringement cases.²²

Agreements between specific players in the domain name sector aim to proactively embed best practices in new domain name operators as an attempt to prevent piracy operators from misusing and profiting from new—and in some cases, existing—domain name operations.

However, good-faith efforts to build on the early success of the Healthy Domains Initiative have slowed, due in part to the huge amounts of resources and attention domain name stakeholders have had to dedicate to the many problems caused by the European Union’s General Data Protection Regulation (GDPR) and its impact on ICANN’s WHOIS data (a public database with the names, phone numbers, email addresses, and mailing addresses of registered domain owners and operators).²³ Law enforcement, IP owners, tech firms, and security and academic researchers use the WHOIS database to contact and manage the various parties responsible for the websites that populate the Internet. However, since GDPR’s passage, some registrars have not been supplying this data to the database over concerns they may face potentially significant fines under GDPR.²⁴

It has also slowed due to misinformation and ideological opposition from the Electronic Frontier Foundation (EFF) and likeminded academics that see these efforts as akin to censorship, including when DNA launched—and then withdrew—an effort to target domain names involving illegal pharmacy operators that may not be licensed to operate in the United States or sell fake/unregulated medicines.²⁵

Cutting Off the Advertising Money Going to Digital Piracy Websites

Most public-facing piracy sites are motivated by money, much of which comes from advertising. This can involve ads from large, reputable brands that inadvertently have their ads placed on these piracy sites. There are a range of initiatives underway to cut off this source of funds.

Established in the United States in 2014, the Trustworthy Accountability Group (TAG) is a not-for-profit cross-industry (self-regulation) program for advertisers that aims to eliminate fraudulent digital advertising traffic, combat malware, fight ad-supported Internet piracy in order to promote brand integrity, and promote brand safety through greater transparency.²⁶ In 2015, the U.S. Interactive Advertising Bureau (IAB) estimated that fraudulent impressions, infringed content, and “malvertising” were costing digital marketers \$8.2 billion annually in the United States alone.²⁷ Companies (advertising and agencies) have the option to achieve the Certified Against Piracy Seal by operationalizing and demonstrating full compliance with the TAG Anti-Piracy

Pledge and abiding by the Certified Against Piracy Guidelines.²⁸ Google, Facebook, Disney, Warner, NBC Universal, and many other major companies are members. Major ad agencies—such as the world’s largest, WPP’s GroupM—have stipulated that their media partners either become TAG certified or use TAG-certified services.²⁹

TAG aims to cut off the money piracy sites earn from digital advertising. Research has documented that up to 86 percent of IP-infringing websites allow web users to download or stream infringing media content for free, with the websites earning money via online advertising.³⁰ A 2014 report by Digital Citizens’ Alliance and NetNames estimated that over 70 percent of video streaming hosting websites (also known as streaming “cyberlockers”) rely on ad revenue.³¹ The United States Trade Representative’s *Notorious Markets* report consistently highlights how online piracy sites around the world are funded by advertising revenue.³² An independent review of the top-5,000 IP-infringing web addresses in the United States, European Union, Latin America, and Australia estimated that about 13 percent of advertising on websites posing an IP risk are from major brands (including premium household names).³³ Ensuring piracy sites don’t benefit from these ads is becoming a major focus for voluntary agreements around the world.

TAG aims to cut off the money piracy sites earn from digital advertising. Research has documented that up to 86 percent of IP-infringing websites allow web users to download or stream infringing media content for free, with the websites earning money via online advertising.

A 2017 Ernst & Young study showed TAG had helped cut revenue to piracy sites by 48 to 61 percent in the United States, which amounts to an estimated \$102 million to \$177 million loss in potential earnings for piracy sites.³⁴ TAG also reduces fraudulent and malicious activity often associated with piracy sites. A separate December 2017 study found the use of TAG-certified distribution channels reduced fraud by more than 83 percent.³⁵ Most recently, a 2019 study by TAG and its partner Creative Futures estimated that TAG had directly reduced the presence of 76 major brands’ advertising on pirate sites, which led to a 90 percent reduction in (ad) impressions served on piracy sites over two years.³⁶ In 2016–2017, more than 60 brands or agencies each contributed large volumes of ads on pirate sites, with some premium brands generating between 5 million and 25 million impressions per month. By 2018, no premium advertisers could be identified at high volumes on pirate sites.

Cutting Off Piracy Websites From Payment Processing and Other Financial Services

In 2012, the International Anti-Counterfeiting Coalition (IACC), a Washington, D.C.-based nonprofit organization devoted solely to combating product counterfeiting and piracy, launched the RogueBlock initiative to provide a streamlined approach to targeting the online sale of counterfeit or pirated goods in the United States. The initiative was supported by (and continues to receive the support of) the U.S. Intellectual Property Enforcement Coordinator. IACC has over 250 members, including law firms, investigative and product security firms, government agencies, and IP associations. The four core goals of RogueBlock are to increase the cost of doing business for, and decrease profits to, the counterfeiters; shrink the universe of third-party acquiring banks willing to do business with rogue merchants; facilitate an efficient use of resources by both IP owners and partners by sharing relevant data and avoiding the duplication of efforts; and disrupt and dismantle counterfeit networks.³⁷

RogueBlock cuts off financial flows to piracy websites via “payment processor agreements,” which allow members to directly lodge a complaint regarding a counterfeiter or piracy operator.³⁸ Members use a secure process to lodge reports about infringements to IACC, which reviews them and then passes information about the infringement on to such affiliated payment processors as MasterCard, Visa International, Visa Europe, PayPal, MoneyGram, American Express, Discover, PULSE, Diners Club, and Western Union. The aim of this program is to disrupt the processes of counterfeit sellers by blocking their ability to take payments, thereby cutting off a key pathway for piracy operators.³⁹

RogueBlock is considered a success, as it is a win-win for all parties involved. Rightsholders are able to provide timely, relevant intelligence—and in the process aid payment providers in policing bad actors that seek to misuse legitimate commercial tools for illegitimate purposes.

RogueBlock is considered a success, as it is a win-win for all parties involved. Rightsholders are able to provide timely, relevant intelligence—and in the process aid payment providers in policing bad actors that seek to misuse legitimate commercial tools for illegitimate purposes.⁴⁰ To date, the program has terminated over 5,000 individual counterfeiters’ merchant accounts, which has impacted over 200,000 websites.⁴¹

VOLUNTARY AGREEMENTS IN EUROPE

The United Kingdom and the European Commission are leading users of voluntary agreements as part of broader efforts to fight digital piracy—the latter as part of efforts to support its goal for a Digital Single Market in the European Union.⁴²

Cutting Off the Advertising Money Going to Digital Piracy Websites

As part of its “follow-the-money” approach to IP enforcement, the European Commission developed a Memorandum of Understanding (MoU) on online advertising and IP rights (attachment A below). As former vice president of the European Commission Andrus Ansip stated at the signing, “MoUs are a key pillar in the work on the enforcement of IPRs.”⁴³ This represents a key development, as the enforcement of copyright online has stereotypically been characterized by a lack of shared approaches between countries at the European Union level.

