MEIEA®

MUSIC & ENTERTAINMENT INDUSTRY
EDUCATORS ASSOCIATION

Journal of the Music & Entertainment Industry Educators Association

Volume 14, Number 1
(2014)

Bruce Ronkin, Editor
Northeastern University

Published with Support
from

MIKE CURB COLLEGE *of*
ENTERTAINMENT *and* MUSIC BUSINESS
BELMONT
UNIVERSITY

A Survey of Graduated Response Programs to Combat Online Piracy

Serona Elton
University of Miami

A significant portion of this article comes from the following source: Elton, Serona. "Graduated responses to online piracy: Approaches taken in the United States and around the world." In Music and Law (Sociology of Crime, Law and Deviance, Volume 18)*, edited by Mathieu Deflem. Bingley: Emerald Group Publishing Limited, 2013. 37-58. ISBN: 978-1-78350-036-9*

Abstract

Recent studies indicate that a significant amount of all internet traffic is generated by the use of peer-to-peer and cyberlocker sites, and most of the activity involves illegal file sharing. Opinions differ as to how to quantify the losses due to online piracy, however, there is general agreement among the copyright industries that it is a serious problem worthy of significant effort and attention. Efforts to combat online piracy have been underway since the late 1990s and some approaches have proven more successful than others. One of the more recent approaches is the so-called graduated response which involves the imposition of a gradually escalating series of consequences. This article examines the history of digital music and the battle against online piracy in the United States, and the legal, political, and industrial origins and current state of the graduated response programs in France, South Korea, New Zealand, the United Kingdom, Ireland, Taiwan, and the United States.

Keywords: graduated response, intellectual property, copyright, online piracy, file sharing, peer-to-peer, cyberlocker, digital music, music business, entertainment business

Introduction

Online piracy is a huge threat to all of the copyright industries. The copyright industries are described in the World Intellectual Property Or-

ganization (WIPO) 2012 study on the Economic Contribution of Copyright-Based Industries as "industries which are dependent on copyright and related rights protection."[1] These industries include music as well as motion picture, press and literature, software, and others. Online piracy refers to the sharing of content, such as recorded music, movies, ebooks, and computer programs in violation of copyright laws (i.e., illegally), via the internet. According to a recent *New York Times* editorial, online piracy is "growing by leaps and bounds."[2] The article cites a powerful statistic from Cisco Systems' Visual Networking Index indicating that over one-fourth of all internet traffic is generated by the use of peer-to-peer and cyberlocker sites, and most of the activity involves illegal file sharing.[3] Unlike a typical website where a visitor is able to view content hosted on the website's computer server, like iTunes, peer-to-peer file sharing networks enable individuals on the network to share their files with other individuals on the network without the use of an intermediary or central computer server. Cyberlockers provide the ability for a user to store digital files on servers operated by the Cyberlocker provider. Their use becomes problematic when the particular service includes tools that enable the widespread sharing of files among its users. A study by Stephen Siwek at the Institute for Policy Innovation indicates that the annual losses in the United States relating to sound recordings alone number around US$12.5 billion.[4] However, the economic losses resulting from online piracy are difficult to quantify precisely. The U.S. Government Accounting Office (GAO) has indicated that this is due to the illicit nature of the activity and the reliance on assumptions to estimate what purchasing activities consumers would engage in if they were not obtaining the goods illegally. However, the GAO did find that the problem is sizeable and concerning.[5] Even some critics of the various economic studies which have attempted to quantify the size of the problem agree that, through the eyes of the copyright industries, it is seen as a serious problem worthy of significant effort and attention.[6] Efforts to combat online piracy in the United States have been underway since the late 1990s. Some approaches have proven more successful than others. One of the more recent approaches is the so-called graduated response, which involves rights holders, and internet service providers (ISPs) and their subscribers.

Early History of Online Piracy in the United States

The technological seeds of online piracy today were planted as early

as 1988, when the Motion Picture Experts Group (MPEG) was created as a working group of the International Standards Organization (ISO) and International Electrotechnical Commission (IEC), for the purpose of developing standards for digital audio and video compression. Within the MPEG, a sub-group focused on audio was formed. After just over four years of work, the MPEG-1 standard was published around the beginning of 1993. Within the MPEG-1 standard, Audio Layer 3 was the ability to "compress high quality audio CD data by a factor of 12 while maintaining a high quality audio sound."[7] This form of compression became known as MP3. In 1994, the first MP3 encoder software, "L3enc," was released by the Fraunhofer Institute (FI), followed in 1995 with the first MP3 decoder (player) software, "WinPlay3."[8] These software tools were widely available for little to no cost, and relatively easy to use on Microsoft Windows-based personal computers, giving the average computer user the ability to convert a professionally manufactured CD into MP3 files with little effort or training. In 1996, electronics giant Philips demonstrated its audio MPEG technology at the Consumer Electronics Show, and by 1997 unauthorized MP3 copies of recordings were popping up on fan-created websites. An article about this new phenomenon, which appeared in the music industry trade publication *Billboard* contained several important statements which foretold events to come: "More conflicts over copyright violations on websites are likely to arise as the industry aims to protect copyrighted material on the internet" and, "Major entertainment companies that choose to crack down on fan-created sites may find themselves with a public relations nightmare."[9] The record companies, owners of the copyrights in the sound recordings which were being illegally shared, were slowly starting to realize that they had a major problem brewing. That same year, the music industry took what it considered its first collective legal action to stop internet piracy, bringing suit against the operators of three different internet sites, all of which supported the sharing of unauthorized MP3 files.[10]

Concern over this new problem within the music industry continued to grow and attract more attention. Industry conferences, such as the 1998 Webnoize conference, held panel sessions dedicated to the topic, including one titled "MP3s: Friend or Foe."[11] The 1998 *Billboard* article titled "Industry Grapples with MP3 Dilemma" warned that Pandora's digital box had been opened and that "no amount of policing pirate Websites will force the lid shut."[12] The article's author also pointed out, insightfully, that

"Ironically, the CD format that revived and invigorated a stalled music industry may be responsible for its greatest future worries," referencing the fact that every professionally manufactured CD had become, in effect, a digital master from which an unlimited number of MP3 files could be created.[13] In a short amount of time, a large number of websites sprang up to offer illegal MP3 files of popular music. A *New York Times* article published in 2000 said that "MP3" was as popular a search term in internet searches as "sex."[14]

In 1998, the Digital Millennium Copyright Act (DMCA) was passed in the U.S., which made numerous amendments to the existing copyright law in order to address digital technologies. One of the components of the law, which plays a major role in the fight against online piracy, was the establishment of a safe harbor from copyright infringement liability for online service providers, which includes ISPs as well as website operators and others, so long as they comply with the conditions of the law. Without such a safe harbor, online service providers may be found liable for copyright infringement based on the actions of their users or subscribers, under the theories of vicarious and/or contributory liability. These theories of liability hold that those who assist and facilitate copyright infringement should be held responsible for their actions in the same way that the party who actually commits the infringement is. Section 512(i)(1)(A) of the DMCA requires ISPs to maintain a policy for "the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers."

Looking Back: Fighting Online Piracy in the U.S. With Lawsuits

A series of highly publicized lawsuits followed the first collective legal action taken by the music industry to stop internet piracy in 1997. During this initial phase of fighting internet piracy, the music industry focused on stopping the operators of websites and services which enabled the sharing of unauthorized MP3 files. The key question raised in these lawsuits was whether or not the operators could be held vicariously and/or contributorily liable for the unauthorized peer-to-peer sharing of MP3 files that was taking place on their services.

