

Comments of the
THE SOFTWARE & INFORMATION INDUSTRY
ASSOCIATION

in Response to the Inquiry on
Copyright Policy, Creativity, and Innovation in the
Internet Economy

by

The Department of Commerce's Office of the Secretary, United
States Patent and Trademark Office, and National
Telecommunications and Information Administration

[Docket No. 100910448-0448-01]

December 9, 2010

The Software & Information Industry Association ("SIIA") respectfully submits these comments in response to the Notice of "Inquiry on Copyright Policy, Creativity, and Innovation in the Internet Economy" published in the Federal Register (75 Fed. Reg. 61,419) on October 5, 2010.

SIIA is the principal trade association of the software and information industry and represents over 500 companies that develop and market software and digital content for business, education, consumers, the Internet, and entertainment.¹ One of SIIA's primary missions is to protect the intellectual property of member companies, and advocate a legal and regulatory environment that benefits the entire industry. Consistent with these goals, for over twenty years SIIA's Anti-Piracy Division has conducted a comprehensive, industry-wide campaign to fight software and content piracy.

¹ A list of the more than 500 SIIA member companies may be found at:
<http://www.sii.net/membership/memberlist.asp>.

The success of the software and content industries depend on a meaningful international framework to protect the industries' intellectual property. The U.S. software and content industries are among the fastest-growing and most important industries of the U.S. and world economies. However, this rapid and significant growth is threatened by the pervasive amounts of piracy and general disrespect for the rights of copyright owners. It threatens the livelihoods of companies that create and distribute these products and services, stifling their ability to increase investment, hire additional employees and make and distribute new and existing copyrighted works.

Copyrighted works must be protected against piracy and other unauthorized online distribution. No industry can compete with free-by-theft distribution of its own products. Online piracy threatens the legitimate commercialization of copyrighted works by driving out lawful distribution channels with access to the very same, but illegal, content. There is a critical need for an effective enforcement regime that deters piracy and counterfeiting, while encouraging investment, innovation and employment.

Unfortunately there are no "silver bullet" solutions to these piracy problems. There are practical limitations on the ability of copyright owners to adequately combat the problems. Copyright owners often not only lack sufficient resources to adequately combat the problem but they also often lack sufficient information about the extent and source of the piracy. Moreover, because these infringers are continuously devising new ways to engage in piracy and to avoid detection, it is exceedingly difficult, and often impossible, for copyright owners to meaningfully combat this piracy alone. The best way to effectively address these large-scale piracy problems is through the cooperation of multiple stakeholders, including Federal, state and local government agencies and intermediaries who provide financial transaction and ad placement services or facilitate online commerce through their auction or classified ad sites.

Please find below our answers to the questions posed in the Federal Register Notice. Because many of the questions focused on specific details within a more general topic (*e.g.*, counter-notices, data collection, collaborative approaches), rather than repeating our answers we grouped these questions together by subject matter. If you have any questions or require additional information please contact Keith Kupferschmid, SIIA's Senior Vice President for Intellectual Property Policy and Enforcement at (202) 789-4442 or keithk@siia.net.

Category 1

Rights Holders: Protection and Detection Strategies for Online Infringement

What are stakeholders' experiences and what data collection has occurred related to trends in the technologies used to engage in online copyright piracy, and what is the prevalence of such piracy? What new studies have been conducted or are in-process to estimate the economic effects of this piracy? What assumptions are made in such studies on the substitution rates among the different forms of content?

The large-scale theft of copyrighted works undermines incentives to produce and distribute new software and information products and services. More tangibly, a 2009 report by economist Stephen E. Siwek concluded that theft of copyrighted works costs the U.S. economy \$58 billion in total output.² According to the Organization for Economic Co-Operation and Development (OECD), international trade in physical counterfeit and pirated goods was as high as \$250 billion in 2007. However, the report explains that, if the “significant volume of pirated digital products being distributed via the Internet” were included in the damage calculation, “the total magnitude of counterfeiting and piracy worldwide could well be several hundred billion dollars more.”³

According to Outsell Inc., informational content is illegally distributed at least 56 billion times per year, just by U.S. corporate workers alone, causing substantial monetary losses by the content industry.⁴ Attributor has also done studies on the piracy of digital content, such as books, magazines and newspapers.

Newspapers: In its November 2010 graduated response trial study,⁵ Attributor identified more than 400,000 unlicensed full copies⁶ across 44,906 sites from 70,101 online news articles from newspapers. A similar study on the illegal copying of newspaper articles was done by the Fair Syndication Consortium during a 30-day period in 2009. The study found that more than 75,000 sites reused 112,000 unlicensed newspaper articles.⁷

Magazines: The Attributor study of magazine piracy⁸ estimates that there are more than 2,000 domains (cyberlockers and torrents) that host infringing copies of magazines.⁹ During a one-week period in March 2010, Attributor monitored all issues of 133 English-language magazines on 20 sites and found 3,996 instances of downloadable, full issues of all 133 magazines.

² See Stephen E. Siwek, *Copyright Industries in the U.S. Economy, 2003-2007 Report*, 2009, available at <http://www.iipa.com/pdf/IIPASiwekReport2003-07.pdf>. at i, 11-13 (hereafter Siwek Report).

³ See OECD Study on “*The Economic Impact of Counterfeiting and Piracy*,” June 2007 available at http://www.oecd-ilibrary.org/science-and-technology/the-economic-impact-of-counterfeiting-and-piracy_9789264037274-en;jsessionid=2kpekoss8qmvcs.delta

⁴ Software & Information Industry Association, *Software and Information: Driving the Knowledge Economy* (January 24, 2008) at 39, available at <http://www.siiia.net/estore/globecon-08.pdf>. (hereafter “SIIA Report”)

⁵ See Attributor report at <http://www.fairsyndication.org/blog/2010/graduated-response-trial-unmasks-a-cooperative-internet/>.

⁶ A ‘full copy’ was defined as containing more than 80 percent of the original article and comprising more than 125 words.

⁷ See <http://fairsyndication.org/guidelines/USnewspapercontentreusementudy.pdf>

⁸ See http://attributor.com/docs/MagazineResearch_Attributor_April2010.pdf.

⁹ An infringement was defined as a full-issue copy of a magazine that is available for download.

Books: Attributor's study of book piracy¹⁰ covering 1,000 books of various genres found that over 9 million pirated books were downloaded, representing potential losses of \$2.75-3 billion to the book publishing industry. The study estimates that online book piracy represents roughly 10% of total U.S. book sales and that, on average, about 10,000 copies of every book published are downloaded for free. According to the study, business and investing, professional and technical and science books are being pirated the most and may be losing over \$1 million per title to online book piracy.

The economic impact of piracy does not just affect the companies that produce and distribute copyrighted works.¹¹ It adversely affects:

Consumers. Consumers feel "taken" when they buy software, content or any other product only to find out that it's a fake. This diminishes consumer confidence in the legitimacy of software and content purchased online. Using pirated software and content is also risky business for consumers. It increases the chances that the software will not function correctly or will fail completely and increases the user's risk of catching a debilitating virus that can destroy valuable data.¹² Users of this illegal software often forfeit access to customer support, upgrades, technical documentation, training, and bug fixes and have no warrantee to protect themselves.

Federal State and Local Governments. The Siwek report concluded that that theft of copyrighted works costs Federal, state and local governments \$2.6 billion in lost tax revenue.¹³ They lose not only from copyright owners not paying taxes on revenue they never made because of piracy, but also to those who profit from the piracy.¹⁴

¹⁰ See http://www.attributor.com/docs/Attributor_Book_Anti-Piracy_Research_Findings.pdf.

¹¹ Siwek Report at p. 3 (stating the "economic impact of copyright piracy is not limited to companies that design, create and sell copyrighted works. The impact of piracy flows throughout the U.S. economy. Piracy in one segment of the economy can affect other industries because the economy is an interdependent system.")

¹² See Ashlee Vance, *Chasing Pirates: Inside Microsoft's War Room*, New York Times (Nov. 6 2010) at p. 4 available at <http://www.nytimes.com/2010/11/07/technology/07piracy.html> (stating that Microsoft studies have shown that 35 percent of the counterfeit software they find contains harmful code) (hereafter *Chasing Pirates*).

¹³ Siwek Report at i, 11-13.

¹⁴ See Verne Kopytoff, *IRS urged to go after eBay sellers / Tax experts say online auctions should report users' gross sales* (February 24, 2007) available at http://articles.sfgate.com/2007-02-24/news/17230503_1_national-taxpayer-advocate-ebay-online-sales. (stating that "[w]hen it comes to paying income taxes, eBay's legions of small-time entrepreneurs are on an honor system in which they are supposed to declare their profits to the Internal Revenue Service. Many users, however, ignore the law or are unaware of their obligation. Now a growing chorus of tax experts is hoping to crack down on the cheating by requiring eBay -- and other online auctions, such as those on Yahoo, Ubid.com and Amazon -- to track users and report their gross sales to the federal government. Armed with such information, the IRS could better seek any taxes owed, potentially reaping millions of dollars in extra revenue for the U.S. Treasury.")