The European Union is starting to use specific voluntary agreements to limit advertising on piracy websites and mobile applications that infringe copyrights or disseminate counterfeit goods, including by integrating parts of TAG’s European operations into these agreements. On June 25, 2018, TAG, White Bullet, and many European trade bodies signed the European Commission’s Memorandum of Understanding on Online Advertising and IPR.⁴⁴ As part of this, TAG offers a Certified Against Piracy Program through which companies can demonstrate they adhere to the requirements of the MoU.

Specific voluntary agreements are operationalizing this broader framework to address different parts of the digital piracy ecosystem in Europe.

The Trustworthy Accountability Group

On the heels of its success in the United States, TAG has set up and expanded operations in Europe, where the same issues and goals exist, and many of the same stakeholders in the United

States also operate. For example, more than 130 non-U.S. companies from 27 countries have applied for TAG registration. In early 2018, TAG announced an agreement with the United Kingdom's leading standards body and opened an office in London to help expand its operations in Europe.⁴⁵ On February 12, 2019, TAG launched Project Brand Integrity in Europe to help advertisers and their agencies avoid brand risk and damage by monitoring pirate sites and alerting them to the placement of their ads on those sites.⁴⁶ White Bullet, a "Digital Advertising Assurance Provider" under the TAG Certified Against Piracy Program, scans the top ad-supported, infringing sites serving European markets in order to identify ads from reputable brands appearing on such sites. When a brand has ad exposure on infringing sites, White Bullet notifies TAG, which then contacts the advertiser or its advertising agency to alert them to the ad misplacements, so they can then take remedial action.

Infringing Website Lists

The United Kingdom has set up a process to identify and update a central infringing website list (IWL) to help reputable brands and advertising agencies avoid placing ads on piracy sites. The central goal of these systems is to ensure reputable advertisers don't inadvertently provide financial support for piracy sites by placing ads on their sites—which might otherwise happen as ads are often automatically placed by software without direct human intervention.

Initially developed in 2013, Operation Creative is a voluntary arrangement set up by the United Kingdom between the City of London Police Intellectual Property Crime Unit (PIPCU) and various advertising and rightsholder stakeholders to identify websites engaged in copyright infringement and take remedial measures targeting them.⁴⁷ PIPCU is funded by the United Kingdom's Intellectual Property Office.⁴⁸ As part of this, rightsholders identify and report copyright-infringing websites to PIPCU, which then evaluates and verifies the websites are infringing copyrights. PIPCU then contacts the site owners in an attempt to give them the opportunity to engage with the police and remove the content. If the website fails to engage and comply with the police, then PIPCU moves to remedial measures, such as contacting the domain registrar to seek suspension of the site, or cutting off advertising revenue by adding it to the IWL.

The United Kingdom has set up a process to identify and update a central infringing website list (IWL) to help reputable brands and advertising agencies avoid placing ads on piracy sites. The central goal of these systems is to ensure reputable advertisers don't inadvertently provide financial support for piracy sites.

PIPCU's IWL is the first of its kind in that it represents an online portal containing an up-to-date list of the key copyright-infringing sites, identified and evidenced by the creative industries and verified by PIPCU. Indicative of the need for these types of initiatives, the head of PIPCU estimated that a single website owner involved in large-scale piracy can make as much as \$84,200 a year from advertising.⁴⁹ Operation Creative supports broader follow-the-money efforts in that it is available to all agencies involved in the sale and trade of digital advertising, with the goal of allowing them to voluntarily cease the placement of ads on these piracy websites.

The program has been successful. A March 2017 report documented a 64 percent decrease in advertising from the United Kingdom's top ad-spending companies on copyright-infringing websites (comparing 205 websites on the IWL in both January 2016 and January 2017).⁵⁰

Furthermore, another study from White Bullet in June 2017 showed an 87 percent drop in advertising from licensed gambling operators on illegal sites that infringe copyright laws (as compared with the previous year).⁵¹

Elsewhere in Europe, Denmark set up an IWL based on websites determined by Danish courts to be facilitating copyright infringement. The Danish government helped facilitate a memorandum of understanding (MoU)/code of conduct between the various Internet stakeholders so Internet service providers (ISPs) can block access to, and advertisers don't show ads on, these sites.⁵² Other countries, including Italy, Germany, and Spain, have announced their own initiatives to tackle suspected ad-funded IP infringement.⁵³

Cutting Off Piracy Websites From Payment Processes and Financial Services

RogueBlock's success in the United States has led to its expansion to Europe. In April 2017, IACC and the City of London Police announced a collaboration to target counterfeiting through the RogueBlock initiative. The program expands RogueBlock to encompass the .uk domain wherein the British authority processes complaints.⁵⁴ The collaboration is part of PIPCU's Operation Ashiko, which aims to tackle the online trade in counterfeit goods and protect the integrity of the U.K. domain tree by suspending websites committing IP crimes. The initiative supports PIPCU's IP enforcement objectives by providing a streamlined source of counterfeit websites that are identified by rightsholders and that includes all the information required to take action against them. Since its inception, Operation Ashiko has suspended in excess of 20,000 websites by working with industry partners.⁵⁵

Additionally, in June 2018, the EU announced a similar collaboration between the European registry for Internet Domains and IACC. This collaboration namely exists to address cybercrime in the .eu (and other) domains, especially as a means to target counterfeiting.⁵⁶ As of yet, according to IACC, the international program has resulted in the termination of over 5,000 distinct counterfeit sellers' accounts, and has involved over 200,000 websites.⁵⁷

United Kingdom: De-indexing Piracy Sites in Search Results

An ongoing problem in fighting digital piracy is piracy sites often feature among many of the top search-engine results, even when there are many legal service providers. Many countries are looking at using voluntary agreements between search engines and the creative-content sector to ensure piracy sites are removed from results or "demoted" in that they do not feature on the first (or first few) search results pages. Research has shown demoting search results that link to piracy websites can shift user behavior toward legal consumption, which highlights that search engines are useful partners to reduce piracy's impact.⁵⁸

In 2017, the United Kingdom's Intellectual Property Office brokered a voluntary code of practice between representatives from the creative industries and leading search engines, including Google and Bing, to both remove links to infringing content from the first page of search results and make sure piracy search terms do not show up in autocomplete suggestions.⁵⁹ The agreement went into effect on February 9, 2017, and set targets for reducing the visibility of infringing content in search results by June 1, 2017. At the heart of the code of practice is a process for testing whether search engines have met "targets for reducing the visibility of infringing content in search results." Google has passed at least four rounds of tests.⁶⁰

The code of practice is part of the United Kingdom's broader strategy to fight digital piracy and support its creative sector. It follows a 2013 Ofcom study (funded by the Intellectual Property Office of the United Kingdom) that estimated one in four downloads in the United Kingdom were pirated.⁶¹ The U.K. "IPO Strategy 2018 to 2021" report outlined its aim to "broker greater engagement from online intermediaries in the fight against infringement and IP crime."⁶² This follows a Creative Industries Industrial Strategy that outlined plans to host a series of roundtables with copyright holders, social media companies, platforms that host user-generated content, digital advertising firms, and online marketplaces to explore other potential areas of cooperation.⁶³ The U.K. government outlined to all stakeholders that it would consider legislative solutions to these issues if sufficient voluntary progress were not made in a reasonable timeframe.