In August 1999, a new software client called Napster became available via the internet. Napster users were able to download the software for free and install it on their computers. The software enabled the central

Napster server to identify the MP3 files which existed on each of the users computers. When users wanted to find an MP3 file of a particular recording, they would initiate a search of Napster's central server index, find an instance of that recording on another Napster user's computer, and click on the file to download it from the computer where the file was stored. In December 1999, the Recording Industry Association of America (RIAA), the trade association representing the major record labels, on behalf of its members, brought suit against Napster. The case was considered the first time a company was sued for trafficking in unauthorized music.[15] The lawsuit alleged that Napster was guilty of copyright infringement, under the theories of contributory and vicarious liability. In March 2000, the *New York Times* ran a cover story titled "Potent Software Escalates Music Industry's Jitters," describing Napster and how prevalent its use had become, including diagrams of how the system worked. The article quoted the RIAA as saying it "has no plans to prosecute individual users of Napster, though copyright experts say the industry would have a very strong case" and that doing so would be counterproductive.[16] The article confirmed that not only the music industry, but also the television and film industry, had growing concerns about whether or not the internet would undermine the control of copyright holders. After a few court decisions and appeals in the case, Napster ultimately had to block access by its users to recordings owned by the record companies that the RIAA represented, which resulted in Napster shutting down its service in July 2001.

Once Napster stopped working, its more than 50 million users went looking for alternative ways to share files.[17] The music industry pursued lawsuits against each of the new peer-to-peer services that popped up, including Kazaa, Morpheus, Grokster, Aimster, LimeWire, and MegaUpload. New technical protocols for sharing files became more popular, such as BitTorrent, and operators of services moved overseas where some copyright laws treat secondary liability for infringement differently than the United States laws. Lawsuits have been filed in many countries around the world, including Finland, Hong Kong, Sweden, and New Zealand. Some of these have been civil suits initiated by the copyright owners, while others have been criminal cases brought by the governments. In the Grokster case, once the file sharing service ceased operating, the following text appeared on the site, at the URL http://grokster.com/, and remains there today:

> The United States Supreme Court unanimously confirmed that using this service to trade copyrighted material is illegal. Copying copyrighted motion picture and music files using unauthorized peer-to-peer services is illegal and is prosecuted by copyright owners. There are legal services for downloading music and movies. This service is not one of them. YOUR IP ADDRESS IS XX.XX.XXX.XX AND HAS BEEN LOGGED. Don't think you can't get caught. You are not anonymous.

This got the attention of peer-to-peer service users who mistakenly thought their actions could not be tracked.

In 2003, the RIAA filed suit against 261 individuals who had been using peer-to-peer sites to illegally trade music files.[18] In these cases, unlike those brought against the operators of the peer-to-peer services, the individuals' actions were alleged to have directly infringed the rights of the copyright owners. Individuals were identified via their Internet Protocol (IP) address, which is the unique identifier assigned to a device participating in a computer network. The identification process involved the John Doe subpoena process. The copyright owner, or its representative, uses a variety of means, including automated or manual searches of file sharing sites, to identify the IP addresses associated with the sharing of large numbers of their recordings. The most common way this is accomplished is with the aid of a third party online investigative service, like BayTSP, which uses a number of techniques, including masquerading as pirates and digital fingerprint and/or watermark analysis of shared files, to snoop out the illegal sharing of copyrighted content owned by its clients.[19] With the IP address, the copyright owner can readily find, through the American Registry for Internet Numbers (ARIN), which entity owns the IP address. This is typically the ISP, such as a cable or telephone company. In 2003, the process involved the RIAA sending subpoenas to ISPs to obtain the identity that corresponded to the IP address before the RIAA actually filed the copyright infringement lawsuit. At the beginning of 2004, this legal process changed, requiring the RIAA to file a suit against the John Doe before issuing the subpoena to find out their identity. That year, the RIAA announced that it had brought suit against an additional 532 individuals. Defendants in these suits were typically given the opportunity to settle the suit by paying the RIAA US$3,000, although that figure varied depending

on the number of infringements. The RIAA was widely criticized for its approach in going after individuals. Despite the fact that the RIAA had no way of knowing the identity of a particular IP address until the legal proceeding was already underway, it was often characterized as a bully going after twelve-year-olds and grandmothers. While most of these lawsuits resulted in settlements, a few highly publicized trials took place, including one against Jammie Thomas-Rasset and another against Joel Tenenbaum, both of which resulted in judgments against the defendants for more than $200,000 and $675,000 respectively. In December 2008, the RIAA, after bringing more than 35,000 suits, announced the end of its approach to suing individual file sharers, saying that it was going to focus instead on working with the ISPs to disconnect the internet access of repeat infringers.[20]

Looking Back: Fighting Online Piracy in the U.S. With Technology

In response to the rapidly growing use of the MP3 file format, in 1998 the five major record labels of the day, EMI, Sony Music, Warner Music, Universal Music, and BMG, launched the Secure Digital Music Initiative (SDMI). The goal of the initiative was to, "develop open technology specifications for protected digital music distribution."[21] They hired the originator of the MPEG/MP3 standard, Dr. Leonardo Chiariglione, to spearhead the effort, and formed an independent coalition of over 150 recorded music, information technology, and consumer electronics companies. The specification was to be implemented in two phases. The first involved creating an SDMI standard for portable player devices which would prepare them for special handling of SDMI-tagged music files through the use of a digital watermarking system. A digital watermark is essentially identification information embedded into a digital file in a way that is invisible to the user of the file without a decoder. The idea was that SDMI-compliant devices would treat SDMI-tagged files differently from unsecured files, like MP3s, by limiting certain uses such as making copies of copies, or only permitting the file to be listened to for a specified trial period. In the second phase, record companies would begin commercially releasing SDMI-tagged digital files into the market. Owners of SDMI-compliant devices would have the option of upgrading the software on the device to enable listening to SDMI-tagged music files. The upgraded software would be able to accommodate the special handling requirements

that were embedded in the music files. The application of rules governing how a digital file can be used is referred to as Digital Rights Management. DRM technology enables control over the "rights" that an end user has with respect to use of the content it is applied to. At the time, portable digital music players and digital music files were generally not compatible across manufacturers. The SDMI standard was intended to support interoperability by enabling different music file types and music players to work together. It was also intended to support the sorts of activities that legitimate owners of CDs wanted to be able to do, like rip their CDs and copy the digital files to their computers or portable devices.

As part of phase one of the project, the SDMI announced a public challenge, promising to pay $10,000 to any hacker who could successfully crack the watermarking technology the initiative had selected. The watermark was hacked, there was a dispute over the rules of the contest with respect to how the sound quality of the digital file had to be preserved, there was a controversy regarding the publication of an academic paper about the SDMI standard by the hacker, and there was a backlash from the information security community who regarded the contest as a way for SDMI to test the security of their system without paying for a typical system security audit.[22] In 2001, the initiative was suspended indefinitely because, according to Chiariglione, "Unfortunately it turned out that none of the technologies submitted could satisfy the requirements set out at the beginning, e.g., of being unnoticeable by so-called "golden ears." So SDMI decided to suspend its work in this area and wait for progress in technology."[23]

In Germany and Japan in 2000, and then in the U.S. in 2003, the physical compact discs that were released as albums by some record labels also included a form of DRM. They were not legally referred to as CDs because use of the "CD" trademark was limited to compact discs which were in compliance with the official audio CD Red Book standard, which they were not. They included technology that interfered with the ability to play them in CD ROM drives like those typically found in a computer. Consumers were generally displeased with the copy protected discs, and there was a public outcry for required labeling which would make clear to the consumer that the discs may not play in some devices. In 2005, there was a widely publicized controversy over a particular DRM technology on compact discs released by Sony BMG, one of the major record labels at the time, which included software called a rootkit that secretly embed-

ded itself into the operating system of the PC it was played on, making the computer vulnerable to hackers. The use of this hidden software resulted in class action lawsuits and a Federal Trade Commission settlement over unfair and deceptive business practices. By late 2006, the two major labels which had been releasing copy protected discs in the U.S.—Sony BMG and EMI—both discontinued the practice.[24]

When iTunes was launched in 2003, the digital files available for purchase were not MP3 files, rather they were another type of audio file called an Advanced Audio Coding (AAC) file, which included a form of DRM called FairPlay. The AAC file format was designed to be the successor to the MP3 format. FairPlay limited a consumer's ability to play the files on anything other than a limited number of iPods or other Apple devices. The use of DRM was widely criticized as doing little to help combat illegal piracy and for interfering with legitimate consumers doing what they were entitled to do under copyright law, like make limited copies for personal use. It was also seen as interfering with competition by stifling interoperability. Consumers could not decide to switch from their Apple iTunes account and iPod to a competitor without losing the ability to play all of their previously purchased AAC files. In late 2006 and early 2007, both Steve Jobs and Bill Gates went on record to express their opinion that DRM for music files should be abolished. Soon after, Apple and EMI, one of the major record labels at the time, announced that EMI's music would be available in the iTunes store in a DRM-free format. By 2009, all of the music on iTunes was available for sale in a DRM-free format.[25]

Today: Internet Service Providers and Access

Pursuing legal action against the operators of websites and services that encourage peer-to-peer sharing of unauthorized copies of music is often described as being analogous to the arcade game, Whac-A-Mole, such that for every site that ceases to operate, a new one pops up. Pursuing legal action against individuals who share unauthorized music files proved to be a public relations nightmare for the music industry, and didn't achieve the deterrent effect that had been hoped for. In searching for a more effective means to combat online piracy, the music industry shifted its focus to how websites which encourage peer-to-peer sharing are accessed. This latest phase of the fight to stop online piracy has a number of different components to it, including the seizing of internet domains and so-called graduated responses to continued infringement by individuals.