Workforce. The Siwek report concluded that that theft of copyrighted works costs the about 375,000 jobs.¹⁵

Businesses. Even those businesses that do not produce or distribute copyrighted products or services make revenue that is directly or indirectly tied to the copyrighted works being pirated (*e.g.*, test centers that are administering copyrighted tests or the company using software to run its business). These unrelated, often small and medium sized, businesses are also adversely affected by piracy.

In addition to the harm to the U.S. economy, piracy causes numerous other harms, such as the harms caused to:

Society. Rampant online copyright infringement contributes to a culture of lawlessness online and has created a generation that fails to respect the hard work, innovation and creativity of others. It is simply too easy to anonymously make, obtain and distribute illegal copies of copyrighted works today. Otherwise honest people who would never consider stealing a CD or book from a store have no problem stealing the digital equivalent that is illegally available online. Should this trend continue it will severely limit the growth of electronic commerce as companies may decide that it just too risky to invest in the digital distribution business models.

Connectivity. Online piracy leads to vast amounts of unlawful traffic that clogs the Internet. It slows service to legitimate users and jeopardizes the ability of broadband networks to handle increased Internet traffic. It is estimated that peer-to-peer file sharing applications represent over 20% of the total bytes that pass through the Internet and 17% of the bandwidth used during peak hours.¹⁶ The top 1% of subscribers account for 25% of total Internet traffic, and 40% of the upstream traffic; more than 46% of top subscribers' traffic comes from file-sharing applications – which primarily contain pirated movies, music, software and content.¹⁷

Mobility. Mobile applications are not immune from piracy. It is estimated that 75% of all mobile applications are pirated.¹⁸ Many of these mobile applications are produced by small entities or recent college graduates who are trying to make a living creating and marketing their new applications. Piracy makes that a difficult, if not impossible, undertaking because unlike larger companies these creators do not have the resources to bear the brunt of piracy or to adequately protect themselves against piracy.

¹⁵ Siwek Report at i, 11-13.

¹⁶ Sandvine, 2009 *Global Broadband Phenomena*, Oct. 2009 at 6, 9, available at <http://current.com/1diai4c>

¹⁷ *Id.* at 14-15.

¹⁸ Garrett W. McIntyre, *Apple App Store Has Lost \$450 Million To Piracy* (January 13, 2010) available at <http://247wallst.com/2010/01/13/apple-app-store-has-lost-450-million-to-piracy/>.

Some of these harms are simply not possible to precisely measure. However, this fact does not mean that the harm is not real and substantial. The impact on our economy and society is undoubtedly severe.

There are also many non-economic harms associated with software and content piracy. It is rare that we encounter a pirate who is not also engaged in some other illegal (and often dangerous) activity. Studies have also shown a nexus between piracy, organized crime and terrorism.¹⁹ Moreover, many pirates operate sites that expose users to viruses, identity theft, malware, phishing and other types of consumer fraud or health and safety concerns. For example:

Health and Safety Issues. Health and safety issues don't just arise in counterfeit pharmaceutical or car part cases. They also arise in software and content piracy cases. Take for example, the case of Adam Perahia, a pediatrician who was sentenced to two years in prison for copyright infringement and child pornography. An initial investigation by SIIA into Perahia's involvement in an electronic message board group, which provided pirated copies of medical textbooks and other copyrighted medical info, led investigators to seize Perahia's computer. The computer hard drive contained pirated medical textbooks that contained medicine dosage charts. Perahia incorrectly copied the dosage charts, which resulted in some of the charts listing fatal dosage amounts. After seizing the computer, Federal authorities made an even more disturbing discovery of a cache of child pornography.

Identity Theft. Jeremiah Mondello, formerly a college student from the University of Oregon, was sentenced by a U.S. District Court in Oregon on charges of copyright infringement, aggravated identity theft and mail fraud. Mondello received a sentence of 48 months in Federal prison, three years supervised release following jail time, and 150 hours of community service per year. Mondello's personal computers and \$220,000 in cash were also seized. SIIA began investigating the eBay seller later discovered to be Mondello in 2007. Using data collected by SIIA's proprietary Auction Enforcement Tool, SIIA identified Mondello through his eBay seller ID and determined there were many more additional eBay identities that likely were being used by Mondello. SIIA then referred all of its case information to the Department of Justice's (DOJ) Computer Crimes and Intellectual Property Section (CCIPS) and the Department of Homeland Security's (DHS) U.S. Immigration and Customs Enforcement Cyber Crime Center -- where investigators were able to determine that Mondello was not only using a handful of falsified identities -- but also created more than 40 fictitious seller IDs. He did so by recording and stealing peoples' bank account information through a keystroke logger that he distributed over the Internet. He then used that information to set up false PayPal accounts using fictitious seller names. By creating these fake seller IDs, he was able to artificially inflate his

¹⁹ See Film Piracy, Organized Crime, and Terrorism, The RAND Corporation (2009) available at http://www.rand.org/pubs/monographs/2009/RAND_MG742.pdf. See also Chasing Pirates at p. 1 at <http://www.nytimes.com/2010/11/07/technology/07piracy.html>.

relatively high standing in the eBay marketplace, which he then used to attract sales and deliver the pirated goods.

Drugs and Weapons. Nathan Peterson, was the owner and operator of iBackups – a site that sold pirated software over the Internet, incorrectly claiming it was “backup software” (*i.e.*, legal copies of software to be used by the software licensee for backup in case of a system crash). SIIA alerted the FBI of the software piracy by Peterson and subsequently worked with investigators and prosecutors to assure that Peterson’s operation was stopped and that he was properly punished. While on bond in this case Peterson was convicted in Los Angeles for the sale of six handguns and an illegal assault weapon to an alleged heroin dealer. He was later sentenced to 87 months in prison for his copyright crimes and ordered to pay restitution of \$5,402,448 and a \$250,000 punitive fee.

As illustrated by these few examples, some of the largest and most damaging counterfeiting and piracy problems take place on auction sites and other commercial websites. The sale of pirated software and content on these sites is especially harmful because it not only hurts those companies that are being pirated, but it also reduces consumer confidence in the legitimacy of purchasing software and content online. Consumers may feel they are buying legitimate software and content only to find out that they have been bamboozled by an online seller who has sold them illegal products.

Because these types of piracy cases involve consumers who are trying to do the right thing by buying legal product and are willing to pay money for the products, these cases of commercial piracy are especially harmful to the software and information industries as these consumers would very likely have purchased legitimate products had the illegal products not been so easily available. Thus, the substitution rate for pirated products bought on these auction sites, classified ad sites and other commercial websites is extremely high.

Similarly, websites like Scribd, DocStoc and Test King are likewise havens of content piracy. These sites allow consumers to search for the content they wish to access, often allowing access to full copies of pirated books, magazines, tests and other copyrighted documents. While these sites may differ from the aforementioned commercial websites in that pirated works are not being sold, they still cause significant damage to content owners by allowing users to post thousands of illegal articles, reports, tests and other illegal content. Piracy of tests and testing materials is of special concern because such piracy threatens to destroy the integrity of the tests, the test takers and those administering the tests. Not to mention the impact this can have on the professions that have chosen to administer these tests to individuals as entry to a specific trade or profession.

Another significant problem of somewhat recent vintage is caused by sharehosting sites, also commonly referred to as “cyberlocker,” “one-click hosting” or “file hosting” sites. These are sites, such as Rapidshare, SendSpace and MegaUpload, that provide Internet hosting services specifically designed to provide storage for files, typically, very large files such as movies, music, software, games, books, etc. Most of these sites simply provide a website address (URL) which can be given out freely to other users who can then access the file at a later point in time. Because of their ease of use and anonymity, sharehosting sites have become a haven for software and content piracy. Unlike the sites mentioned previously, these sharehosting sites do not allow

for users to search for materials by name. The only way to access content stored on these sharinghosting sites is to have the exact URL of the file (made available initially only to the user who uploaded the content). However, there exist communities of consumers who have created “indexing” websites that archive and continually update URLs that lead to the illegal content downloads (e.g., RapidLibrary.com). Piracy on sharehosting sites has quickly become one the most pervasive and damaging types of piracy.

What technologies are currently used to detect or prevent online infringement and how effective are these technologies?

Prevention: Software and content companies use various technological solutions, or Digital Rights Management (DRM) solutions, to protect their copyrighted works from infringement. DRM is essential to protect copyrighted works from piracy and to encourage widespread distribution of copyrighted works. DRM systems enable copyright protection, distribution, usage and payment for digital content such as text, music, images or software via any electronic medium. Importantly, the use of effective DRM systems provides the requisite security to encourage copyright owners to look beyond the risks posed by piracy and make their digital works available to the public. Without such systems, copyright owners would likely be unwilling to make their digital works as widely available as they are today.

The functionality provided by these technological protection systems basically fall into three categories:

Access Control Functions: These functions control the user’s right of entry to the protected content, e.g., encryption and/or authentication.