Many countries are looking at using voluntary agreements between search engines and the creative-content sector to ensure piracy sites are removed from results or "demoted" in that they do not feature on the first (or first few) search results pages.

VOLUNTARY AGREEMENTS IN THE ASIA-PACIFIC REGION

Infringing Website Lists

The success and easy scalability of the United Kingdom's IWL model has led many countries in Asia to set up their own IWLs. In Asia, Indonesia (October 2017), Malaysia (October 2017), Hong Kong (December 2016), Vietnam, and Taiwan (September 2017) have set up IWLs.⁶⁴ On October 3, 2017, the Hong Kong Creative Industries Association reported Hong Kong's IWL scheme resulted in the removal of advertisements on infringing websites by 50 brands in Hong Kong, and reduced traffic to a number of infringing websites by 14 percent on average.⁶⁵ This is progress, given online advertising spending in Hong Kong in 2017 was estimated to be around \$730 million, of which approximately 30 percent went to these infringing websites.

Australia: De-indexing Piracy Sites in Search Results

Stakeholders in Australia have also set up a voluntary agreement to de-index piracy websites. However, the Australian model is different in that it involves only one major search provider: Google. The Australian model is particularly interesting in that it links the de-indexing agreement with the country's legal framework for blocking access to websites involved in large-scale piracy, which has proven to increase consumption of legal content and reduce consumption of pirated material.⁶⁶ Russia has done likewise, albeit via legislation.

In 2019, Google reached a voluntary agreement with local ISPs and content rightsholders to de-index piracy websites from its Australian website (google.com.au) that have been blocked by Internet providers under Australian law.⁶⁷ As of May 2019, Google had de-indexed 832 piracy websites. Australia's former Minister for Communications, Mitch Fifield, points out that, while not legislated, Australia's website-blocking legislation has led to these types of voluntary and positive partnerships between platforms and content creators.

In a way, these voluntary agreements to demote piracy-site rankings build on what major search engines, such as Google, have been doing themselves as they incorporate copyright-removal notices into their search engine algorithms to help with page ranking.⁶⁸ In late June 2018, a

Google spokesperson stated that it had demoted 65,000 websites globally each week, and such demotion resulted in sites losing around 90 percent of their visitors from Google Search.⁶⁹ This shows the impact of demotion. And while this is definitely progress, piracy websites have reacted—including by hopping from domain to domain—in order to circumvent downranking settings for a particular website.⁷⁰ This highlights the need for other ways for search engines to work with other stakeholders in making it harder for piracy sites to feature prominently in search results—such as Google blocking piracy sites in Chrome and Firefox due to malware—while comprehensively, consistently, and prominently featuring sites that provide legal sources of content.⁷¹

VOLUNTARY AGREEMENTS AND THE WORLD INTELLECTUAL PROPERTY ORGANIZATION

WIPO and its member countries have enacted a new program to support the growing use of IWLs by individual countries. In June 2019, it set up a central database—called the “Building Respect for Intellectual Property” database—to allow authorized agencies in member countries to upload lists of piracy websites they’ve identified in their own systems to help others decide for themselves which sites to cut off from advertising revenue.⁷² It is important to note here that these are not sites wherein occasional infringing content might be posted, but rather sites dedicated to piracy.

WIPO and its member countries have enacted a new program to support the growing use of IWLs by individual countries.

This follows earlier discussions on the issues, such as in December 2018 and March 2019.⁷³ WIPO recognizes the role voluntary agreements can play in supporting IP, stating:

The project responds to increased interest among policymakers in methods of building respect for intellectual property which rely on voluntary cooperation, rather than on judicial or other compulsory measures.⁷⁴

Approved actors from the advertising sector (such as brand owners and advertising agencies) would be allowed to download this list to inform their own decisions as to where they place their ads (i.e., it’s voluntary). To accommodate the different systems and approaches, WIPO stipulates the central criteria that each website on uploaded national lists be a “site of concern,” meaning it’s reasonably suspected the website is deliberately infringing copyright and related works. Responsibility for managing these lists, and any right of appeal or review, remains with the managers of the national lists, not WIPO.

SUPPORT FOR AND OPPOSITION TO VOLUNTARY AGREEMENTS: CIVIL SOCIETY, ACADEMIA, AND STAKEHOLDERS

Despite the fact that these agreements involve good-faith efforts by governments and a wide range of stakeholders involved in the digital economy to enact reasonable measures to proactively address certain parts of the piracy ecosystem, ideological opponents of IP portray a grim picture, relying on vague claims that such actions represent an attack on a broad range of rights, and that these stakeholders are controlling the Internet.

EFF spoke for many in this camp when it stated, “We are calling these invisible and unaccountable arrangements Shadow Regulation.... [T]o defend our Internet, we need to pay attention to the encroachment of these secretive, exclusive agreements, and challenge them when they pose a threat to our digital rights and democracy.”⁷⁵ Note that “their Internet” is not necessarily “our Internet,” as most Internet users would see it. “Their” Internet is an Internet wherein there are no rules, and illegal actions are allowed to run rampant. Also, most of these agreements are enacted in countries with independent judiciaries and legal protections for human rights and other related concerns. Similar to their other efforts to portray copyright as some conspiratorial tool for nefarious ends, EFF goes on to list examples of voluntary initiatives (most of which concern copyright infringement) which it plans to “bring... into the bright light of public scrutiny.”⁷⁶

As ITIF’s president Rob Atkinson outlined in “EFF Throws and Provides Shade,” EFF rejects both the rule of law and the right to self-organize, which in essence is a defense of anarchy.⁷⁷ After all, it was EFF founder John Perry Barlow who, in his nihilistic, libertarian rant “A Declaration of Independence of Cyberspace” declared that the Internet should not be subject to any rules whatsoever, from government or private actors. For EFF, digital rights mean the right not only to shout, “Fire!” in a crowded theatre, but to light fire to the theatre itself. Indeed, EFF cannot claim to be protecting digital rights when it proclaims voluntary agreements should have no standing. Collective action is how order and progress occur, whether it be through government or other associations. For example, neither the Donuts/Radix nor MPA voluntary agreement create new categories of action. All action taken under these agreements must be for causes, and using remedies, already enumerated in other contracts between ICANN and the registry, the registry and some registrar, and the registrar and some registrant. Only the process of notification is affected.⁷⁸ EFF and likeminded academics seem only interested in inaction, as they see efforts to limit piracy as an attack on their view of Internet freedom, and digital rights as license, not responsibility.⁷⁹

These voluntary agreements, and other debates about public policy issues online, represent a growing consensus that the values, laws, and norms we cherish offline are clearly underrepresented online. As tech pioneer and Internet security expert Paul Vixie stated in a piece responding to an article by University of Idaho Law Professor Annmarie Bridy that criticized the Donuts-MPA agreement:

The courts have borders, where the DNS (domain name system) does not.... The Internet's technical and contractual structure has helped millions of criminals effectively bypass the system of laws and treaties by which the world's economies capped their losses in the pre-online era. Adjustment and redress of this imbalance is as inevitable as it is necessary.⁸⁰

In conclusion, Vixie noted that the trusted notifier program represents the engagement of Internet industry stakeholders with rightsholder communities to create efficient takedown-related activities, which is exactly what the Internet technical community told rightsholders they should pursue instead of the Stop Online Piracy Act (SOPA), a draft piracy website blocking bill that was considered, but never enacted, by the U.S. Congress in 2011.⁸¹ But of course, Internet extremists such as EFF and Bridy not only oppose laws (e.g., SOPA); they oppose voluntary agreements. For them, anything that might get in the way of individual license, even to do wrong, must be opposed, for as they say, “The Internet must be free.”