In 2010, the U.S. Department of Homeland Security's Immigration and Customs Enforcement branch (ICE) began a major crackdown on websites promoting copyright infringement and dealing in counterfeit goods. This crackdown involved the government taking over control of a number of domains and replacing the websites that they previously mapped to with a warning page. The warning page reads:

> This domain name has been seized by ICE—Homeland Security Investigations, pursuant to a seizure warrant issued by a United States District Court under the authority of 18 U.S.C. §§ 981 and 2323. Willful copyright infringement is a federal crime that carries penalties for first time offenders of up to five years in federal prison, a $250,000 fine, forfeiture and restitution (17 U.S.C. § 506, 18 U.S.C. § 2319). Intentionally and knowingly trafficking in counterfeit goods is a federal crime that carries penalties for first time offenders of up to ten years in federal prison, a $2,000,000 fine, forfeiture and restitution (18 U.S.C. § 2320).

The United States government controls all of the .com and .net domains, as well as those ending in .org, .cc, and several others. Other countries control their own top-level domains, such as .uk for the United Kingdom and .fr for France. The enforcement initiative falls under an umbrella of activities overseen by the National Intellectual Property Rights Coordination Center (IPR Center), a U.S. government task force which focuses on combating intellectual property theft. Similar efforts have been launched in other countries including Italy and Denmark. One of the most notable international seizures was of the Pirate Bay website, which began with a Swedish domain (.se). After getting wind of the imminent seizure of its domain by Swedish authorities, it quickly moved its website to a .gl domain in Greenland where it was then also seized, then to a .is domain in Iceland, then, fearing what the Icelanders would do, finally settling with a .sx domain in Sint Maarten in the Caribbean. The Pirate Bay's aggressive effort to evade intellectual property law serves as a good example of the challenges faced when seeking to enforce intellectual property rights in the international arena.

In 2007, France became the first country to seriously consider imple-

menting a graduated response to the infringing actions of individual file sharers. The broad concept, which has been implemented differently in various countries, involves an escalating series of consequences each time an individual is caught engaging in illegal file sharing. The response is therefore graduated in that it gradually increases in severity. The theory behind it is that once people realize they have been caught, and are made aware of the consequences, they will stop the behavior. This approach differs from the one in which individual filer sharers were sued for copyright infringement as the first step in an attempt to curtail their efforts in that there are numerous warnings given, many of which involve an educational component.

The graduated response approach has been implemented in numerous countries, and has become one of the primary ways online piracy is being combatted today. In some countries, the approach had been codified into law, while in others it has been implemented as a result of voluntary agreements between rights holders and ISPs. How an ISP is defined also differs somewhat from country to country, and some graduated response programs exclude certain ISPs, such as governments or schools, and those with fewer subscribers than a specified threshold. In most cases, the ISP is not monitoring peer-to-peer use by its subscribers. Rather, copyright owners must use a variety of measures, including anonymously venturing onto the peer-to-peer websites, and using third party monitoring companies, such as Dtechnet, to detect the illegal sharing. In almost all of the cases, the graduated response program is paired with an educational initiative to make the public more aware of copyright law, and an effort to expand the number and awareness of legal digital music services and retailers.

Critics of the approach tend to focus on two main arguments. One is that access to the internet is a fundamental right, which is tied closely to free speech, and therefore should not be restrained in any way. The other is that there is not sufficient due process involved in the approach, to wit, the typical appeals process puts the burden of proving that the access or sharing was permissible on the subscriber, which looks like a guilty-until-proven-innocent schema. Proponents of the approach often cite studies which show that most people sharing music illegally would stop if they received a notice from their ISP. Nevertheless, rights holders in numerous countries continue to pursue the implementation of such programs.

Prior Research

The topic of graduated responses to piracy has been the focus of considerable study. The vast majority of research was published in 2010, which aligns with the implementation of the first program. Much of the research is found in journals focused on business, law, or technology. Many researchers have taken an in-depth look at the implementation of graduated response programs in only a single country, such as Bomsel and Ranaivoson,[26] Meyer,[27] and Danaher, Smith, Telang and Chen[28] who all focus on France, Suzor and Fitzgerald[29] on Australia, Moreno[30] on the U.K., Wan[31] on Hong Kong, and Yu[32] and Bridy[33] on the U.S., while others focus on only two or three countries, such as Rayna and Barbie[34] on France and the U.K., and Bridy[35] on France, Ireland, and the U.S. Researchers such as Haber,[36] Yu,[37] Suzor and Fitzgerald,[38] Bridy,[39] and Moreno[40] explored the due process implications of graduated response programs, and other related questions regarding the principles of proportional justice, privacy, and fairness. Bomsel and Ranaivoson[41] and Wan[42] explored the programs from an economic perspective, while Bridy[43] explored the legal underpinnings of limited liability for ISPs and how that may be changing. Bridy[44] and LaFrance[45] call attention to the lack of transparency regarding the negotiations of the Anti-Counterfeiting Trade Agreement (ACTA), and the voluntary industry agreement in the U.S. Barron[46] and Meyer[47] argue that there is far more at stake here than simply addressing online piracy such as freedom and internet governance. Danaher, Smith, Telang, and Chen[48] performed a statistical analysis to arrive at the conclusion that the French graduated response program was effective at increasing legitimate digital sales, while Giblin[49] argues there is little to no evidence that these programs are effective or successful. This paper builds upon previous research, and provides the reader with both a retrospective and updated view of the graduated response programs in each of the seven countries where they have been implemented, in a manner designed to appeal to a broader population, helping to bridge the divide between theoretical and applied research.

Graduated Responses: Approaches Around the World

France

In 2001, the European Parliament and Council enacted the European Copyright Directive, which was designed to harmonize some aspects of

copyright law across the different countries in the European Union. Each member state of the European Union was required to implement the directive into its own national law. In 2006, the French enacted DADVSI, which is an acronym for the French title, *Loi sur le Droit d'Auteur et les Droits Voisins dans la Société de l'Information*, or the law on authors' rights and related rights in the information society. Parts of the law were designed to address illegal peer-to-peer sharing of copyrighted works, and in many ways it is similar to the U.S. Digital Millennium Copyright Act. The law was considered highly controversial and went through a complicated and protracted political process. It prohibited certain acts, such as taking the action "to edit, place at the public's disposal or communicate to the public, voluntarily and under any form, a means destined to place non-authorized works at the disposal of the public," or "voluntarily incit[ing], including through advertisement, such use," making them punishable by up to three years imprisonment and a fine of up to EUR300,000. The law also provided for establishing an independent commission to oversee the implementation of portions of the law. The commission was created and called ARMT, which is an acronym for *Autorité de Régulation des Mesures Techniques*, or authority for the regulation of technical measures, otherwise known as digital rights management (DRM). DRM is a type of technical measure that controls the use of digital content, preventing unauthorized copying. ARMT focused primarily on regulating DRM, rather than on the peer-to-peer sharing. In 2007, at the request of the French Minister of Culture, a task force was created, called the Olivenne Commission, to explore sanctions for illegal file sharing. The commission's work resulted in a Memorandum of Understanding (MoU) between rights holders and ISPs to experiment with new ways to address illegal file sharing. The recommendations of the Olivenne Commission led to the enactment of another law, in May 2009, designed to supplement DADSVI, called the Creation and Internet Law, which expanded and renamed the ARMT commission. The new name became HADOPI, an acronym *Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet* or High Authority for the dissemination of works and protection of rights on the internet.[50] Because HADOPI puts in place a three-level graduated response to illegal file sharing, it is often referred to as a *three strikes law*. In June 2009, part of the HADOPI law was declared unconstitutional because it would have allowed a non-governmental body to impose a sanction. A revised version of the law was approved in October 2009, and HADOPI first began send-

ing notices in October 2010.