Use Control Functions: These functions control how the user can interface with the protected content, e.g., read-only rights (the user is unable to print, save or distribute the content).

Tracking Functions: These functions allow the content provider to track the subsequent use and/or distribution of its content online, e.g., watermarking and digital footprints.

As the chart below demonstrates, within each category of protection system, there are varying degrees of protection.

Types of Protection

| Type of Protection | Level of Protection | | |
|--------------------|-------------------------------------|---------------------------------|---|
| | High Level | Medium | Low |
| Access Controls | Encryption | Subscription | Registration/Password/Click-through Agreement |
| Use Controls | Read-only | Read & Print Rights | Full Access |
| Use Tracking | Watermarking/ Digital Footprints | Online/Electronic Clearinghouse | Voluntary User Compliance |

A technological protection system may include one or more of these functions. For example, a certain technological protection system may incorporate password access controls and read-only use controls to prevent wrongful access and wrongful re-distribution of the protected product. To some extent access control and use control functions may also be overlapping. For instance, access controls also serve as use controls since a user who does not have access to the content may not use it.

Depending on the level of protection afforded by the DRM, it may be quite easy or very hard to circumvent. For example, many businesses implement subscription services to be able to control the duration of the use and the distribution of the content. However, in some cases, infringers have found ways to obtain stolen credit cards to purchase subscriptions and then resell the stolen license keys. Many software companies use product activation to discourage copyright infringement. However, many skilled hackers develop cracked serial keys and offer duplicate keys through crack sites online.

Copyright owners are very cautious about using DRMs to protect their products. Often the more powerful and effective a DRM solution is at preventing illegal activity the more cumbersome it is for legitimate, law-abiding customers to use. No DRM is 100% effective. It is often said that DRMs simply make help keep honest people honest. If someone is determined to circumvent or hack a DRM to pirate a copyrighted work then they will probably be able to do it. These are some of the factors that a copyright owner must consider when deciding whether and what type of DRM to use.

Detection: In addition to using DRM to help prevent infringement, SIIA and its members also use different technologies to detect infringement online. SIIA targets piracy of participating members' products on a wide range of Internet protocols, including websites, auction sites, classified ad sites, P2P networks, Torrent and FTP sites, sharehosting sites and other forms of electronic distribution on the Internet. SIIA staff monitors these protocols through both automated and manual means, using a variety of criteria, including, but not limited to, file size, filenames and their contextual location to generate a list of potential pirated sites. When searching for illegal content SIIA and our members may simply copy a word string from a copyrighted article and search for it using Google to see who and how the content is being used online. There are also various organizations, like iCopyright and Attributor, that will "fingerprint" entire documents for copyright owners and then use their automated search tools to search the Internet for illegal copies and uses.

Is litigation an effective option for preventing Internet piracy?

Litigation against infringers is not an effective option for preventing piracy primarily because it is only effective at preventing future potential piracy by the defendant-infringer. It does not prevent that infringer from engaging in the infringement at the outset and thus, only comes into play once harm has already been caused. Litigation is also costly, time consuming and can take a long time to get resolved. Further, there are so many individual infringers that it is simply not practical to sue all of them and, even if it were, many of them reside outside the court's jurisdiction, making litigation impossible.

Another problem with litigation is that it is usually not possible to identify or locate the infringer. Infringers posting pirated products rarely identify themselves or provide accurate names or addresses. This is often true even when the infringer is selling pirated products on commercial sites like eBay, iOffer and Amazon. Even though a site where the infringement is taking place may be willing to turn over the infringer's contact information, the information is often inaccurate and not useful. As a result, SIIA faces a significant challenge enforcing its members copyright on these sites because such false contact information severely limits SIIA's ability to pursue these egregious offenders.

Even when the identity and location of the infringer can be determined and we are able to sue, in many cases, the defendant-infringer is often judgment proof (*i.e.*, financially insolvent and incapable of paying for the resulting damage). Frequently the pirate has long since spent the money made from the piracy and it cannot be recovered by the rights owner. To add insult to injury, not only are the rights owners harmed by the damages caused by the pirate, but in these instances they are also out additional money resulting from the significant attorneys fees and court costs that are incurred to sue the defendant.

There is often no way to know that the defendant is judgment proof before a civil case is brought by the copyright owner. In this instance the copyright owner is in a no-win situation. The options are to either let the piracy continue and continue to incur damages or to bring a civil suit. While the infringement will eventually stop, it will cost the rights owner a significant amount in court costs and attorneys fees.²⁰

If a civil case is brought against a pirate and the defendant turns out to be judgment proof, we may forward the information we have about the case to a Federal or state agency and request that they bring a criminal case against the defendant so that the defendant receives some penalty for his crimes. However, these agencies are generally unwilling to take a case against a defendant once the defendant has been sued civilly by the rights owner for the same acts – even when there is a court record clearly establishing infringement and intent in the civil proceeding.

In addition, because of the limited resources, the vast number of piracy cases, the length of time it takes to bring a criminal case, threshold requirements for cases and other factors, there are practical limits to the number of potential criminal cases that we forward to the Federal and state agencies and that these agencies can pursue.

While our strong preference is to litigate against direct infringers, where a substantial amount of infringement is taking place on a particular site there is also the possibility of pursuing litigation against that site for the infringing acts of its users under theories of secondary liability. However, many of the aforementioned limitations continue to apply. It is costly, time consuming, takes years to get relief, and many sites lie outside the jurisdiction of U.S. courts. In addition, over the past several years U.S. courts have limited the doctrine of secondary liability to such an extent that is extremely difficult for sites to be found liable – even when the site is predominantly used to facilitate piracy and the site operators know that to be the case.

²⁰ Although the copyright law allows attorneys fees and court costs to be recovered in certain instances, if the defendant is judgment proof it will be impossible to collect them.

These comments should not be construed to suggest that that litigation has no role to play in enforcement efforts, because it does. Through its Anti-Piracy Litigation Program (ALP), SIIA regularly sues the most egregious infringers who are attempting to sell pirated software and content on commercial sites like eBay, iOffer, Craigslist and Amazon. The program was designed to establish a greater level of deterrence for pirate and/or counterfeit software sellers on auction sites and other ecommerce sites because the then-current strategy of sending takedown notices was having little effect. We file numerous lawsuits each month. Given the volume of indisputable evidence of infringement that SIIA has in each of these cases, the cases tend to settle quickly with the infringers paying an average damage award of about \$15,000 and an agreement to cease selling the pirated software or content.

In addition, SIIA regularly works with various Federal and state agencies to combat software and content piracy. SIIA works closely with agencies such as the Department of Justice, the Federal Bureau of Investigation (FBI), the Department of Homeland Security, the U.S. Postal Service and other Federal and state agencies to protect SIIA member companies' copyrighted software and content. SIIA routinely forwards cases involving criminal copyright infringement to these agencies.

Consistent with free speech, due process, antitrust, and privacy concerns, what incentives could encourage use of detection technologies by online services providers, as well as assistance from payment service providers, to curb online copyright infringement?

Copyright owners have no hope of succeeding in reducing the staggering level of piracy unless they get more cooperation from intermediaries, like ISPs, ecommerce sites, payment processors, and advertising networks. This is especially true where copyright owners are unable to use their own self-help measures such as with sites in jurisdictions that can't be reached through normal channels. This goal can be accomplished through voluntary and/or involuntary means and through the imposition of penalties and liability for failure to act or incentives to encourage action. Our strong preference is for the intermediaries to get more involved in the fight against piracy through voluntary incentives and not through involuntary imposition of penalties.

In *Perfect 10, Inc. v. Visa International Service Ass'n*,²¹ a divided panel of the Ninth Circuit held that Visa/MasterCard and several banks and data processing services were not, as a matter of law, contributorily or vicariously liable for copyright infringement by virtue of use of their cards to pay for infringing material available through various websites. However, even if copyright liability might not compel credit card companies to address piracy matters, concerns about tarnishment of their brands by association with illegal activity and their ability to recover debts incurred for illegal activity might be sufficiently compelling. This seems to be the case in other areas of illegal activity. For example, many major credit card companies appear to have programs of policing the Internet for certain violations of their rules, such as sites engaged in child pornography.²²

²¹ 494 F.3d 788 (9th Cir. 2007).

²² Visa (as well as American Express) testified at congressional hearings concerning child pornography that they employed web crawling technology to monitor websites for child pornography. See *Deleting Commercial Pornography Sites from the Internet: The U.S. Financial Industry's Efforts to Combat This Problem*, Hearing

The Federal and/or state governments have been involved in many prominent successful cases that entailed enlisting the aid of credit card companies to help prevent illegal activity. We see no reason why the Government should not explore means of enlisting the support of the payment card industry and other payment processing companies and ad placement services for copyright infringements as well.

One possible approach would be to enable the U.S. Department of Justice to bring *in rem* actions against domain names associated with Internet sites that sell pirated and counterfeit goods to enjoin the use of the domain name, and to serve the resulting court order on an ISP, domain name registrar and/or registry, payment processors and other financial transaction providers, and advertising placement services to stop them from transacting business with these domain names that peddle pirated and counterfeit goods and services.