These voluntary agreements, and other debates about public policy issues online, represent a growing consensus that the values, laws, and norms we cherish offline are clearly underrepresented online.

As the Internet & Jurisdiction report “Cross-Border Domain Suspension” states, tensions around these two approaches—between the “Internet freedom” absolutists that oppose both government action and industry self-regulation and others that recognize that at least the latter is legitimate and necessary—tend to prevent a constructive discussion on substance.⁸² It’s time for EFF and their ideological fellow travelers to stop peddling fear to consumers and users—and providing shelter to “vandals, vigilantes, and mercenaries” who hide in their shadow—and work with other responsible stakeholders on constructive proposals that address a mutually recognized and supported goal: an innovative, creative digital economy that is based on legal content.

In line with this, despite Stephen Crocker (chair, ICANN Board of Directors) having pointed out that while these initiatives are outside of ICANN’s remit, he has stated that ICANN is hopeful these voluntary agreements will produce usable tools and mechanisms for registries and registrars.⁸³ The Framework to Address Abuse is another constructive contribution. On December 9, 2019, 48 registrars and registries (including Donuts, Neustar, and other major providers) signed on to this initiative to address some of the most egregious abuses of the DNS.⁸⁴ The Framework differentiates between what ICANN calls “DNS abuse” (e.g., malware, botnets, phishing, pharming, and spam) and “website content abuse” issues (e.g., piracy). The members are not required under their agreements with ICANN to monitor or suspend domains based on website content abuse. While ITIF may disagree, it supports this distinction given there is no universally accepted standard for evaluating content on the Internet.

However, these registrars and registries believe there are certain forms of website content abuse—relating to physical threats to human life—that are so egregious they should act when provided with specific and credible notice, such as on child sex abuse materials, the illegal distribution of opioids, human trafficking, and specific and credible incitements to violence. To help them do this, the framework suggests registrars and registries consider using trusted notifier systems, which are a form of voluntary agreement. It also notes that each registrar and registry has its own acceptable use policies or terms of use that set forth provisions that may cover these and additional forms of website content abuses, which presumably include piracy.⁸⁵ While the framework does not deal with IP, it is at least a pragmatic and constructive proposal built on the recognition that responsible stakeholders have a role to play in supporting a healthy and safe digital environment—as well as being based on the processes and voluntary agreements outlined in this report.

The Center for Democracy & Technology (whose founder Jerry Berman used to sit on the board of a former voluntary agreement, the Copyright Alert System) and other civil society voices also take a far more sensible tone. As it stated in a 2013 blog, “The Internet Society is, generally, in favor of industry-based initiatives to address various issues, including those related to intellectual property; however, we are also mindful of the risks associated with these approaches.”⁸⁶ Given the potential for stakeholders to potentially misuse these agreements, this is a reasonable response to ensure they’re properly based in a country’s legal system and its inbuilt checks and balances. While we should always monitor developments, many of these voluntary agreements have been in force for years, have proven useful in addressing a specific part of the piracy ecosystem, and have not led to a large-scale negative impact on how the Internet works (as the opposition’s “Chicken Little” rhetoric suggests would happen).

CONCLUSION AND RECOMMENDATION: THE MORE COOPERATION AND ANTI-PIRACY TOOLS, THE BETTER

The global phenomenon of digital piracy cannot be tackled by any single government or international organization. Communication, collaboration, and cooperation across relevant actors, including government and the private sector, will be essential in reducing digital piracy and supporting the legal market for creative content. Within this, voluntary cooperation between different stakeholders in the digital economy can and does play an important role in addressing a host of harms that take place on the Internet, including piracy.

This report has provided a snapshot into some voluntary agreements.⁸⁷ Some agreements have come and gone, such as the Copyright Alert System.⁸⁸ Forming and operating voluntary agreements can be challenging given the legal and business issues between different stakeholders that have often been in protracted conflict over their respective roles in addressing digital piracy. However, the success of TAG, IWLs, RogueBlock, and others, and the fact that other countries and WIPO are replicating and supporting them, is evidence voluntary agreements should be one of the policy tools countries use to fight digital piracy. There is still a lot of room for other countries to adopt existing agreements and for everyone to look at other potential areas for cooperation, as the level of policy experimentation and adoption in fighting digital piracy is still far below where one would expect it to be given the size and growth of the digital economy.

Policymakers from the United States, the EU and its member states, and other countries should support further research and discussion around how voluntary agreements can be a standard part of every country’s digital piracy toolkit, and should work more proactively to encourage more agreements. The United States and European Union have moved toward such a holistic approach to protecting and supporting the creativity behind digital IP in considering the entire lifespan of IP rights, from registration to enforcement, and what anti-piracy tools can be used within each of these.⁸⁹ This should obviously involve the organizations and stakeholders involved in current voluntary agreements sharing their experience and best practices to see how they could be applied to different parts of the piracy ecosystem. These parties should also include voluntary agreements as part of the best practices they support in other countries’ efforts to develop a healthy and creative legal digital economy.

Current experience shows governments have an important role to play in building the base for stakeholders to develop voluntary agreements (as has happened in the United States and the United Kingdom). This makes sense, as the government has an interest in how these

mechanisms are developed and implemented to ensure they follow principles of good governance and contribute to broader public policy goals. Indicative of the key facilitating role of government, the WIPO Advisory Committee on Enforcement stated in its submission (referring to the EU's, United Kingdom's, and Israel's experience with voluntary agreements) that they “highlight not only the value of effective partnerships between public and private sector actors but also the important role that state authorities can play in bringing together and facilitating cooperation between different industry actors.”⁹⁰

There is still a lot of room for other countries to adopt existing agreements and for everyone to look at other potential areas for cooperation, as the level of policy experimentation and adoption in fighting digital piracy is still far below where one would expect it to be given the size and growth of the digital economy.

In line with this, the EU, United States, United Kingdom, and others should ask OECD to make sure it includes voluntary agreements as part of its IP discussions, and does more detailed research into the impact of existing agreements, in order to identify the key principles and best practices that feature in existing agreements—and whether it's possible to develop template frameworks for others to use. OECD should also build on the core points and provisions outlined by the EU in both its MoUs (see Appendix A) and WIPO submission in developing a model template (including core principles and processes) for developing voluntary agreements. This includes ensuring that agreements involve most, if not all, key firms in a sector, that these firms act in good faith in finding ways to work together. Within this model framework, the first step would be for government and industry to build a common narrative for stakeholders to engage on the issue. The stakeholders then have to dedicate time to building trust and understanding among themselves about how they each operate in a sector (which can vary widely), thus allowing them to collaborate in a way that is flexible (accounting for how businesses in the sector operate) and thus mutually beneficial. It should also include mechanisms to measure compliance and the impact of the agreement.⁹¹

The United States, European Union, United Kingdom, Australia, and others should encourage other countries to use voluntary agreements (which at the moment they don't do), and other anti-piracy policies, as part of a holistic approach to protect and support the creation of legal content in their respective countries. Ultimately, this needs to be part of a broader, energized effort to support the development of a global digital economy based on legal (and not illegal) content.⁹² Overall, the debate around the critical role of IP in the digital economy is fairly lackluster, especially in comparison with the growing digital economy and the focus on some other key issues, such as cross-border data flows. Wherever possible, nations and businesses around the world should rectify this imbalance and work together to support the development and spread of new tools, such as voluntary agreements.