The first step in the HADOPI graduated response procedure involves a copyright owner providing an IP address to HADOPI, which then obtains the IP address owner's contact information from his or her ISP, and the Commission for the Protection of Rights sending the subscriber a warning via email. The warning informs the subscriber of the allegations and the existence of legal alternatives available in the market. If a second infringement is detected within the six-month period following the warning, a certified letter, requiring acknowledgement of receipt, is sent to the subscriber with similar information as that found in the first email warning. The subscriber is then monitored for an additional period of one year. If a third infringement is detected during that period, another letter is sent informing him or her that the actions are subject to criminal prosecution. The Commission may also decide to refer the case to a criminal prosecutor. Subscribers may find themselves in court, subject to a fine of up to EUR1,500, and to a court order disconnecting internet access for a period of up to one month. Throughout the entire process, a subscriber may challenge the notices by contacting HADOPI.

By the end of 2012, HADOPI had sent over a million first warnings, over 100,000 second warnings, and 340 third warnings. Of the 14 cases referred to a criminal prosecutor, judgments were reached in only three of them, with only one resulting in a fine of EUR150. A study was released in March 2012 by HADOPI, analyzing the effects of its warning system, and it found a steady decline in use of illegal peer-to-peer sharing in France since the warnings went into effect, and that 71% of internet users surveyed said they would stop downloading illegal content if they received a warning from HADOPI. However, numerous other studies that followed, including one by the French music industry body SNEP, found that illegal peer-to-peer sharing was increasing while legal digital download sales were dropping. In May 2013, the report of a government-commissioned panel, referred to as the Lescure report, named after the person who led the panel, was published, reporting on the efforts against online piracy. It recommended numerous actions, including shutting down HADOPI and handing over the policing of online piracy to the *Conseil supérieur de l'audiovisuel* (CSA), the agency that regulates electronic media in France. Part of its proposal included replacing the three-strikes approach with automated fines that would kick in after two warnings, which start at around EUR60 and escalate for repeat offenders. In July 2013, it was announced

that HADOPI would be shuttered and replaced with a new system of fines overseen by the CSA. The official statement announcing the change also stated that the new focus of online anti-piracy efforts would be on websites that commercially profit from the activity. Information regarding how the new program has been implemented has not been publicly released.

South Korea

In July 2009 South Korea enacted amendments to its copyright law that addressed online piracy. One section of the law gave the Minister of Culture, Sports, and Tourism the right to order Online Service Providers (OSPs) to (a) issue warnings to subscribers who are transmitting illegal reproductions, and (b) suspend the accounts of infringers who had received at least three warnings. In November 2010 the internet accounts of eleven subscribers were ordered suspended, which is considered the first instance globally of someone losing internet access as a result of illegal file sharing activities. Another section of the law created the Korean Copyright Commission (KCC) and gave it the power to recommend that OSPs send warnings, delete the illegally copied materials, and/or suspend subscriber accounts.[51] Compliance with the recommendations of the KCC is voluntary; however, if not complied with, the KCC may request that the Minister of Culture issue an order requiring the suspension. While the law does not require the KCC to utilize a three-warning approach before making a suspension recommendation, that is the process currently specified in the Commission's bylaws. Some have argued that South Korea enacted the copyright law amendments, such as the graduated response provision, because of pressure from the United States and the European Union, which required increased protection of intellectual property in the trade agreements they each entered into with South Korea. In 2009, South Korea was removed from the United States Trade Representative's piracy watch list for the first time in twenty years.

The process is outlined in the Enforcement Decree of the Copyright Act, issued in February 2010, and begins with the KCC monitoring illegal file sharing activity on its own. When it detects illegal activity, it sends the subscriber a warning. A process whereby a subscriber can challenge the allegations is also established by the decree. Under the law, the penalties are a one-month suspension of internet access for a first suspension, which comes after three warnings, between one and three months for a second suspension, and between three and six months for a third or subsequent

suspension.

During the first year of operation after the law went into effect, the KCC recommended that warnings be sent to 32,878 subscribers. 31 subscribers had their accounts suspended by their OSPs for less than one month, which was the recommendation of the KCC. There were very few instances of an OSP declining to follow the KCC recommendation. By early 2013, according to the press, over 450,000 warnings had been sent and 380 user accounts had been shut down. In early 2013 Korea's National Human Rights Commission recommended the law be reexamined because it may violate constitutional rights. Around the same time, a member of the Korean National Assembly, Congressman Choi Jae-cheon, put forth a proposal to repeal the graduated response portion of the law. He argues that the law violates due process and is inefficient from an economic perspective, imposing a punishment that is disproportionate to the crime. Proponents of the law argue that it has been very effective at curtailing illegal file sharing and has helped to support the growth of the legitimate digital music business in South Korea.

New Zealand

In 2008 New Zealand passed the Copyright (New Technologies) Amendment Act, to address copyright in the digital world. A specific section of the act, labeled Internet Service Provider Liability, required internet service providers to have a policy for terminating the accounts of repeat infringers. There was significant public outcry against how broadly internet service providers were defined in the law and how the provision was to be implemented. Public protests were staged and, for a period of time, New Zealand internet users changed their avatars to black squares to express their disdain for the particular section of the law. The implementation of the section was postponed until it was announced that it would be removed from the law and redrafted. In April 2011 a new law was passed, titled the Copyright (Infringing File Sharing) Amendment Act, which repealed the prior section. The new law established a graduated response approach, and replaced the term Internet Service Provider with Internet Protocol Address Provider (IPAP) to exclude schools and government departments that provide internet access, but are not traditional ISPs.[52]

The first step in the graduated response process in New Zealand involves a copyright owner providing an IP address to the IPAP. The IPAP then sends the subscriber a detection notice, informing the subscriber of

the allegations and informing him or her that what has been done is illegal. If a second infringement occurs within the 28 days from when the detection notice was received, a warning notice is sent, which says the same thing as the detection notice, but makes clear that it is a second notice. If a third infringement occurs within the 28 days following when the warning notice was received, an enforcement notice is sent. The copyright owner may bring the subscriber before the Copyright Tribunal and seek damages from the subscriber of up to NZD15,000. It is not until the process gets to the Copyright Tribunal phase that the identity of the subscriber is revealed to the copyright owner. The subscriber can challenge the notices all throughout the process. While the 2011 Act contemplates the suspension of a repeat offender's internet connection, that portion of the act can only be activated by an Order in Council, a form of legislation, which has not yet taken place. The Commerce Minister has stated that it will not be activated unless the existing process is unsuccessful.

In early 2013 the first case where the Copyright Tribunal assessed a fine after the graduated response protocol had been followed was decided, resulting in a fine of NZD616.57. A short time after came the second case, resulting in a fine of NZD557. By that time the Recording Industry Association of New Zealand (RIANZ) had requested that around 6,000 notices be sent by IPAPs, and 11 subscribers had been forwarded to the Copyright Tribunal. As of late 2013 there had been 17 rulings by the Copyright Tribunal, all of which found the account holders liable and assessed each of them fines averaging approximately NZD500. Currently, the copyright owner must pay a NZD25 fee for each notice they want issued, and the fee is designed to pay for the costs incurred by the IPAP. The RIANZ has argued that the fee is too high, particularly given that they are dealing with issuing thousands of notices, and are asking for it to be lowered to NZD2. The IPAPs have argued the fee is too low because it does not adequately cover the administrative costs of the notice program. In September 2012 after conducting a review, the Minister of Commerce recommended the current fee not be changed.