SIIA believes that this approach could greatly extend our reach and ability to thwart piracy – especially illegal operations taking place on foreign websites. A pervasive problem for software and content companies is the online sale of pirated and counterfeit software and content, frequently hosted in foreign countries where copyright enforcement is impracticable. The sites selling the offending software and content typically accept major credit cards as payment. These sites divert potential paying customers from legitimate resellers and may be perceived as having a patina of legitimacy deriving in part from their acceptance of credit cards.

Another potential option would be to provide rights holders with the ability -- not unlike that provided under the notice and takedown provisions of the DMCA – to notify a credit card company or payment processing company of an instance of online piracy or counterfeiting that accepts payment using a company’s credit card and request that the company terminate its relationship with the site. While not stopping the piracy, it would make it harder for pirates to profit from their activities and remove the aura of legitimacy that pirates enjoy by presenting established payment processor trademarks on their sites. If credit card companies are concerned about their liability if they terminate a merchant, similar to the DMCA, the law can provide them with immunity from any liability that might result from such termination. A similar approach can also be used with ad placement services.

There are many other steps that the Federal Government can take to encourage – or the very least not discourage – cooperation between copyright owners and intermediaries. One such step is to ensure that rules or regulations relating to “Network Neutrality” clearly allows for ISPs and content owners to proactively implement technological measures to protect against the theft of copyrighted works.

Can commenters make any generalizations about the online business models that are most likely to succeed in the 21st century, as well as the technological and policy decisions that might help creators earn a return for their efforts? (Again, keeping in mind free speech, due process and privacy concerns.)

Before the Subcomm. on Oversight & Investigations of the H. Comm. on Energy & Commerce, 109th Cong. 71-72 (2006) (statement of Mark McCarthy, Senior Vice President, Public Policy, VISA U.S.A., Inc.) (“McCarthy Statement”); Christenson Statement at 55.

Perhaps the most significant change taking place in the software industry, and the one that will potentially have the largest affect on piracy, is the movement to the Software as a Service model (SaaS), or On-Demand computing model. Whether described as SaaS, On-Demand or Cloud Computing, the new business model is now successfully followed by many large and small, on-demand native firms. Under the On-Demand model, software is not distributed through an enterprise-license, nor is the software installed and run on an individuals' workstation. Instead, the application resides remotely on the vendor's servers and is licensed per seat or by usage on a monthly basis, with a renewable contract for a year or two. The utility-based business model is common with services as diverse as cell phone service and electricity.

At this early stage it is not possible to determine to what extent the On-Demand model will effectively address existing piracy concerns or what new piracy challenges might be created by the On-Demand model. Presently, On-Demand companies use different, but related, means for tracking piracy. The use of IP addresses to track improper usage and comparing named users to concurrent users are two such ways.

Similarly, the content industry also struggles to combat circumvention of DRM and password sharing. These illegal acts present a significant risk not only to copyright owners, but also to the uninterrupted use and access by legitimate customers and a potential risk to customer computer networks. For example, one growing problem facing copyright owners of online content is the misuse or theft, and subsequent trading or sharing, of institutional login credentials for access to the content owners' entire online databases licensed to well known academic institutions. In addition to potentially enabling distribution of pirated materials on a massive scale, this unauthorized access compromises the legitimate accounts and systems of the major educational institutions whose credentials are misused or stolen

What challenges have the creative industries experienced in developing new business models to offer content online and, in the process, to counteract infringing Internet downloads and streaming? How can government policy or intellectual property laws promote successful, legitimate business models and discourage infringement-driven models? And, how can these policies advance these goals while respecting the myriad legitimate ways to exchange non-copyrighted information (or the fair use of copyrighted works) on the Internet?

The Internet has permanently changed the relationship between users and the software and information industries. Electronic commerce has provided users with more options, more alternatives and more opportunities than ever before. The richness and inherent value of electronic commerce and high-tech products to consumers is derived from the wide availability of software and content and the ease by which these products and services can be realized by people using new high-tech products. For users of products and services that incorporate software and/or information, electronic commerce facilitated through licensing provides a robust new delivery channel. By using the Internet to deliver software and digital content, users can take advantage of the lower transaction costs, simplified delivery systems, direct interaction with the provider, and minimal time-to-market.

This has resulted in consumers now having unprecedented choice, convenience and access to informational, as well as creative, content and new high-tech products that simplify their lives. Today's consumers benefit from access to a range of software and information products — the likes of which have never been seen before.

But these benefits do not come without certain risks and problems. One of the most significant is the risk of copyright infringement. The fact that everyone can be a publisher means that everyone can also be an infringer. And because it is so easy for the public to access software and content, these infringements can often have a significant adverse affect on the value of the software and content and the ability of the publisher to continue making their products available online.

It is one thing to battle rival publishers for eyeballs, but it's another thing entirely for a publisher to compete against itself. And that is exactly the dilemma caused by online piracy. For instance, many publishers try to create new revenue streams by licensing their content to online sites exclusively or on a limited basis. This has proven difficult, however, because the very same content they are trying to license is available illegally on numerous sites and potential licensees are reluctant to pay for content to draw users to their sites when the content they are licensing is so widely available. Similarly, just as publishers in the past (and present) draw readers to their print publications through their content, these publishers are now attempting to draw readers to their websites. Instead of (or, in addition to) making money through print ads associated with the content, they attempt to recoup their investments by surrounding the content with banner ads on their website. But it's difficult for these publishers to make this business model work when their content appears illegally on other sites which causes less traffic to their site.

People will be able to take advantage of new technologies and business models only to the extent that the laws do not inhibit the creation and use of new technologies and business models. If the law creates undue burdens on providers that raise transactional costs, without producing any corresponding tangible benefits to users, in the end, only the users' interests will be harmed. This is especially true where the legal requirement on the provider is one that the user cares little about or has the ability to secure in the absence of any legal requirement.

For instance, the average person who licenses software and informational products does not decide whether to license a product or service based on whether they can make a back-up copy of the product, transfer the product or take advantage of some other exception in the copyright law. In reality, the person will ultimately decide whether to purchase a product or service based on factors such as price, compatibility, or brand loyalty.

There is an incentive for publishers of information products to try to extend the audience for their products through a pricing strategy called price differentiation - that is, through charging different prices for the same or very similar information to different users or to users seeking different packages of information. Software publishers use a similar strategy to make their products more widely available by distributing educational and OEM versions of their software. However, these publishers will not be able to extend the audience for their products through price differentiation unless copying and resale are controlled through adequate statutory protection that does not impinge upon the principle of freedom of contract.

Fortunately for users, market dynamics and the law are already working to ensure that the only business practices that will survive in the long-term are those that balance convenience, price and consumer protections. As users become more educated and aware of their choices, businesses that do not effectively respond to online user preferences and interests will simply fade away. In response to user demand, publishers have created many different types of licenses, which vary greatly depending on the customer needs. Such licenses include, site licenses, pay-per-use licenses, click-through agreements, and “true-up” agreements, to name just a few. Similarly, in response to customer demand, publishers have also joined together through collective licensing arrangements, such as that provided by the Copyright Clearance Center (CCC), to create a type of one-stop-shop where licensees are allowed to use any works from a vast collection of works owned by participating publishers. This business model is especially effective in today’s technology-driven economy where each individual use of a work may not be of sufficient value to warrant effort on the part of either rights holder or user to negotiate a unique license.

Software and information publishers are able, through licensing to meet customer needs – whether the general public or discrete customer groups – and at the same time protect against misuse of their rights. If undue restrictions are placed on either the ability of those publishers to license or the manner in which publishers license, they may be less willing to widely distribute their products and services to the public. This is especially true with mass market click through agreements. Certain informational products can only be distributed freely through the use of license terms and conditions. If these terms could not be enforced these products may not be distributed, and in some cases, the incentive to create certain products may have been so reduced that these new products would never have been created.

The software and information industries have long relied upon licenses for the mass market distribution and use of their products. Licenses provide the substantial legal framework for the industry. There are many reasons for this, including the typically ongoing nature of the relationship between publisher and customer, including support, maintenance, bug fixes, updates, and upgrades. Licenses have been the standard regardless of the media on which software and information products are distributed – whether floppy disc, CD, or even no media at all (Internet download). And licenses have allowed software and information publishers the flexibility to tailor their products to its various customers, adjusting features, benefits, rights, and price according to the needs of each customer base rather than a “one size fits all” model – a model which logically could require a higher price. Consequently, more often than not these licenses provide benefits to consumers not provided by copyright law.