APPENDIX A: ARRANGEMENTS TO ADDRESS ONLINE IP INFRINGEMENTS

On June 25, 2018, 14 companies and 14 associations signed an MoU.⁹³ Signatories agreed to measure the effectiveness of the MoU by reporting on the concrete means they individually have in place, and by monitoring the impact of the MoU on the online advertising market. The agreement has an assessment period of 12 months, during which the signatories will meet quarterly.

The signatories were Adform, Amobee, Associação Portuguesa de Anunciantes (APAN), Associazione Italiana Commercio Estero (Aice), comScore, Hrvatsko udruženje društava za tržišno komuniciranje (HURA) (Croatian Association of Communications Agencies), DoubleVerify, European Association of Communications Agencies (EACA), European Gaming and Betting Association (EGBA), Google, GroupM, Integral Ad Science (IAS), Internet Advertising Bureau Europe (IAB Europe), Internet Advertising Bureau Italy, Związek Pracodawców Branży Internetowej IAB Poland, Internet Advertising Bureau Slovakia, Internet Advertising Bureau UK (IAB UK), ISBA, OpenX, Publicis Groupe, Sovrn, SpotX, Sports Rights Owners Coalition (SROC), TAG, Uniunea Agentiilor de Publicitate din Romania (UAPR) (Romanian Association of Communications Agencies), Utenti Pubblicità Associati (UPA), White Bullet, and the World Federation of Advertisers (WFA).⁹⁴

According to the European Commission, the MoUs complement the legislative framework that continues to be the basis of the fight against counterfeiting and piracy. In conclusion, it states that the European Commission will hold further discussions in an effort to develop other MoUs, in the interest of stakeholders and society as a whole.⁹⁵

Signatories	Commitments
All Signatories	Undertake the actions provided for by the MoU in a manner that ensures full compliance with EU and national competition law
	Support the follow-the-money approach to IPR infringements, seeking to deprive commercial-scale IPR infringers of the revenue flows that make their activities profitable
	Ensure that, in relations with their contracting parties, for the services that fall within the scope of the MoU, they act in a manner that upholds the spirit of their commitments under the MoU
Advertisers (directly responsible for the placement of advertising)	Undertake reasonable measures to minimize the placement of their advertising on websites or mobile applications that infringe copyright or disseminate counterfeit goods on a commercial scale
	Take reasonable steps to ensure that, when they become aware their advertising is appearing on such websites and mobile applications, the advertising will be removed
	Limit the placement of their advertising on websites and mobile applications, based on their own individual policies and assessment criteria
	Adopt an IPR policy and make it publicly available
Advertising Intermediaries (directly involved in buying, selling, or brokering the sale or purchase of advertising space)	Undertake to allow, in their contractual agreements, advertisers or other media buyers to use or require the use of tools and safeguards with the aim that the advertising placed through or with support of the advertising intermediaries' services is not placed on websites and mobile applications that infringe copyright or that disseminate counterfeit goods on a commercial scale
	Allow individual advertisers to use or require the use of tools and safeguards with the aim that the advertising placed through—or with the support of—the advertising intermediaries' services are not placed on websites or mobile applications that have been identified by advertisers in their advertising placement policies, or with the aim that the advertising is removed from such websites when detected
	Adopt an IPR policy and make it publicly available
Associations	Use their best efforts to encourage their members not to offer for sale, recommend, or buy advertising space on websites or mobile applications that infringe copyright or disseminate counterfeit goods on a commercial scale—and allow their services to be used to place, or in connection with the placement of, advertising in such advertising space in compliance with the principles of the MoU and subject to applicable laws
	Encourage their members, where appropriate, to sign the MoU individually

About the Author

Nigel Cory is associate director, trade policy, with the Information Technology and Innovation Foundation. 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, which included positions working on G20 global economic and trade issues and the Doha Development Round. Cory also had diplomatic postings to Malaysia, where he worked on bilateral and regional trade, economic, and security issues; and Afghanistan, where he was the deputy director of a joint U.S./Australia provincial reconstruction team. Cory holds a master's in public policy from Georgetown University and a bachelor's in international business and a bachelor's in 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 the world's leading science and technology think tank, 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.

ENDNOTES

1. Brett Danaher, Michael D. Smith, and Rahul Telang, “Copyright Enforcement in the Digital Age: Empirical Evidence and Policy Implications,” *Communications of the ACM*, February 2017, Vol. 60 No. 2, Pages 68–75, <https://cacm.acm.org/magazines/2017/2/212432-copyright-enforcement-in-the-digital-age/fulltext#R21>.
2. Ibid.
3. Professor Joel Waldfoegel, Carlson School of Management, speaking at a World Intellectual Property Organization event on “Digitization and New Copyrighted Goods.” Youtube, “WIPO Seminar on Digitization and New Copyrighted Goods,” October 16, 2015, <https://www.youtube.com/watch?v=D0gWM2WRjGE#t=9m20s>.
4. “WIPO Assemblies, Address by the Director General Francis Gurry,” World Intellectual Property Organization website, https://www.wipo.int/about-wipo/en/dgo/speeches/a_51_dg_speech.html.
5. United States Intellectual Property Enforcement Coordinator (IPEC), *Annual Intellectual Property Report to Congress* (Washington, D.C.: IPEC, March, 2018), https://www.whitehouse.gov/wp-content/uploads/2017/11/2018Annual_IPEC_Report_to_Congress.pdf.
6. U.S. Department of Commerce, *Copyright Policy, Creativity, and Innovation in the Digital Economy* (Washington, D.C.: U.S. Department of Commerce Internet Policy Task Force, July, 2013), <https://www.uspto.gov/sites/default/files/news/publications/copyrightgreenpaper.pdf>.
7. U.S. Intellectual Property Enforcement Coordinator, *Annual Intellectual Property Report to Congress* (Washington, D.C.: White House, March, 2018), https://www.whitehouse.gov/wp-content/uploads/2017/11/2018Annual_IPEC_Report_to_Congress.pdf.
8. U.S. Intellectual Property Enforcement Coordinator (IPEC), *2013 Joint Strategic Plan on Intellectual Property Enforcement*, (Washington, D.C.: IPEC, June, 2013), <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/IPEC/2013-us-ipeec-joint-strategic-plan.pdf>.
9. For example: See “Comments the Motion Picture Association (MPA), Independent Film and Television Alliance (IFTA), Creative Future, and Screen Actors Guild-American Federation of Television and Radio Artists (SAG-AFTRA), U.S. Department of Commerce inquiry about the state of counterfeit and pirated goods trafficking and recommendations,” MPA website, July 29, 2019, <https://www.mpa.org/wp-content/uploads/2019/07/190729-MPAA-IFTA-CreativeFuture-SAG-AFTRA-comments-to-DOC-re-presidential-memorandum-on-counterfeiting-and-piracy.pdf>.
10. U.S. Department of Commerce, *Copyright Policy, Creativity, and Innovation in the Digital Economy*.
11. Donuts and Motion Picture Association of America, “Donuts and the MPAA Establish New Partnership to Reduce Online Piracy,” news release, February 9, 2016, <https://www.mpa.org/wp-content/uploads/2016/02/Donuts-and-MPAA-Establish-New-Partnership-2.9.16.pdf>.
12. Donuts, “Characteristics of a Trusted Notifier Program,” accessed by the Internet Wayback Machine on January 17, 2020, <https://web.archive.org/web/20160615074509/https://donuts.domains/images/pdfs/Trusted-Notifier-Summary.pdf>; Daniel Castro and Nigel Cory, “Industry cooperation takes another step in fighting online piracy,” *The Hill*, March 3, 2016, <https://thehill.com/blogs/pundits-blog/technology/271587-industry-cooperation-takes-another-step-in-fighting-online>.
13. @Icann_President on Twitter, “Congrats Donuts & MPAA on collaborating to fight online piracy & showing the voluntary multistakeholder model works! <http://pco.lt/1O1DP1xm>” Twitter, February 9, 2016, https://twitter.com/icann_president/status/697135725297315840.
14. Daniel Castro, testimony on “Stakeholder Perspectives on ICANN: The .SUCKS Domain and Essential Steps to Guarantee Trust and Accountability in the Internet’s Operation” before the Committee on the