The United Kingdom

A government commissioned report published in 2006, called the Gowers Review of Intellectual Property, highlighted the damage being caused to the creative communities in the U.K. by illegal file sharing. It called for rights holders and ISPs to work together to create a set of best

practices which would change attitudes and behavior with respect to illegal file sharing. Further, it said that if the two groups cannot reach agreement on the practices, the government should intervene and establish a statutory protocol. The trade associations for the music and film industries, six of the leading ISPs, and the government, came together and entered into a Memorandum of Understanding (MoU) in July 2008. The goal of the MoU was to achieve a significant reduction in illegal peer-to-peer activity within two to three years. Each ISP was to put in place a three-month trial to send notifications to 1,000 subscribers per week, and the results were to be analyzed to determine how to move forward. The ISPs and rights holders were to craft a Code of Practice, which would be facilitated by Ofcom, the independent regulator for the U.K. communications industry. Despite much effort, the rights holders and ISPs were not able to reach an agreement over the practices. At the same time, the government was considering the results of several other commissioned studies on how intellectual property law supported innovation and growth in the digital realm. Another such study, published in June 2009, titled the Digital Britain Report, outlined the U.K.'s strategic vision for its role in the digital economy. The report included a section which addressed protecting and rewarding creativity, which recommended that Ofcom be required to place obligations on ISPs to (a) notify alleged infringers that their conduct is illegal, and (b) collect information on repeat offenders which can be, subject to a court order, turned over to copyright owners so that may pursue individual legal action against the infringer. If, after twelve months from initial implementation, these two approaches do not prove effective in reducing illegal peer-to-peer sharing, then Ofcom would be able to direct the ISPs to implement a series of other steps, including blocking particular URLs and capping subscriber bandwidth. However, the report did not recommend the penalty of having a subscriber lose his or her internet access.

In April 2010 the U.K. passed the Digital Economy Act, which was based heavily on the Digital Britain Report, as well as the Gowers Review and MoU. Unlike the Digital Britain Report, the act included the penalty of losing one's internet access for repeat infringement. This additional remedy was included at the urging of the Secretary of State, Lord Mandelson, who some argue was swayed by lobbyists from the content communities such as music and film. The law could not be implemented until Ofcom set forth a code of practice, which would explain how the law would be implemented in detail. A draft code of practice has to go through a number

of stages before it becomes law, to wit, a period where public comments are solicited, a review by the European Commission to ensure it does not pose any potential barriers to trade, the approval of the Secretary of State, and then the approval of Parliament. The initial draft of the code was published in May 2010. However, before the end of the public comment period, in July 2010, two of the largest ISPs in the U.K., BT and TalkTalk sought a judicial review of the law on a number of grounds, including that it breached European Law. The High Court decided in April 2011 in favor of the law, and BT and TalkTalk appealed the decision. During the time period while the law was under judicial review, its implementation was put on hold. In March 2012 the appeals court dismissed the appeal, clearing the way for the law to be implemented. In June 2012 a revised draft of the code was put forth by Ofcom. However, issues regarding how costs associated with the program would be shared were raised, requiring the draft to be further altered, resulting in the expectation that the first warning notices will not go out until late 2015 at the earliest.[53]

The first step in the proposed Ofcom graduated response process involves a copyright owner sending the ISP a Copyright Infringement Report, which includes the IP address associated with the illegal file sharing. The ISP then sends a warning notice to the subscriber, on paper, via first class mail. If the subscriber is issued three warnings within a twelve-month period, his or her name is to be placed on the ISPs Copyright Infringer List. Copyright holders are allowed to ask for a copy of the list once a month. The list does not contain any identifying information about the subscribers other than their IP addresses. However, if copyright owners see that a subscriber has received three or more warnings within the twelve-month period, they may go into court to seek an order requiring the ISP to reveal the identity of the subscriber, and then pursue direct legal action. A subscriber who has received a warning notice may appeal the notice at any stage throughout the process. There are costs involved with the process. Copyright owners must pay a fee that is meant, in the aggregate, to cover all of the costs incurred by Ofcom for administering the program, the majority of the costs incurred by operating an appeals body, and 75% of the cost that the ISPs incur for administering the program. Subscribers must pay a fee of GBP20 to challenge the warnings, but the money is refunded if the challenge is successful.

However, progress has been made in reaching a voluntary agreement between the rights holders and the ISPs. According to several news re-

ports in May of 2014, a deal had been struck between BT, Sky, TalkTalk, and Virgin Media (ISPs), and BPI and MPA (which represent music and film content creators, respectively) to create the Voluntary Copyright Alert Programme (Vcap). The Vcap calls for ISPs to send out "alerts" which are educational in nature, promoting legal downloading services, starting sometime in 2015. The rights holders will pay for 75% of the costs of the program. The ISPs will keep a record of which subscribers have received alerts, and how many, for up to twelve months, and will provide rights holders with a monthly report of how many alerts were sent out. The ISPs will not provide the rights holders with any identifying information about subscribers who have received alerts. A maximum of four alerts will be sent to a subscriber, with escalating language, but no threats with respect to service disruption or potential legal language will be included. The program will run for three years and then be reviewed to determine its effectiveness.

Ireland

In 2008 the Irish Recorded Music Association (IRMA), on behalf of its member record companies, sued Eircom, the largest ISP in Ireland. The suit alleged that Eircom failed to remove copyright infringing material from its systems, and failed to put in place measures to combat piracy. In February 2009 the parties decided to settle the case, resulting in an agreement where Eircom agreed to put in place a graduated response program, which would ultimately disconnect a subscriber's internet access after repeated warnings. The agreement was reviewed by the court and the graduated response process was found to be lawful. The agreement also required IRMA to do all that it could to put in place a similar agreement with Eircom's competitors. After the other ISPs declined to voluntarily agree to implement the same program, IRMA sued one of them, seeking to force their hand. In October 2010 the court found that laws to suspend internet access for illegal file sharers were not enforceable under the present law in Ireland, which, the court pointed out, meant that Ireland was not in compliance with its obligations under European law. Specifically, Irish law was not in line with the European Directive, 2001/29/EC, Article 8(3), which provides that an injunction may be sought by a rights holder who is affected by an infringing activity. However, since the graduated response program in place at Eircom was the result of an agreement, rather than a law, the court decision did not stop the program's implementation.

The same month, due to a technical glitch, Eircom mistakenly sent out warnings to 300 subscribers who were not at fault. This got the attention of the Office of the Data Protection Commissioner (ODPC), which decided to launch an investigation to determine if the program was violating data protection laws. In December 2011 the ODPC issued an enforcement notice banning Eircom from operating their graduated response program, which temporarily shut the program down. In July 2012 a court overturned the ban, and the program re-started.[54] In February 2012 an amendment to the Irish copyright law was enacted to remedy Ireland's non-compliance with European law, which paved the way for IRMA to once again pursue voluntary agreements with or legal action against the other ISPs. In early 2014, after attempts by the IRMA to enter into a voluntary agreement with Ireland's second largest internet service provider UPC failed, the three major music companies brought suit to compel compliance. The case is still pending.

The first step in the graduated response process involves a copyright owner sending the ISP notice regarding a specific IP address engaged in illegal file sharing. The ISP then contacts the subscriber, in writing, as well as by telephone and browser pop-up windows, to let him or her know that his or her IP address has been associated with copyright infringement, that such acts are illegal, and where legal alternatives can be found. If subscribers continue to engage in the illegal behavior, they are sent a second warning letter, making it clear that if they continue, their internet access will be suspended for a period of seven days. If subscribers continue the same behavior, internet access is suspended for the seven-day period. If subscribers still continue to engage in illegal behavior, internet access is suspended for a period of twelve months.