The software and information industries have been built almost exclusively upon a business model of licensing. For decades there had been virtually no question about the legal enforceability of these licenses and, accordingly, the terms therein. Many courts accepted the status of the transaction as a “license,” rather than a sale, as obvious on its face. Other courts provided deeper analysis and justification. *See, e.g., ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996) (Easterbrook, J., discussing why the terms of the shrinkwrap license at issue were enforceable); *Wall Data Inc. v. Los Angeles County Sheriff's Dep't*, 447 F.3d 769, 775-76, 785 n.9 (9th Cir. 2006); and most recently *Vernor v. Autodesk*, 621 F.3d 1102 (9th Cir. 2010) (first sale defense not applicable to licensed software being sold on eBay because software license specified that the user was granted a license, significantly restricted the licensee’s ability to transfer the software; and imposed notable use restrictions). Hundreds of cases enforced software licenses, and the few that did not turned on deficiencies in facts, not a different legal

approach.²³ See, e.g., *Novell, Inc. v. Network Trade Center, Inc.*, 25 F.Supp.2d 1218, 1222 (D. Utah 1997) (first sale defense applied to upgraded software in that case because Novell provided the upgrades without any license restrictions, thereby making them sales and subject to the first sale doctrine); *Krause v. Titleserv, Inc.*, 402 F.3d 119, 124 (2d Cir. 2005) (consultant who left engagement with defendant could not assert ownership of source code he wrote for defendant, because defendant had the right to continue using the software at all times and without any limitations, even after the consulting/development engagement expired).

The economic foundations of the software and information industries depend upon its licensing business model. “Overriding” such licenses would have far-reaching, adverse effects on everything from the availability of educational software and content, to warranties and support services, to the development of new products. It is therefore essential that the basic principle of freedom of contract be recognized and preserved by any copyright legislation. As a general rule, nothing in the law should restrict the rights of parties to enter freely into licenses or any other contracts with respect to the use of copyrighted works. Parties should retain the freedom to structure an agreement as they desire, with some exception (such as provisions relating to consumer protections). This is more important now than ever before because in an increasingly digital knowledge economy it is almost certain that software and information publishers will make their products and services available subject to critical contractual terms.

In addition to ensuring the continued vitality of the system of copyright licenses under copyright and other commercial laws, there are several steps the Government can also take with regard to domain names and websites that can help combat online piracy. First, when the Government takes action against an online pirate it ought to shut down the website immediately and replace it with a notice explaining why the website was taken down. This will serve as an educational tool to those who may access the site looking for pirated works and educate those that may have been unaware that the enterprise was illegal. In many cases this does happen, but it needs to happen in every instance.

Second, when a website is taken down as part of a criminal case and the primary purpose of the website is for making available pirated or counterfeit goods, the Government should seek an order from the court requiring registrars or registries to keep the domain name for the offending website out of circulation for at least five years. For example, SIIA has been working with the Government to pursue pirates who had been engaging in several massive software piracy schemes through various eBay accounts and various websites, such as SoftwareDiner.com and Fivedollarsoftwarehouse.com. SIIA initially discovered several massive software piracy schemes and began an investigation. SIIA forwarded the results of its investigation to the U.S. Department of Justice and other government agencies, and then worked closely with them to pursue the pirates who operated the sites. The pirates involved in this scheme duped nearly 8,000 unsuspecting consumers out of hundreds of thousands of dollars and cheated software companies such as Adobe, Symantec, Apple, Corel, Intuit and many others out of millions of dollars in revenue. On February 26, 2009, one of the pirates, Matthew Purse, was sentenced to 21 months in Federal prison, 3 years probation and \$12,000 in fines and restitution for conspiracy, mail fraud and criminal copyright infringement. His accomplice, Chris Walters, was

²³ The one known exception (until the recent Ninth Circuit trio) is *Softman Products Co. v. Adobe Systems Inc.*, 171 F. Supp.2d 1075 (C.D. Cal. 2001). The case was simply wrongly decided, and was not followed by other courts, even within the Ninth Circuit.

a fugitive for about a year but was apprehended earlier this year and is scheduled for trial early next year. Although the Government took down the SoftwareDiner.com site, they did not seize it. As a result, it was subsequently obtained by another group that is now using the domain name to sell pirated software. This type of activity should not be permitted to occur.

Third, currently copyright owners can use the DMCA to take down a site offering infringing goods. However, it is fairly easy for a site to return under the same domain name but through a different ISP. There are some steps that the Federal Government can take to potentially prevent this from occurring. For example, the Federal Government could manage a centralized database of DMCA takedown notices and provide ISPs with access to this database. The ISP could automatically check this database before agreeing to host a new website. Therefore, if the pirate attempts to re-post the website using the services of a different ISP, the ISP could first automatically check the database and reject the attempt. Search engines and others could also be granted access to this database to prevent the domain name from being sold as a search term. This would help prevent a pirate's whose website has been taken down by an ISP from creating the same website under a different domain name and then trying to direct traffic to the new website through sponsored ads on search engines using the old domain name as a search term. Of course, these steps would require the voluntary cooperation of the ISPs, search engines and others.

Fourth, it is essential that the Federal Government continue to ensure that public access to Whois data is preserved. Public access to Whois data²⁴ is essential to the investigation and prompt resolution of online piracy and counterfeiting. The data includes contact information on the registrant of Internet domain names, as well as data on administrative and technical contacts, and leads for identifying the entity hosting the content on World Wide Web sites associated with the domain. When such misconduct is associated with a particular IP address, Whois enables the investigator to identify the ISP or other entity to which the IP address was initially assigned, and also to learn of sub-allocations to other providers, though rarely, if ever, to the end-user. Without this data it would be virtually impossible for rights owners to successfully pursue these cases of online piracy and counterfeiting.

It is essential that U.S. policy continue to make the preservation and enhancement of this vital tool a priority.²⁵ The investigation of virtually every case of piracy involves the use of Whois data. For example, when an investigator seeks to determine who is responsible for a website where infringing activity is taking place, a review of the Whois data for the domain name which resolves to that site is usually the first step. This data is essential not only to law enforcement, but it is also relied upon by private parties (including copyright and trademark owners) whose independent enforcement of their rights allows law enforcement to conserve scarce resources.

²⁴ "Whois data" refers to information about the allocation of blocks of Internet Protocol (IP) addresses (the numeric addresses for all resources connected to the Internet).

²⁵ U.S. enforcement policy should also recognize that the Whois Data was collected for a wide variety of purposes, including combating fraud, promoting confidence in doing business on the Internet, and enforcement of intellectual property laws by the private sector. As such, *Whois data has always been collected and made available to the public primarily for the purpose of enabling contact with the operators of online resources to which domain names resolve (with respect to domain name Whois) or with the network operators to which an IP address has been allocated or sub-allocated (in the case of IP Address Whois)*. Since IP Whois address information by itself cannot identify any end-user, other than in exceptional cases, public access to such data has little if any impact on privacy or free expression concerns.

The U.S. Government can preserve public access to Whois in three main ways, depending on the type of domain name registration involved:

- With regard to generic Top Level Domains (gTLDs), such as .com, .net, or .info, public accessibility of Whois depends on the terms of contracts between the registrars (and registries) and the Internet Corporation for Assigned Names and Numbers (ICANN). Through its participation in the ICANN Governmental Advisory Committee, the USG should continue to advocate for reliable, accurate, and real access to Whois Data.
- With regard to country code Top Level Domains (ccTLDs), such as .uk, .fr, and .de, ICANN plays almost no role on Whois, the U.S. has entered into free trade agreements with several countries that set baseline standards that our trading partners pledge to maintain in the ccTLDs allocated to each country. These standards include providing public access to reliable and accurate contact information on domain name registrants. The U.S. Government must continue to seek inclusion of these provisions in future agreements, and ensure that existing commitments are fully implemented.
- With regard to the .us ccTLD, Whois policy is set by the National Telecommunication and Information Administration (NTIA) of the U.S. Department of Commerce. NTIA should continue to ensure that existing policy regarding Whois is maintained and that information in the .us database is accurate and up-to-date.

We strongly urge that the Report by the PTO-NTIA Internet Task Force include a reaffirmation of the U.S. Government's policy of reliable, accurate, publicly accessible and timely Whois Data.

Category 2

Internet Intermediaries: Safe Harbors and Responsibilities

What are stakeholders' experiences with the volume and accuracy of takedown notices issued for allegedly infringing content across the different types of online services (i.e., storage, caching, and search) and technologies (e.g., P2P, cyber lockers, streaming, etc.)? What processes are employed by rights holders to identify infringers for purposes of sending takedown notices?

SIIA monitors for piracy of participating members' products on a wide range of Internet protocols, including websites, auction sites, classified ad sites, P2P networks, Torrent and FTP sites, sharehosting sites (i.e., cyberlockers) and other forms of electronic distribution on the Internet. SIIA and its members use different technologies and procedures to detect infringement

and identifying infringers which are largely dependent upon the type of protocol where the infringement is taking place.

SIIA staff monitors these protocols through both automated and manual means. We use various software services to scour the Internet for pirated software and content on these protocols using various factors to weigh the likelihood of whether the software or content being made available is illegal. We evaluate the results and send out DMCA takedown notices and cease-and-desist letters accordingly. When sending a takedown request, we subsequently follow up to confirm that the illegal products, auction, link or site has been taken down and has not been re-posted. We also have a team of investigators that monitors specific sites that are most problematic to SIIA's members. These investigators are versed in various languages in order to give us the ability to monitor both domestic and international sites.