- Judiciary, Subcommittee on Courts, Intellectual Property, and the Internet, Information Technology and Innovation Foundation website, May 13, 2015, http://www2.itif.org/2015-ICANN.pdf?_ga=1.235100161.1235692253.1449185070; Daniel Castro, "If ICANN Won't Stand Up to EU in WHOIS Dispute, Then the U.S. Congress Should," *CircleID*, December 19, 2019, http://www.circleid.com/posts/20191219_if_icann_wont_stand_up_to_eu_whois_dispute_then_us_congress_should/.
15. Andrew Allemann, "11 domains affected by Donuts' 'trusted notifier' deal with MPAA," *Domain Name Wire*, February 28, 2017, <https://domainnamewire.com/2017/02/28/11-domains-affected-donuts-trusted-notifier-deal-mpaa/>; "One Year Later: Trusted Notifier Program Proves Effective," media release, Motion Pictures Association, March 6, 2017, <https://www.motionpictures.org/press/one-year-later-trusted-notifier-program-proves-effective/>.
 16. Ibid; Mitch Stoltz, "MPAA May Like Donuts, but They Shouldn't Be the (Copyright) Police," Electronic Frontier Foundation, February 10, 2016, <https://www.eff.org/deeplinks/2016/02/mpaa-may-donuts-theyshouldnt-be-copyright-police>; Allemann, "11 domains affected by Donuts' 'trusted notifier' deal with MPAA."
 17. Radix and the Motion Picture Association of America, "Radix and the MPAA Establish New Partnership to Reduce Online Piracy," news release, May 13, 2016, <https://www.mpaa.org/wp-content/uploads/2016/05/Radix-and-the-MPAA-Establish-New-Partnership-to-Reduce-Online-Piracy.pdf>.
 18. Radix website, accessed November 4, 2019, <https://radix.website>.
 19. National Telecommunications and Information Administration, "NTIA Statement on Amendment 35 to the Cooperative Agreement with Verisign," news release, November 1, 2018, <https://www.ntia.doc.gov/press-release/2018/ntia-statement-amendment-35-cooperative-agreement-verisign>.
 20. Neustar, "usTLD Registration Management" (volume 1, technical capability, November 21, 2018), https://www.ntia.doc.gov/files/ntia/publications/technical_proposal_volume_1.pdf.
 21. Domain Name Association, "Domain Name Association Unveils Healthy Domains Initiative Practices," news release, February 8, 2017, <https://thedna.org/domain-name-association-unveils-healthy-domains-initiative-practices/>.
 22. "DNA Health Domains Initiative: Registry/Registrar Healthy Practices," Torrent Freak website, 2017, http://thedna.org/wp-content/uploads/2017/02/DNA_Healthy_Practices_2017.pdf.
 23. Shane Tews, "Digital identities and privacy: Time to change how domain names are registered?" *American Enterprise Institute*, March 25, 2019, <http://www.aei.org/publication/digital-identities-and-privacy-time-to-change-how-domain-names-are-registered/>.
 24. Daniel Castro, "If ICANN Won't Stand Up to EU in WHOIS Dispute, Then the U.S. Congress Should," *CircleID*, December 19, 2019, http://www.circleid.com/posts/20191219_if_icann_wont_stand_up_to_eu_whois_dispute_then_us_congress_should/.
 25. Jeremy Macolm and Mitch Stoltz, "Healthy Domains Initiative Isn't Healthy for the Internet," Electronic Frontier Foundation, February 9, 2017, <https://www.eff.org/deeplinks/2017/02/healthy-domains-initiative-censorship-through-shadow-regulation>; Jeremy Malcolm, "Healthy Domains Revisited: the Pharmaceutical Industry," Electronic Frontier Foundation, March 2, 2017, <https://www.eff.org/deeplinks/2017/03/healthy-domains-revisited-pharmaceutical-industry>; "Warning Letter: Divyata," Letter from the United States Food and Drug Administration and the United States Drug Enforcement Administration, U.S. Food and Drug Administration website, September 6, 2019,

<https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/divyata-09062019>.