Taiwan

In May 2009 Taiwan passed an amendment to its Copyright Act which created a liability safe harbor for ISPs, so long as they comply with a number of different requirements. Among the requirements, the ISPs had to inform subscribers of their copyright protection policy, and let them know that, in the case of repeat infringements of three times or more, the ISP will terminate the subscriber's internet access in whole or in part. The Taiwan Intellectual Property Office (TIPO) would oversee the implementation. TIPO, after a period of consulting with rights holders and ISPs, prepared Regulations Governing Implementations of Limitations on Liabil-

ity for Internet Service Providers, which were promulgated in November 2009.[55] A 2013 report on Taiwan by the International Intellectual Property Alliance (IIPA), an alliance of trade associations representing U.S.-based copyright industries, drew attention to the fact that, despite being enacted four years prior, the law had not yet been implemented as the regulations only addressed the proper notice and counter-notice process, and did not set out the process regarding how ISPs should implement the law. The report urged further work by the rights holders, ISPs, and TIPO to reach agreement on a Code of Conduct. The report refers to a 2012 meeting which was held on the subject, but only resulted in an agreement by one ISP to test a proposed process for a limited time period. Although the U.S. Trade Representative removed Taiwan from the list of countries that do not sufficiently protect intellectual property in January 2009, the IIPA has indicated that its failure to implement its graduated response law remains an important issue to be watched closely.

While the graduated response process has yet to be ironed out, the first step involves a copyright owner sending the ISP notice regarding a specific IP address engaged in illegal file sharing. The ISP then sends a warning to the subscriber. If subscribers are warned three or more times, their internet access is somehow restricted, although the specifics of the restriction are yet to be determined. The ISP is not required to provide the identity of the subscriber to the copyright owner unless the subscriber files a counter-notice, claiming he or she has a right to access the content. Once the copyright owner knows the identity of the subscriber, in addition to whatever actions the ISP might take with respect to restricting internet access, the copyright owner is also free to pursue a direct legal action against the subscriber for infringement.

Other Countries

A number of other countries including Australia, Belgium, Colombia, and Spain have considered a graduated response program, but thus far have decided not to implement one. In 2009 the European Parliament voted against keeping a three-strikes policy within a telecommunication reform legislation, because it found that including it would restrict the fundamental rights and freedoms of users, without affording them an opportunity to be heard before a judicial authority. In June 2011 more than forty nations, including the U.S., signed a statement made by Sweden to the United Nations Human Rights Counsel condemning three-strike laws

against online copyright infringers as violating human rights. Neither France nor the U.K. signed the statement. New Zealand did sign the statement, despite having its own graduated response law, although the portion of its law that allowed for restricting internet access was not activated at the time, nor has it been thus far.

Graduated Responses: The United States Approach

As early as December 2003, the RIAA sent letters to the fifty largest ISPs in the United States asking them to voluntarily notify subscribers involved in file sharing over peer-to-peer networks that their activity is illegal. This letter came right at the time when the RIAA lost a lawsuit arguing that it had the power to send ISPs subpoenas for the identity information corresponding to IP addresses, without first needing to file a legal action against those John Doe subscribers. The court disagreed, which resulted in the RIAA changing its process to first bring suit against the John Doe subscriber before issuing a subpoena to learn his or her identity. As already discussed, the RIAA program of pursuing legal action against individual file sharers continued from 2003 until late 2008, when the RIAA announced that it was going to cease filing new actions against individuals, and instead seek cooperation from ISPs. In a hearing in May 2008, in front of the U.S. House of Representatives, Subcommittee on Telecommunications and the Internet, Committee on Energy and Commerce, on the then-proposed Internet Freedom Preservation Act of 2008, Mitch Bainwol, the RIAA CEO, testified that the industry was engaged in discussions with a number of ISPs about ways to address the illegal piracy issue, including a graduated response approach, among others. In the months that followed, the RIAA, as well as leaders from the movie and television industries, worked with New York Governor Andrew Cuomo to craft an agreement with the ISPs.

In January 2009 it was reported in the press that AT&T and Comcast, two of the largest ISPs in the U.S., were among the group of ISPs working with the RIAA on a solution. In March 2009 AT&T announced it would begin implementing, on a trial basis, a notification program. Two additional ISPs, Comcast and Cox, also confirmed they were exploring working with the RIAA on a new program, although they had been forwarding infringement notices to their subscribers for years. In July 2011, over two years later, the Memorandum of Understanding (MoU) was finally announced. Parties to it included numerous trade associations from the

entertainment industry, as well as their members, such as the RIAA, the Motion Picture Association of America (MPAA), the Independent Film & Television Alliance (IFTA), the American Association of Independent Music (A2IM), and five ISPs: AT&T, Cablevision, Comcast, Time Warner Cable, and Verizon. It is worth mentioning that Cox chose not to sign the MoU, and instead maintains its own graduated response protocol, which involves internet restrictions and potentially, after more than ten notices, termination of the subscriber's internet access. The MoU established a six-step Copyright Alert System (CAS), which is a common framework of best practices, and created the Center for Copyright Information (CCI), to support implementation of the program.[56] In a White House blog post the same month, Victoria Espinel, the United States Intellectual Property Enforcement Coordinator, commended the entertainment industry and ISPs for reaching the agreement, and stated the administration would continue to pursue solutions to the problems posed by online piracy. In order to give the ISPs time to implement the system, the first notices under the new program were not expected to be sent out until the second quarter of 2012. In September 2011 the CCI was formed, and in April 2012 an Executive Director was appointed at the CCI, its advisory board was established, which included members from the consumer and privacy protection groups, and it announced that it had entered into an agreement with the American Arbitration Association to implement an independent review process. After numerous delays, said to be the result of those involved wanting to ensure the program was consumer-friendly and remained true to the MoU, the CCI said in October 2012 that the program would be launching within several weeks. Unfortunately, hurricane Sandy hit the east coast of the U.S. in October which affected the CCI final testing schedules. In February 2013 the Copyright Alert System was officially launched. In May 2013 the press reported that the CCI had somehow lost its status as an official corporation due to a likely paperwork mishap, however that was quickly remedied and the CCI continues to operate as before. In May 2014 the CCI issued a progress report, indicating that 1.3 million alerts were sent out in the first ten months of the program, 70% of which were in the initial phases which focus on education, with fewer than 3% at the final escalated stage. During that time, 265 challenges were filed, and only 47 were successful based on an "unauthorized use of account" defense.

The first step in the CAS process involves a copyright owner providing an IP address to one of the participating ISPs. The ISP then notifies

the subscriber associated with the IP address, via email and/or other technologies such as in-browser alerts, that the account was involved in sharing copyrighted content over a peer-to-peer network. The notice, which is meant to be educational in nature, also includes information about how one can prevent this from occurring again, such as securing a wireless internet connection with a password, and where one can legally access or purchase digital music. The second time an alert is sent, the notice is essentially the same as the first. The third and fourth alerts require subscribers to acknowledge that they have received the alert and pledge to stop the unlawful activity. If a fifth and sixth alert are sent, mitigation measures will be utilized, such as requiring a subscriber to take a copyright tutorial, or reducing internet speed significantly for several days. If no further alerts are sent within a twelve-month period, the number of strikes against the subscriber is reset to zero. If a subscriber's activity warrants alerts beyond the sixth alert, he or she is considered to be the type of infringer who falls outside of the scope of the CAS, and no further alerts will be sent. A copyright owner's ability to pursue legal action against an individual infringer is not affected by the CAS process, and that may be the recourse a copyright owner seeks with respect to hardcore infringers. Subscribers who have received three or more alerts may appeal the alerts, based on six different grounds, to an independent arbiter, but they have to pay a $35 fee to do so. The fee is refunded if the appeal is successful, and if they are not able to afford it, it can be waived. The goal of the fee is to prevent frivolous appeals. Unlike some graduated response programs in other countries, a subscriber's internet connection will not be suspended or terminated, nor will a fine or criminal penalty be incurred.