We also receive hundreds of online piracy reports daily from the public through our online reporting forms (at <http://www.siiia.net/piracy/report/report.asp>); via email (at piracy@siiia.net) and through our anti-piracy hotline (at (800) 388-7478). These reports come from buyers and potential buyers of software and content products who may have been defrauded by online sellers and often have physical evidence of the piracy and specific information about the seller and piracy.

In addition to reports from consumers, we also routinely receive piracy reports directly from SIIA members. Often consumers will have problems with the pirated software and content they bought online and will contact the software or content publisher for assistance. For example, the defrauded buyer may attempt to register their copy of the software only to find out they cannot because the copy is illegal and the registration number is invalid. A buyer may also call the company for customer support and find out that they are ineligible because their copy is a pirated version.

A few of the indicators that we use to help us spot illegal software and content being offered online include:

Price: If the price is too good to be true, it probably is. For example, \$20 for a \$200 retail-priced product. As a general rule, if there is more than a 20% discount on the Manufacturer's Suggested Retail Price (MSRP) without rebates, then there is a significant risk that the seller is selling illegal software or content.

Seller's Reputation: On auctions listings, we check the seller's reputation, including their user comments and whether they have any neutral/negative feedback from buyers claiming fraud by the seller.

Other Sales/Auctions by the Seller: We check the seller's other auctions and online sales. When the seller has placed 10, 20 or more auctions for the exact same piece of software or content, it is often an indicator that the person is selling pirated software or content.

Seller's History: We check the seller's history. If the seller just recently appeared and started selling massive amounts of the same piece or set of software or content products this may indicate, along with other factors, that they are selling illegal software or content.

Seller's Location: We check the location of the seller and whether they are offering product from another region of the world. In addition to the potential for piracy, the buyer could be lured into purchasing software that will be incompatible for their computer or may be unlicensed for distribution in the United States or, in the case of content, the buyer may be purchasing content that may not have information as current as the U.S. version, may be of lower print and/or image quality, or may be written in another language entirely. Many foreign sellers will attempt to mask their location to appear as though they are U.S.-based sellers. We check the seller's information (such as bidding currency, language used, etc) to help us assess the true location of the seller. If the seller is lying about their location, this may indicate, along with other factors that they are also selling illegal software or content.

Auction Length: Most auctions last from five to seven days. Auctions for less than that - one and three day auctions - are often posted by those selling illegal software and content who are trying to make a quick sale before the copyright owner takes down their auction.

Special Activation or Registration Process: If the seller provides a special number or procedure for activating or registering the software or content before the buyer can use it, the product is almost certainly illegal. The same is true when the seller states that the product cannot be registered.

Sale Text: Warning signs that may appear in the text of the auction or classified ad:

- The software or content is being offered at a price well below the retail price.
- The software is identified as "OEM" and is not bundled with authorized hardware.
- The content is being sold on a hard drive ("HDD") or other media storage device. Content is never legally sold in this manner directly to consumers.
- The software is being sold as a "back-up copy."
- Offers for software of "brand new CD in sleeve," not in a box.
- Offers of "beta," pre-release or NFR ("not for resale") versions.
- The software or content is being sold as a compilation. For example, multiple products from different publishers on the same CD, multiple years of a magazine, multiple editions of a textbook, or an entire class preparation—often using language such as "everything you need to complete this course!" Legal software and content is rarely, if ever, sold that way.
- Offers of academic versions of software that do not state the eligibility requirements.
- The software is advertised as a "full version," but the auction states that you will only receive CDs.

Downloadable Products: In addition to many of the factors listed above, when the software or content is downloadable we look at other factors, such as file size, filenames and their contextual location.

All these criteria, and more, are contained in SIIA's software and content buying guides, which can be found on SIIA's website, eBay, Craigslist, SIIA-member sites and various other online locations. SIIA publishes these guides to help online buyers identify pirated software and

content. The guides teach buyers the tricks used by unscrupulous sellers to lure them into buying illegal software and content and instruct them on questions to ask so they can avoid buying illegal copies.

For cases in which we only send a DMCA takedown notice to ISP or ecommerce site we may not take any steps to uncover the true identify of the infringer. However, when we contact the pirate directly by a cease-and-desist letter or by filing a lawsuit we use various means for determining the identity of the pirate. These include:

- Making a personal information request upon the intermediary or ISP
- Using the WHOIS database (as discussed above)
- Hiring outside investigators
- Using various software and other technical online tools, such as the U.S. Postal Services online address database, to search for the pirate's identity and location.

(As noted throughout this submission, however, often times the information we get from these sources is not accurate.)

***What processes do Internet intermediaries employ in response to takedown notices?
Are Internet intermediaries' responses to takedown notices sufficiently timely to limit
the damage caused by infringement?***

Each sites has its own process for responding to takedown notices. Often this process is set forth in the terms and conditions for use set forth on the website, which may require sellers' and sometimes other users' consent before using the site. The procedures differ greatly from one site to another. Regardless of the actual policies and procedures adopted by each of these sites our experience has been that these policies and procedures may not be fully implemented. For example, it is a violation of eBay's terms and conditions for eBay sellers to include incorrect contact information and those who fail to correct the information are subject to sanctions by eBay, including being banned from the site.²⁶ Before sending a cease-and-desist letter to an eBay seller we will submit a personal information request to eBay to obtain the seller's contact information. If this information is incorrect and we are unable to contact the seller we will often notify eBay that the seller is unreachable due to eBay's incorrect information and request that eBay either obtain and provide us with the correct contact information or immediately terminate the seller's account. Despite the terms and condition requiring sellers to provide eBay with their correct contact information, we are not aware of any instance of a seller's account being terminated for having incorrect contact information and have never been provided with the correct contact information in response to our requests.²⁷

This past year, SIIA conducted a study designed to gather information regarding the responsiveness of intermediaries to our DMCA takedown notices. One of the goals of this study

²⁶ See <http://pages.ebay.com/help/policies/identity-misrepresentation.html> and <http://pages.ebay.com/help/policies/identity-false.htm>.

²⁷ It is possible that eBay did take action but simply unable or unwilling to disclose to us whether they have complied.

was to determine the accuracy of contact information for intermediaries as provided in the U.S. Copyright Office's list of DMCA Designated Agents.²⁸ The SIIA sent email notifications to the list of DMCA Designated Agents and requested that they confirm that they are the correct point of contact for receiving and responding to DMCA takedown notices for specific intermediaries identified on the designated agents list.²⁹

The results of this study show that there are major issues with accuracy in the contact information currently available on the U.S. Copyright Office's list of designate agents. We found that slightly less than half of all email addresses contacted were returned as "undeliverable" (*i.e.* they no longer existed). Of the remaining that were deliverable:

- 76% were non-responsive (*i.e.*, no specific response to SIIA's request was received). In about half of these cases we received an auto-response acknowledging receipt of the email but nothing more.
- 24% were completely responsive to SIIA's request (*i.e.*, directly confirmed in a separate email that they were the correct point of contact for receiving DMCA takedown notices). Of those that were responsive, 95% responded within 24 hours of receiving SIIA's request.

Our study also included an analysis of responses to takedown notices by various Internet intermediaries. Some intermediary responses are sufficiently timely (*e.g.*, eBay, iOffer, Craigslist), while others need to improve (*e.g.*, Amazon, Google).

In SIIA's experience, the Internet intermediaries listed above have been responsive accordingly:

- eBay: Responds within 48 hours over 99% of the time, within 24 hours 90% of the time.
- iOffer: Responds within 48 hours over 99% of the time, within 24 hours 90% of the time.
- Craigslist: Responds within 24 hours 99% of the time.
- Amazon: Responds within 1 week 99% of the time, within 48 hours 75% of the time, 24 hours 25% of the time.
- Google: Responds within 1 month 99% of the time, within 3 weeks 90% of the time, within 2 weeks 80% of the time, within 1 week 50% of the time, within 48 hours 20% of the time, within 24 hours 5% of the time.³⁰

²⁸ Found at http://www.copyright.gov/onlinesp/list/a_agents.html.

²⁹ Because the list spans tens of thousands of entries SIIA was able to reach out to only a small fraction of those listed and then extrapolate the results.

³⁰ There is reason to believe that Google's response time will improve. On December 2nd, Google announced that it will be making changes to be more responsive to copyright infringement and the DMCA's notice

What are the challenges of managing this system of notices?

There are several challenges associated with managing the notice and takedown system.

Volume: The most significant challenge is the sheer volume of takedown requests. Piracy of software and content has risen to such endemic proportions that we cannot possibly monitor for every infringement and cannot send takedown notices for each infringement we find. Further, many intermediaries, like Rapidshare, restrict the number of takedown notices we can send them at one time. This practice is inconsistent with the DMCA safe harbors and also presents significant challenge to managing of notices because, among other things, it requires us to calculate the relative damage caused by each infringement prior to sending the notice.