26. “About Us,” Trustworthy Accountability Group website, <https://www.tagtoday.net/aboutus/>; “Winning the Fight Against Ad-Supported Piracy: Successes, Challenges, and Best Practices” (paper, Trustworthy Accountability Group), https://cdn2.hubspot.net/hubfs/2848641/TAG_WhitePaper_AntiPiracy_Final.pdf.
27. “Digital Ad Industry Will Gain \$8.2 Billion By Eliminating Fraud And Flaws In Internet Supply Chain, IAB & EY Study Shows,” press release, Interactive Advertising Bureau, December 1, 2015, <https://www.iab.com/news/digital-ad-industry-will-gain-8-2-billion-by-eliminating-fraud-and-flaws-in-internet-supply-chain-iab-ey-study-shows/>.
28. “Participating Companies,” TAG website, <https://www.tagtoday.net/participating-companies/>.
29. “GroupM Requires Partners to use TAG-Certified Anti-Piracy Services,” press release, Trustworthy Accountability Group, September 23, 2015, <https://www.tagtoday.net/pressreleases/groupm-requires-partners-to-use-tag-certified-anti-piracy-services>.
30. “Report reveals the six business models being online copyright infringement,” press release, PRS for Music, July 18, 2012, <https://www.prsformusic.com/press/2012/report-reveals-the-six-business-models-being-online-copyright-infringement>.
31. NetNames and the Digital Citizens Alliance, “Behind the Cyberlocker Door: A Report on How Shadowy Cyberlocker Businesses Use Credit Card Companies to Make Millions” (paper), <https://media.gractions.com/314a5a5a9abbbbc5e3bd824cf47c46ef4b9d3a76/7843c97d-fd81-4597-a5d9-b1f5866b0833.pdf>.
32. United States Trade Representative (USTR), *2017 Out-of-Cycle Review of Notorious Markets* (Washington, D.C.: USTR, 2017), <https://ustr.gov/sites/default/files/files/Press/Reports/2017%20Notorious%20Markets%20List%201.11.18.pdf>.
33. Dana Neale, “White Bullet Q3 2018 Report: Why Are Ad Companies with IP Compliance Commitments Still Funding Digital Piracy and Counterfeiting?” White Bullet website, November 9, 2018, <https://www.white-bullet.com/white-bullet-q3-report-why-are-ad-companies-with-ip-compliance-commitments-still-funding-digital-piracy-and-counterfeiting>.
34. EY, “Measuring digital advertising revenue to infringing sites” (report for Trustworthy Accountability Group to benchmark the United States), September 2017, <https://cdn2.hubspot.net/hubfs/2848641/Measuring%20digital%20advertising%20revenue%20to%20infringing%20sites-1.pdf?t=1534882176284>.
35. 614 Group, “TAG Fraud Benchmark Study” (report for Trustworthy Accountability Group), December 2017, <https://www.tagtoday.net/hubfs/TAG%20Fraud%20Benchmark%20Study/TAG%20Fraud%20Benchmark%20Study.pdf?hsLang=en-us&t=1534882176284>.
36. Creative Future, “Follow the Money Update,” January 24, 2019, <https://creativefuture.org/follow-the-money-update/>.
37. *Challenges and opportunities for U.S. business in the digital age, Hearing before the Committee of Finance, United States Senate*, 114th Congress. 664, June 15, 2016, <https://www.finance.senate.gov/imo/media/doc/262471.pdf>.
38. “RogueBlock,” International Anticounterfeiting Coalition, <https://www.iacc.org/online-initiatives/rogueblock>.

39. *Challenges and opportunities for U.S. business in the digital age, Hearing before the Committee of Finance, United States Senate, 114th Congress.*
40. Ibid.
41. "RogueBlock," International Anticounterfeiting Coalition, <https://www.iacc.org/online-initiatives/rogueblock>.
42. European Commission, "Intellectual Property Rights Enforcement," European commission website, November 29, 2017, https://europa.eu/rapid/press-release_MEMO-17-4943_en.htm.
43. "Statement by Vice-President Ansip at EU Blockathon 2018 on the Memorandum of Understanding on online advertising and intellectual property rights," European Commission website, June 25, 2018, https://ec.europa.eu/commission/commissioners/2014-2019/ansip/announcements/statement-vice-president-ansip-eu-blockathon-2018-memorandum-understanding-online-advertising-and_en.
44. "Memorandum of Understanding on online advertising and IPR," European Commission website, https://ec.europa.eu/growth/industry/intellectual-property/enforcement/memorandum-of-understanding-online-advertising-ipr_en.
45. "Trustworthy Accountability Group hires former IAB UK executive, opens EU office to accelerate global expansion," press release, March 16, 2018, <https://www.tagtoday.net/pressreleases/tag-hires-former-iab-uk-executive-opens-eu-office-to-accelerate-global-expansion->.
46. "Trustworthy Accountability Group launches new anti-piracy initiative to protect European brands," press release, February 12, 2019, https://www.tagtoday.net/pressreleases/project_brand_integrity.
47. "Operation Creative and the Infringing Website List (IWL)," City of London Police website, May 25, 2016, <https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/Pages/Operation-creative.aspx>; "PIPCU: the IP police," The Trademarks and Brands Online website, October 1, 2014, <https://www.trademarksandbrandsonline.com/article/pipcu-the-ip-police>.
48. "PIPCU secures £3.3m funding until 2019," The Trademarks and Brands Online website, August 22, 2017, <https://www.trademarksandbrandsonline.com/news/pipcu-secures-3-3m-funding-until-2019-5061>.
49. "PIPCU: the IP police," The Trademarks and Brands Online.
50. "Operation Creative sees 64 per cent drop in UK advertising," City of London Police, March 2, 2017, <https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/pipcu-news/Pages/Operation-Creative-sees-64-per-cent-drop-in-UK-advertising-.aspx>.
51. "Gambling adverts on illegal sites drop 87%: research," The Trademarks and Brands Online website, June 14, 2017, <https://www.trademarksandbrandsonline.com/news/gambling-adverts-on-illegal-sites-drop-87-research-5015>.
52. "Code of Conduct to promote lawful behavior on the Internet," Denmark's Ministry of Culture, https://kum.dk/fileadmin/KUM/Documents/Nyheder%20og%20Presse/Pressemeddelelser/2015/Code_of_Conduct_-_Engelsk_version.pdf; "Codex," codex website, <http://adkodex.com/codex/>.
53. European Union Intellectual Property Office (EUIPE), *Digital Advertising on Suspected Infringing Websites*, (EUIPO, January, 2016), <https://euiipo.europa.eu/ohimportal/documents/11370/80606/Digital+Advertising+on+Suspected+Infringing+Websites>.
54. "The International Anti Counterfeiting Coalition and City of London Police Partner to Protect Consumers from Online Counterfeits," City of London Police, April 3, 2017, <https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/pipcu-news/Pages/The-International-Anti-Counterfeiting-Coalition-and-City-of-London-Police-.aspx>.

55. Ibid.
56. "EURid and IACC Team Up to Fight Cybercrime," EURid, June 27, 2018, <https://eurid.eu/en/news/eurid-and-iacc-team-up-to-fight-cybercrime/>.
57. "RogueBlock," International AntiCounterfeiting Association (IACC), 2019, <https://www.iacc.org/online-initiatives/rogueblock>.
58. Liron Sivan, Michael D. Smith, and Rahul Telang, "Do Search Engines Influence Media Piracy? Evidence from a Randomized Field Study," Evidence from a Randomized Field Study (September 12, 2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2495591.
59. "Search engines and creative industries sign anti-piracy agreement," press release, United Kingdom Intellectual Property Office, February 20, 2017, <https://www.gov.uk/government/news/search-engines-and-creative-industries-sign-anti-piracy-agreement>.
60. "How Google Fights Piracy," Google, November 2018, https://blog.google/documents/25/G0806_Google_FightsPiracy_eReader_final.pdf.
61. Kantar Media, "OCI Tracker: High volume infringers analysis report" (report for the United Kingdom's Ofcom, 2012), https://www.ofcom.org.uk/__data/assets/pdf_file/0024/77352/high_volume_infringers.pdf.
62. "Corporate report: IPO Strategy 2018 to 2021," United Kingdom Intellectual Property Office, June 11, 2018, <https://www.gov.uk/government/publications/ipo-strategy-2018-to-2021>.
63. "Policy paper: Creative industries: Sector Deal," United Kingdom Department for Digital, Culture, Media, and Sport, March 28, 2018, <https://www.gov.uk/government/publications/creative-industries-sector-deal/creative-industries-sector-deal-html>.
64. Ari Juliano Gema, "Intellectual property rights: Indonesia can win the war on online piracy," *The Jakarta Post*, May 3, 2018, <https://www.thejakartapost.com/academia/2018/05/03/intellectual-property-rights-indonesia-can-win-the-war-on-online-piracy.html>; Masriwanie Muhamading, "Malaysia launches Infringing Website List initiative to combat digital piracy," *New Strait Times*, October 10, 2017, <https://www.nst.com.my/news/nation/2017/10/289556/malaysia-launches-infringing-website-list-initiative-combat-digital>; Lauly Li, "MOU signed to cut ads on piracy sites," *Taipei Times*, September 5, 2017, <http://www.taipeitimes.com/News/biz/archives/2017/09/05/2003677797>.
65. "Infringing Website List enlists 50 HK brands to cut pirate ad revenue," Marketing Interactive website, October 4, 2017, <https://www.marketing-interactive.com/infringing-website-list-enlists-50-hk-brands-to-cut-pirate-ad-revenue/>.
66. Nigel Cory, "How Website Blocking Is Curbing Digital Piracy Without 'Breaking the Internet'" (The Information Technology and Innovation Foundation, August 22, 2016), <https://itif.org/publications/2016/08/22/how-website-blocking-curbing-digital-piracy-without-breaking-internet>.
67. Jennifer Duke, "'From enemies to allies': Google removes piracy websites from search results," *The Sydney Morning Herald*, May 13, 2019, <https://www.smh.com.au/business/companies/from-enemies-to-allies-google-removes-piracy-websites-from-search-results-20190510-p51m55.html>.
68. "How Google Fights Piracy," Google, <https://drive.google.com/file/d/0BwxyRPFduTN2NmdYdGdJQnFTeTA/view>.
69. Jennifer Duke, "'Empty desks everywhere': film industry reeling from online piracy," *The Age*, June 27, 2018, <https://www.theage.com.au/business/companies/empty-desks-everywhere-film-industry-reeling-from-online-piracy-20180627-p4zo37.html>.
70. Ernesto, "Google's New Search Downranking Hits Torrent Sites Hard," *Torrent Freak*, October 23, 2014, <https://torrentfreak.com/googles-new-downranking-hits-pirate-sites-hard-141023/>.