Conclusion

The graduated response approach and its implementation is an evolving area of law, policy, and industry. The fundamental issues facing each of the countries that have implemented some form of graduated response are the same, to wit, how the content industries get the ISPs to participate, who administers the program of issuing notices, who pays for the program, and how due process rights of consumers will be protected. In terms of how to obtain ISP participation, the options range from statutory regulation (France, New Zealand, South Korea, Taiwan) to voluntary or court-sanctioned agreement (Ireland, U.K., U.S.). The programs are administrated by government agencies (France, South Korea), by non-gov-

ernmental entities created primarily for this purpose (U.S.), by the ISPs (Ireland, New Zealand, U.K.), or are stalled because it remains unclear how they will be implemented (Taiwan). In some countries, dissatisfaction regarding the cost and efficiency of administering the programs has been raised as a significant issue (France, New Zealand), and the question of due process protection for the purported infringer has been raised as a challenge to the applicable legislation (France, South Korea). As with any attempt to curtail online piracy, there will be proponents and critics of the approach. As results of studies on the effectiveness of graduated responses continue to be reviewed and compared to other approaches such as seizing domains, and the digital music marketplace is influenced by factors such as the availability of free streaming services like Spotify and Deezer, the approach may be refined, more widely embraced, or abandoned.[57]

Endnotes

1. WIPO, *WIPO Study on the Economic Contribution of the Copyright Industries* (Geneva, Switzerland: 2012), 1.
2. Eduardo Porter, "The Perpetual War: Pirates and Creators," *New York Times*, Feb. 5, 2012, SR.10.
3. Ibid.
4. Stephen Siwek, "The True Cost of Sound Recording Piracy to the U.S. Economy," *The Institute for Policy Innovation*, Aug. 21, 2007, http://www.ipi.org/ipi_issues/detail/the-true-cost-of-sound-recording-piracy-to-the-us-economy.
5. GAO, *Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods* (Washington, D.C.: GPO, 2010).
6. Julian Sanchez, "SOPA, Internet regulation, and the economics of piracy," *Ars Technica*, Jan. 18, 2012, http://arstechnica.com/tech-policy/2012/01/internet-regulation-and-the-economics-of-piracy/.
7. MPEG, *ISO/IEC 11172, Coding of moving pictures and associated audio at up to about 1.5 Mbit/s* (Geneva, Switzerland: 1993).
8. Simon den Uijl, Henk J. de Vries, and Deniz Bayramogluden, "The rise of MP3 as the market standard: how compressed audio files became the dominant music format," *International Journal of IT Standards and Standardization Research* 11, no. 1 (2013): 1.
9. Brett Atwood, "Oasis in c'right dispute with fans' web sites," *Billboard*, May 24, 1997, 3.
10. Jeffrey Don, "Downloading songs subject of RIAA suit," *Billboard*, June 21, 1997, 3, 83.
11. Doug Reece, "Conference call. The Skinny on Two Upcoming Musical Meetings of Minds and Machines," *Billboard*, Nov 7, 1998, 88.
12. Doug Reece, "Industry grapples with MP3 dilemma," *Billboard*, July 18, 1998, 1, 80.
13. Ibid.
14. Rob Walker, "Between rock and a hard drive," *New York Times*, April 23, 2000, SM74.
15. Bill Holland, "RIAA sues MP3 search site," *Billboard*, Dec. 18, 1999, 9.
16. Amy Harmon, "Potent software escalates music industry's jitter,"

New York Times, March 7, 2000, A1, C6.
17. Matt Richtel, "With Napster down, its audience fans out," *New York Times*, July 20, 2001, A1, C2.
18. David Kravets, "Copyright lawsuits plummet in aftermath of RIAA campaign," *Wired*, May 18, 2010, http://www.wired.com/threatlevel/2010/05/riaa-bump/.
19. Chris Albrecht, "Battling Piracy, BayTSP-Style," *Gigaom*, Oct. 3, 2007, https://gigaom.com/2007/10/03/battling-piracy-baytsp-style/.
20. David Kravets, "RIAA seeks up to $150,000 a song in file sharing trial," *Wired*, July 30, 2009, http://www.wired.com/threatlevel/2009/07/riaa-jugular/.
21. RIAA, "SDMI - Frequently Asked Questions," *RIAA*, last modified Jul 31, 1999, http://www.riaa.com/newsitem.php?id=FCB17200-1028-F1F0-7F41-8BDB994C9022.
22. Ben Rothke, "Doomed to Fail: The Secure Digital Music Initiative," *Information Systems Security* 10, no. 3: 16. For more information on the dispute regarding the SDMI hacking contest, visit the website at URL http://sip.cs.princeton.edu/sdmi/.
23. Leonardo Chiariglione, "Opening Content Protection," *Chiariglione.org*, last modified Aug. 12, 2014, http://ride.chiariglione.org/opening_content_protection/opening_content_protection.htm.
24. Robert Thompson and Tom Ferguson, "Copy-Protection Curtailed," *Billboard*, Dec. 16, 2006, 27.
25. Brad Stone, "Copy an iTunes Song? Go Ahead, Apple Says," *New York Times*, Jan. 7, 2009, B1.
26. Olivier Bomsel and Heritiana Ranaivoson, "Decreasing Copyright Enforcement Costs: The Scope of a Graduated Response," *Review of Economic Research on Copyright Issues* 6, no. 2 (2009): 13-29.
27. Trisha Meyer, "Graduated Response in France: The Clash of Copyright and the Internet," *Journal of Information Policy* 2, (2012): 107-127.
28. Brett Danaher, Michael D. Smith, Rahul Telang, and Siwen Chen, "The Effect of Graduated Response Anti-Piracy Laws on Music Sales: Evidence from an Event Study in France," *Social Science Research Network*, Jan. 21, 2012, http://dx.doi.org/10.2139/ssrn.1989240.
29. Nick Suzor and Brian Fitzgerald, "The Legitimacy of Graduated Response Schemes in Copyright Law," *University of New South*

Wales Law Journal 34, no. 1 (2011): 1.
30. Felipe Romero Moreno, "Incompatibility of the Digital Economy Act 2010 subscriber appeal process provisions with Article 6 of the ECHR," *International Review of Law, Computers & Technology* 29, no. 1 (2014): 81-97.
31. Charn Wing Wan, "Three Strikes Law: A Least Cost Solution to Rampant Online Piracy," *Journal of Intellectual Property Law & Practice* 5, no. 4 (2010): 232-244.
32. Peter K. Yu, "The Graduated Response," *Drake University Law School Florida Law Review* 62 (2010): 1373-1430.
33. Annemarie Bridy, "Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement," *Oregon Law Review* 89 (2010): 81.
34. Thierry Rayna and Laura Barbie, "Fighting Consumer Piracy with Graduated Response: An Evaluation of the French and British Implementations," *International Journal of Foresight and Innovation Policy* 6, no. 4 (2010): 294–314.
35. Annemarie Bridy, "ACTA and the Specter of Graduated Response," *American University International Law Review* 26, no. 3 (2011): 559-578.
36. Eldar Haber, "The French Revolution 2.0: Copyright and the Three Strikes Policy," *Harvard Journal of Sports & Entertainment Law* 2, no. 2 (2011): 297.
37. Yu, "The Graduated Response."
38. Suzor and Fitzgerald, "The Legitimacy of Graduated Response Schemes."
39. Bridy, "ACTA and the Specter of Graduated Response."
40. Moreno, "Incompatibility of the Digital Economy Act 2010."
41. Bomsel and Ranaivoson, "Decreasing Copyright Enforcement Costs."
42. Wan, "Three Strikes Law."
43. Bridy, "Graduated Response and the Turn to Private Ordering."
44. Bridy, "ACTA and the Specter of Graduated Response."
45. Mary LaFrance, "Graduated Response by Industry Compact: Piercing the Black Box," *Cardozo Arts & Entertainment Law Journal* 29, (2012): 238.
46. Anne Barron, "'Graduated Response' à l'Anglaise: Online Copyright Infringement and the Digital Economy Act 2010," *Journal of*

Media Law 3, no. 2 (2011): 305-347.