Timing: It takes us time to detect infringements and time for an intermediary to remove the infringing site or material. If we are fortunate, the time period from detection to takedown will be a day or two. However, as discussed above, often this pendency period may be as long as a month. Any delay in responding to the takedown request may be causing harm to the copyright owner and potentially devaluing the copyrighted work. It is therefore essential that these illegal products be removed or otherwise be made inaccessible “expeditiously” as required by section 512(c) of the DMCA. A delay of anything more than a day or two is unacceptable and a violation of the DMCA.

Each Country And Each Intermediary Has Its Own Procedures: Although the DMCA is not effective outside the United States many other countries have adopted similar approaches. Because SIIA and our members actively enforce their rights on a global basis we must learn and understand the specific requirements for each region. Intermediaries also have their own individual takedown procedures that we must understand. To assist us with this enormous task, we hire vendors and consultants to provide support with setting up these various notices and managing them on an ongoing basis.

Tracking Compliance And “The Whack-a-Mole” Problem: Once a site is taken down, illegal product removed, or an account terminated it is likely that the site, material or pirate resurfaces – almost immediately. It is too easy for a pirate to simply re-register with an intermediary under a different pseudonym and/or address or with a differ credit card in order to remain a fugitive or stay hidden. For more detail see the response below.

The Problem Of Systematic, Judgment-Proof, And “Covert” Or “Fugitive” Pirates That Are Able To Stay Hidden Or Avoid Detection: See response below.

What are stakeholders’ experiences with online copyright infringement by users who change URLs, ISPs, locations, and/or equipment to avoid detection? What challenges exist to the identification of such systematic infringers?

and takedown requests, including acting on takedown requests within 24 hours. See <http://googlepublicpolicy.blogspot.com/2010/12/making-copyright-work-better-online.html>.

One of the biggest problem we have in fighting piracy is the problem of pirates who change domain names, locations, ISPs etc. in order to avoid detection. We can usually identify infringement taking place on the Internet and even track down the infringer. However, those who are in the business of piracy are usually very good at avoiding detection.

There are numerous examples of this. For example, as mentioned above, Jeremiah Mondello, a college student from the University of Oregon who received a sentence of 48 months in Federal prison for copyright infringement stole the identities of at least 40 individuals in order to avoid detection. He did this by recording and stealing peoples' bank account information through a keystroke logger that he distributed over the Internet. Similarly, the defendants in the SoftwareDiner and Fivedollarsoftwarehouse case (discussed above) changed URLs and ISPs numerous times to avoid detection. The defendants mirrored the infringing site to multiple web hosting providers so that when SIIA sent a takedown notice to the ISP, the site would quickly reappear under the prevailing host provider to continue its operations. SIIA traced the defendants' infringing site to web hosting providers in the United States, Japan and finally Germany (where we successfully removed the site). The defendants also avoided detection by registering multiple domains using bogus registrant information.

Within the last few year we have encountered a disturbing new type of piracy problem, which we refer to as the Drop Ship or Mule problem. It occurs when a U.S. citizen is recruited by email or online ads to sell software on eBay or some other online location on behalf of an individual or entity (that we refer to as the "source") that is located abroad (usually in China, Taiwan or Russia). Often, those recruited are just trying to make extra money and don't realize what the source is really getting them to sell is counterfeit software. The source desires many bona fide U.S. seller accounts to sell the counterfeit goods to U.S. consumers in a decentralized way. By doing so the source seeks to avoid a large volume of counterfeit software being sold by any one account to avoid detection himself. The U.S. citizen signs up, agrees to post the listings, and often never sees the goods. A buyer (*i.e.*, the auction winner) sends payment to an account controlled by the source and the source "drop ships" the infringing item directly to the buyer. The U.S. seller simply receives a small royalty check for each listing that produces a sale. This is a type of fraud and counterfeiting that harms not only the rights owner and the buyer of the software but also those who sell legitimate software on the auction site and the so-called "mules" themselves. These sellers are shocked when they receive a takedown notice or a cease-and-desist letter from SIIA or are sued for significant damages resulting from the counterfeiting. When they inform us of the identity of the source there is usually nothing we can do because the source resides abroad, usually in a country with lax copyright enforcement. Once the "mule" receives a notice they usually stop selling the pirated software. However, this hardly stops the problem as the source merely finds other unsuspecting mules to continue the illegal operations.

This problem needs to be addressed through both education of the sellers, which we already do, and through enforcement. This is not your typical copyright crime as there is no way to know who the "mules" are until we proceed civilly against them, they disclose the source of the counterfeit goods and we determine that the source is the supplier in many of our civil cases.

What are stakeholders' experiences with Section 512(i) on the establishment of policies by online service providers to inform subscribers of service termination for repeat infringement?

Often an intermediaries policies regarding the termination of repeat infringers can be vague and nonexistent.

eBay's policy on repeat infringers states: "...we may, in appropriate circumstances and at our discretion, suspend or terminate accounts of users who may be repeat infringers of intellectual property rights of third parties."³¹

While some sites may speak vaguely to termination of accounts, we could not find specific provisions relating to repeat infringer within the policies of the following intermediaries:

Amazon:

http://www.amazon.com/gp/help/customer/display.html/ref=footer_cou?ie=UTF8&nodeId=508088#copyright;

Craigslist: <http://www.craigslist.org/about/terms.of.use#copyright>. or

iOffer: http://www.ioffer.com/info/user_agreement.

Much better is Google's policy, which states: "*Many Google Services do not have account holders or subscribers. For Services that do, Google will, in appropriate circumstances, terminate repeat infringers. If you believe that an account holder or subscriber is a repeat infringer, please follow the instructions above to contact Google and provide information sufficient for us to verify that the account holder or subscriber is a repeat infringer.*"³²

Even when a user is found to be a repeat infringer and their account is terminated by the intermediary the termination has little practical effect because it is much too easy for that same user to create a new account with the intermediary using a pseudonym and other incorrect and/or fraudulent information. More needs to be done by intermediaries to make it more difficult for users who's accounts have been terminated to resurface on the site. For example, we commend eBay for being somewhat responsive to our complaints in this area and taking some additional steps (like requiring a working phone number that eBay calls to confirm the seller can be reached at the number).

Would stakeholders recommend improvements to existing legal remedies or even new and additional legal remedies to deal with infringing content on a more timely basis?

In order to send these cease-and-desist letters or to sue SIIA must obtain seller contact details from the site. However, sellers posting illegal products rarely provide these sites with accurate names or addresses. As a result, even though the sites are willing to turn over the seller's contact information, the information is often not useful. SIIA faces a significant challenge enforcing its members copyright on these sites because such false contact information severely limits SIIA's ability to pursue these egregious offenders.

³¹ See <http://pages.ebay.com/help/policies/user-agreement.html?rt=nc>

³² See <http://www.google.com/dmca.html>

To address this challenge, SIIA began to cross-check the contact information for sellers posting infringing auctions and ads by using a USPS certified web-based program. The goal was to decrease the amount of illegal software and content being sold by getting the accounts of sellers providing false information suspended. SIIA urged the sites to immediately suspend any seller providing incorrect contact information. However, the sites have been either slow or reticent to do this. Further, even where they do suspend the seller it is too easy for the seller to activate a different seller ID and sell under a new fake identity.

We recommend a Federal law be enacted that requires a person who is selling or offering for sale copyrighted or trademarked goods online through a third party for the purposes of commercial advantage or private financial gain to disclose their true name and address to that third party.³³ We believe that this would go a long way to reducing the amount of piracy and fraud on these auction sites, classified ad sites and related sites.

As noted above, another possible legislative approach would be to enable the U.S. Department of Justice to bring *in rem* actions against domain names associated with rogue sites that are dedicated to the sale of pirated and counterfeit goods to enjoin the use of the domain name, and to serve the resulting court order on an ISP, domain name registrar and/or registry, payment processors and other financial transaction providers, and advertising placement services to stop them from transacting business with these domain names that peddle pirated and counterfeit goods and services. An alternative or additional approach would be to make these financial transaction providers and advertising placement services subject to the DMCA's notice and takedown regime so that they would be incentivized to stop transacting business with these pirate sites. Both approaches could greatly extend our reach and ability to thwart piracy – especially operations taking place on foreign websites.

In addition to potential legislation, it is essential that the government increase the amount of funding and resources allocated to combating piracy. Over the past decade the Federal Government has made great strides improving the quantity and types of enforcement activities of the various agencies involved in IP enforcement. Most of these agencies now recognize the severity and significance of the piracy problem and have devoted IP staff and initiatives aimed at addressing it. Nevertheless, piracy continues to be a staggering problem plaguing intellectual property owners. Consequently, the Federal Government must strengthen and improve existing Federal enforcement programs that have proven to be effective, such as:

- *Increasing the Number of IP Attaches:* The IP attachés program³⁴ has become an extremely useful initiative in helping intellectual property owners and other Federal Government agencies protect and enforce intellectual property rights abroad. These IP attachés, which are stationed at American embassies in India,

³³ A somewhat similar approach was taken by the State of California law, which passed a law making it illegal for a person to electronically disseminate a recording or audiovisual work without disclosing their true name and address. 19 Cal. Jur. 3d Criminal Law: Miscellaneous Offenses § 174, Failure to disclose origin of recording or audiovisual work. To be clear, this proposal would not require the seller to disclose their name and address to the buyer but would require them to disclose such information to the auction or related site so that rights owners would be able to locate them if we wanted to send them a cease and desist letter or sue them.