71. Emil Protalinske, “Google blocks The Pirate Bay in Chrome and Firefox over ‘harmful programs,’” *Venture Beat*, September 15, 2016, <https://venturebeat.com/2016/09/15/google-blocks-the-pirate-bay-in-chrome-and-firefox-over-harmful-programs/>.
72. World Intellectual Property Office (secretariat), “Advisory Committee on Enforcement: Building Respect for IP (BRIP) Database Project,” World Intellectual Property Office, September 2-4, 2019, https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_14/wipo_ace_14_9.pdf.
73. “Building Respect for IP (BRIP) Database Project – Second Stakeholders’ Meeting,” World Intellectual Property Office, December 7, 2018, https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_brip_ge_18/wipo_brip_ge_18_inf_1.pdf; “Information Meeting for the Advertising Sector on International Cooperation to Prevent Digital Advertising on Suspected Copyright-Infringing Websites,” World Intellectual Property Office, March 8, 2019, https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_brip_ge_19/wipo_brip_ge_19_inf_1_prov_3.pdf.
74. Ibid.
75. Jeremy Malcolm and Mitch Stoltz, “Shadow Regulation: the Back-Room Threat to Digital Rights,” Electronic Frontier Foundation, September 29, 2016, <https://www.eff.org/deeplinks/2016/09/shadow-regulation-back-room-threat-digital-rights>.
76. Malcolm and Stoltz, “Shadow Regulation: the Back-Room Threat to Digital Rights.”
77. Robert Atkinson, “EFF Throws—and Provides—Shade,” *Innovation Files* blog, October 6, 2016, <https://itif.org/publications/2016/10/06/eff-throws-and-provides-shade>.
78. Paul Vixie, “Notice, Takedown, Borders, and Scale,” *CircleID*, March 1, 2017, http://www.circleid.com/posts/print/20170301_notice_takedown_borders_and_scale/.
79. Hannah Block-Wehba, “Global Platform Governance: Private Power in the Shadow of the State,” *SMU Law Review*, Article 9, Volume 72, Issue 1 (2019), <https://scholar.smu.edu/cgi/viewcontent.cgi?article=4778&context=smulr>; Annemarie Bridy, “Notice and Takedown in the Domain Name System: ICANN’s Ambivalent Drift into Online Content Regulation,” *Washington and Lee Law Review*, Volume 74, pp. 1345–1388, (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2920805.
80. Paul Vixie, “Notice, Takedown, Borders, and Scale,” *CircleID*, March 1, 2017, http://www.circleid.com/posts/print/20170301_notice_takedown_borders_and_scale/.
81. Kebin Madigan, “Trusted Notifier Program Defended Against Misleading Rhetoric,” Center for Intellectual Property Protection at George Mason University, March 2, 2017, <https://cpip.gmu.edu/2017/03/02/trusted-notifier-program-defended-against-misleading-rhetoric/>.
82. Internet & Jurisdiction, “Cross-Border Domain Suspension: Problem Framing” (Internet & Jurisdiction, Paris, 2017), <https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Paper.pdf>.
83. “Letter: Stephen Crocker (Chair, ICANN Board of Directors to Greg Shatan (President, Intellectual Property Constituency)), “June 30, 2016, <https://www.icann.org/en/system/files/correspondence/crocker-to-shatan-30jun16-en.pdf>.
84. “Framework to Address Abuse,” December 6, 2019, http://www.dnsabuseframework.org/media/files/2019-12-06_Abuse%20Framework.pdf.
85. Ibid.
86. Konstantinos Komaitis, “Voluntary Initiatives as a source of policy-making on the Internet,” Internet Society, July 29, 2013, <https://www.internetsociety.org/blog/2013/07/voluntary-initiatives-as-a-source-of-policy-making-on-the-internet/>.

87. "IACC RogueBlock®," RogueBlock website, <https://www.iacc.org/online-initiatives/rogueblock>.
88. Ted Johnson, "Internet Service Providers, Studios and Record Labels Call It Quits on Copyright Alert System," *Variety*, January 27, 2017, <https://variety.com/2017/digital/news/copyright-alerts-piracy-mpaa-comcast-att-1201971756/>.
89. European Union Intellectual Property Office (EUIPO), *International Forum on IP Enforcement* (Brussels: EUIPO, June 12-13, 2019), https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/IP_enforcement_events/International_Forum_on_IP_Enforcement_2019_Report_en.pdf.
90. "Arrangements to Address Online IP Infringements: Advisory Committee on Enforcement, Thirteenth Session," World Intellectual Property Organization, September 3–5, 2018, https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_13/wipo_ace_13_7.pdf.
91. Ibid.
92. Stephen Ezell and Nigel Cory, "The Way Forward for Intellectual Property Internationally" (The Information Technology and Innovation Foundation, April 25, 2019), <https://itif.org/publications/2019/04/25/way-forward-intellectual-property-internationally>.
93. MoU on Online Advertising and Intellectual Property Rights, European Commission website, June 21, 2018, <https://ec.europa.eu/docsroom/documents/30226>.
94. Advisory Committee on Enforcement, "Arrangements to Address Online Ip Infringements," World Intellectual Property Organization, August 3, 2018, 17, https://www.wipo.int/edocs/mdocs/enforcement/en/wipo_ace_13/wipo_ace_13_7.pdf.
95. Advisory Committee on Enforcement, "Arrangements to Address Online Ip Infringements."