47. Meyer, "Graduated Response in France."
48. Danaher, et al., The Effect of Graduated Response.
49. Rebecca Giblin, "Evaluating Graduated Response," *Columbia Journal of Law & the Arts* 37 (2013): 147-209.
50. For more information on the French graduated response program, visit the HADOPI website at the URL http://www.hadopi.fr/.
51. For more information on the Korean Copyright Commission, visit their English-language site at the URL http://eng.copyright.or.kr/.
52. For more information on the implementation of the New Zealand graduated response program, visit their website at the URL http://www.med.govt.nz/business/intellectual-property/pdf-docs-library/copyright/notice-process.
53. For more information on the United Kingdom graduated response program, visit their website at the URL http://stakeholders.ofcom.org.uk/internet/terms-of-reference.
54. For more information on the Irish graduated response program, visit the Eircom website at the URL http://www.eircom.net/notification/legalmusic/intro, and the IRMA website at the URL http://www.irma.ie/piracy_faq.htm#grc.
55. For more information on the Taiwanese graduated response program, visit the TIPO website at the URL http://www.tipo.gov.tw/en/AllInOne_Show.aspx?path=2557&guid=26944d88-de19-4d63-b89f-864d2bdb2dac&lang=en-us.
56. For more information on the United States graduated response program, visit the CCI website at the URL http://www.copyrightinformation.org/.
57. For updates on the development of graduated response programs around the world, visit the WIPO website in the section for Internet Intermediaries and Creative Content (URL http://www.wipo.int/copyright/en/internet_intermediaries/index.html) and visit the Global Censorship Chokepoints website at the URL https://global-chokepoints.org/countries/.

References

Albrecht, Chris. "Battling Piracy, BayTSP-Style." *Gigaom*, Oct. 3, 2007. https://gigaom.com/2007/10/03/battling-piracy-baytsp-style/.

Atwood, Brett. "Oasis in c'right dispute with fans' web sites." *Billboard*, May 24, 1997, 3.

Barron, Anne. "'Graduated Response' à l'Anglaise: Online Copyright Infringement and the Digital Economy Act 2010." *Journal of Media Law* 3, no. 2 (2011): 305-347.

Bomsel, Olivier and Heritiana Ranaivoson. "Decreasing Copyright Enforcement Costs: The Scope of a Graduated Response." *Review of Economic Research on Copyright Issues* 6, no. 2 (2009): 13-29.

Bridy, Annemarie. "ACTA and the Specter of Graduated Response." *American University International Law Review* 26, no. 3 (2011): 559-578.

Bridy, Annemarie. "Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement." *Oregon Law Review* 89 (2010): 81.

Chiariglione, Leonardo. "Opening Content Protection." *Chiariglione.org*. Last modified Aug 12, 2014. http://ride.chiariglione.org/opening_content_protection/opening_content_protection.htm.

Danaher, Brett, Michael D. Smith, Rahul Telang, and Siwen Chen. "The Effect of Graduated Response Anti-Piracy Laws on Music Sales: Evidence from an Event Study in France." Jan. 21, 2012. http://dx.doi.org/10.2139/ssrn.1989240.

den Uijl, Simon, Henk J. de Vries, and Deniz Bayramogluden. "The rise of MP3 as the market standard: how compressed audio files became the dominant music format." *International Journal of IT Standards and Standardization Research* 11, no. 1 (2013): 1.

Don, Jeffery. "Downloading songs subject of RIAA suit." *Billboard*, June 21, 1997, 3, 83.

Elton, Serona. "Graduated responses to online piracy: Approaches taken in the United States and around the world." In *Music and Law (Sociology of Crime, Law and Deviance, Volume 18)*, edited by Mathieu Deflem. Bingley: Emerald Group Publishing Limited, 2013. 37-58.

GAO. Intellectual Property: Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods. Washington,

D.C.: GPO, 2010.
Giblin, Rebecca. "Evaluating Graduated Response." *Columbia Journal of Law & the Arts* 37 (2013): 147-209.
Haber, Eldar. "The French Revolution 2.0: Copyright and the Three Strikes Policy." *Harvard Journal of Sports & Entertainment Law* 2, no. 2 (2011): 297.
Harmon, Amy. "Potent Software Escalates Music Industry's Jitters." *New York Times*, March 7, 2000, A1, C6.
Holland, Bill. "RIAA Sues MP3 Search Site." *Billboard*, Dec. 18, 1999, 9.
Kravets, David. "Copyright lawsuits plummet in aftermath of RIAA campaign." *Wired*, May 18, 2010. http://www.wired.com/threatlevel/2010/05/riaa-bump/.
Kravets, David. "RIAA seeks up to $150,000 a song in file sharing trial." *Wired*, July 30, 2009. http://www.wired.com/threatlevel/2009/07/riaa-jugular/.
LaFrance, Mary. "Graduated Response by Industry Compact: Piercing the Black Box." *Cardozo Arts & Entertainment Law Journal* 29, (2012): 238.
Meyer, Trisha. "Graduated Response in France: The Clash of Copyright and the Internet." *Journal of Information Policy* 2, (2012): 107-127.
Moreno, Felipe Romero. "Incompatibility of the Digital Economy Act 2010 subscriber appeal process provisions with Article 6 of the ECHR." *International Review of Law, Computers & Technology* 29, no. 1 (2014): 81-97.
MPEG. *ISO/IEC 11172, Coding of moving pictures and associated audio at up to about 1.5 Mbit/s*. Geneva, Switzerland: 1993.
Porter, Eduardo. "The Perpetual War: Pirates and Creators." *New York Times*, Feb. 5, 2012, SR.10.
Rayna, Thierry and Laura Barbie. "Fighting Consumer Piracy with Graduated Response: An Evaluation of the French and British Implementations." *International Journal of Foresight and Innovation Policy* 6, no. 4 (2010): 294–314.
Reece, Doug. "Conference call. The Skinny on Two Upcoming Musical Meetings of Minds and Machines." *Billboard*, Nov. 7, 1998, 88.
Reece, Doug. "Industry grapples with MP3 dilemma." *Billboard*, July 18, 1998, 1, 80.

RIAA. "SDMI - Frequently Asked Questions." *RIAA*. Last modified July 31, 1999. http://www.riaa.com/newsitem.php?id=FCB17200-1028-F1F0-7F41-8BDB994C9022.

Richtel, Matt. "With Napster Down, its Audience Fans Out." *New York Times*, July 20, 2001, A1, C2.

Rothke, Ben. "Doomed to Fail: The Secure Digital Music Initiative." *Information Systems Security* 10, no. 3 (July 2001): 16.

Sanchez, Julian. "SOPA, Internet regulation, and the economics of piracy." *Ars Technica*, Jan. 18, 2012. http://arstechnica.com/tech-policy/2012/01/internet-regulation-and-the-economics-of-piracy/.

Siwek, Stephen. "The True Cost of Sound Recording Piracy to the U.S. Economy." *The Institute for Policy Innovation*, Aug. 21, 2007. http://www.ipi.org/ipi_issues/detail/the-true-cost-of-sound-recording-piracy-to-the-us-economy.

Stone, Brad. "Copy an iTunes Song? Go Ahead, Apple Says." *New York Times*, Jan. 7, 2009, B1.

Suzor, Nick and Brian Fitzgerald. "The legitimacy of graduated response schemes in copyright law." *University of New South Wales Law Journal* 34, no. 1 (2011): 1.

Thompson, Robert and Tom Ferguson. "Copy-Protection Curtailed." *Billboard* 118, no. 50 (Dec 16, 2006): 27.

Walker, Rob. "Between Rock and a Hard Drive." *New York Times*, April 23, 2000, SM74.

Wan, Charn Wing. "Three strikes law: a least cost solution to rampant online piracy." *Journal of Intellectual Property Law & Practice* 5, no. 4 (2010): 232-244.

WIPO. *WIPO Study on the Economic Contribution of the Copyright Industries*. Geneva, Switzerland: 2012, 1.

Yu, Peter K. "The Graduated Response." *Drake University Law School Florida Law Review* 62 (2010): 1373-1430.

Serona Elton, Esq., is an Associate Professor, Director of the Music Business & Entertainment Industries Program, and Chair of the Music Media & Industry Department at the University of Miami Frost School of Music. She is the President of the Music and Entertainment Industry Educators Association (MEIEA), serves on the Recording Academy, Florida Chapter Board of Governors, and serves on the Copyright Society of the U.S.A. Advisory Council. She also works for Warner Music Group as a Business Relationship Manager, has consulted for other music companies such as Sony Music Entertainment, and has published numerous articles about the music industry. Previously, she worked for EMI Recorded Music, holding a number of positions including Vice President, Mechanical Licensing, and Repertoire Data Services.