³⁴ See <http://www.uspto.gov/ip/global/attache/index.jsp>.

Brazil, Thailand, the Russian Federation, Egypt, and China have also helped provide assistance on IP issues to law enforcement agencies and judges within these countries. It is our hope that the program will be expanded into other countries as well as deploying an IP attaché to the Organization for Economic Co-operation and Development (OECD).

- *Increase Manpower and Resources Devoted to Intellectual Property Crimes:* The large volume of piracy and counterfeiting cases and the complexity of these cases takes an extraordinary amount of time, money and resources. Additional manpower and resources devoted to anti-piracy is necessary so the government can continue their excellent work and to investigate and pursue a higher volume of IP crimes.
- *Increase Funding for State and Local Enforcement:* State and local enforcement has become increasingly important in the fight against intellectual property-related crime. This is especially true with crimes involving the illegal online trafficking in pirate or counterfeit goods. For instance, SIIA works closely with state and local enforcement to pursue those who sell pirate and counterfeit software on Craigslist. We urge state and local enforcement agencies to continue to work cooperatively with rights owners and the Federal Government, and for the Administration and Congress to support these efforts by funding the states enforcement initiatives. In this regard, we are pleased to highlight the DOJ's recent announcement that the Office of Justice Programs (OJP) would be providing grants totaling over \$1.98 million to state and local enforcement agencies to fund investigation, prosecution, prevention, training, and technical assistance relating to combating intellectual property crimes. The grants can be used to reimburse expenses related to performing criminal enforcement operations; to educate the public to prevent, deter, and identify criminal violations of intellectual property laws; to establish task forces exclusively to conduct investigations and forensic analyses and prosecutions; and to assist in acquiring equipment to conduct investigations and forensic analysis of evidence. While this is a good start we would like to see increased funding devoted to state and local enforcement through this program.

What are stakeholders' experiences with developing collaborative approaches to address online copyright infringement? What range of stakeholders participated in the development of such collaborative approaches? Have collaborative approaches resulted in the formulation of best practices, the adoption of private graduated response systems, or other measures to deter online infringement that can be replicated? What other collaborative approaches should stakeholders consider? How can government best encourage collaborative approaches within the private sector?

SIIA routinely establishes working relationships with intermediaries to collaborate to combat online infringements. For example, SIIA works with iOffer to post customized anti-piracy warning messages on behalf of its member companies. These warning messages serve to educate iOffer sellers and dissuade them from posting illegal software. As an educational tool these messages are quite successful as member companies were able to provide information

within the warning messages that would redirect the seller to their website for product information and to Federal law enforcement for information about cybercrime. SIIA also works with Craigslist and eBay to post SIIA's Software Buying Guides on their respected sites. The Software Buying Guides contain information to assist buyers with purchasing legitimate software on eBay and Craigslist and to also notify sellers of the risks of selling illegal software.

SIIA is also in the nascent stages of establishing a working relationship with an organization that represents all major payment services (*e.g.*, credit card companies) and acquiring banks. We provide the organization with the domain names of sites selling pirated software and content, along with other information obtained when SIIA does a test buy using certain credit cards. The organization then works with the payment services (credit card companies and partner banks) it represents, to stop the use of their credit cards for pirated content on those sites -- usage which invariably violates the terms of the agreements between the site and the payment services. There are several actions the payment services could take, including asking the site owner to remove pirated material, terminating the site's use of the payment services and banks, or other actions. This initiative may prove particularly beneficial in foreign jurisdictions where takedowns and lawsuits often are ineffective.

By cutting off major payment mechanisms for pirated works, this initiative could make it more difficult and less attractive for unscrupulous individuals to profit from piracy (and will increase consumer confidence in the payment mechanisms/cards that respond to piracy concerns). It may also make infringing sites more recognizable to consumers, since they will be forced to use non-traditional payment means. While in its early stages, this initiative has already shown some success as well as a few challenges. The payment mechanisms have been identified for several dozen infringing sites, and in a few cases material was removed, at least initially. On the other hand, identifying the relevant "merchant accounts" (associated payment mechanisms) on other sites remains elusive, even with test buys performed. SIIA is continuing to fine tune the process, and anticipates some continued success as well as challenges.

Category 3

Internet Users: Consumers of Online Works and User-Generated Content

What initiatives have been undertaken to improve the general awareness of Internet users about online copyright infringement and the availability of legitimate sources to access online copyrighted works?

SIIA's mission is to both protect the industry and to inform the public. SIIA has invested in numerous educational initiatives over the years, including:

Educational Videos: In 2008, SIIA created and made available four new educational videos. The videos are entitled:

- *All About Copyright:* Teaches viewers about the copyright law and what they can do to ensure they are using software and content legally.

- *Software Compliance*: Teaches viewers about what constitutes software piracy, what's legal and how to stay within the law.
- *Content Compliance*: Teaches viewers about what constitutes content piracy, what's legal and how to stay within the law.
- *Risk of Infringement*: Teaches viewers about what happens to those who pirate software and content and why it's not worth the risk.

These videos join a stable of older, but still effective, SIIA videos, such as *It Could Have Been So Easy*.

In September 2009, SIIA released the much-anticipated sequel to its 1992 video classic *Don't Copy That Floppy*. The sequel, *Don't Copy That 2*, again features M.E. Hart as "MC Double Def DP" (aka DP or Digital Protector) and can be found at <http://www.dontcopythat2.com>. SIIA launched the *Don't Copy That Floppy* campaign in 1992. The eight-minute video targeted middle school students and was distributed to 20,000 teachers nationwide. The emergence of YouTube and Google Videos gave *Don't Copy That Floppy* a second life online, as the video became a cult phenomenon with more than 1 million YouTube views, new imaginings of the video by viewers and online parodies.

Don't Copy That 2 features DP as he continues his crusade against software and content piracy with the new slogan, "It's not just a copy. It's a crime." When DP discovers a website selling pirated "tunes, games and apps" run by a college student named Jason, he uses a catchy hip-hop song and a startling dream sequence to teach Jason about the costs of engaging in piracy. *Don't Copy That 2* also includes an appearance from convicted software pirate Jeremiah Mondello, who issues a warning about the consequences of software piracy from a Federal prison in Oregon.

Within the first ten days after DCT2's release, it had logged more than a quarter million views on YouTube, and more than a thousand people posted comments about the video. The video has also been a favorite of bloggers and Twitter users around the world, who have made it the subject of hundreds of tweets and postings over that time. In order to reach students with the new campaign, SIIA will soon be releasing a modified and extended educational version of *Don't Copy That 2* that will be distributed to classrooms along with classroom lesson plans.

Compliance Seminars: SIIA offers three compliance seminars – the Certified Software Manager (CSM) seminar, the Advanced Software Manager (ASM) seminar and the Certified Content Rights Manager (CCRM) seminar. The first seminar was the CSM, which was created in 1994. It teaches the skills needed to diagnose, resolve and manage a company's complicated software licensing issues. The CSM educates IT specialists, legal representatives and human resource managers about software asset management procedures, copyright law and license agreements; the software audit process; the benefits and processes of software asset management; and corporate software policies. This includes educating students who enroll in the program about online copyright infringement and the availability of legitimate sources to obtain software.

Due to the success of the CSM and the demand for more software compliance educational programs, in 2007, SIIA and its educational partner LicenseLogic developed the ASM seminar. As a follow-up to the CSM, the ASM facilitates a more in-depth discussion of topics related to understanding software asset management (SAM) and its greater role in an organization, such as: developing an effective and motivated SAM core team; preparing and implementing a successful SAM program; utilizing the latest developments in SAM tools and processes; understanding the latest software licensing trends and the impact those might have on an organization and educating an organization's staff on vendor management and negotiation techniques.

In 2007, SIIA also began teaching a course designed to explain the legal issues surrounding copyright law and how it affects content licensing. This course, entitled Certified Content Rights Manager (CCRM), was designed for professionals who purchase and manage copyrighted content and are responsible for ensuring it is used appropriately at all levels throughout their organization. Among other things, students in the course are taught about online copyright infringement and the availability of legitimate sources to obtain software.

Speeches and Other Educational Resources: SIIA staff routinely give speeches throughout the country to educate anyone who is willing to listen about Internet piracy and the availability of legitimate sources for obtaining and accessing software and content.

SIIA also provides a library of free resources on its website to further educate the public. This includes a copyright compliance toolkit. The kit contains posters that people can hang around the office as a friendly compliance reminder, as well as educational videos. SIIA's goal with this kit and the website is to educate the public about copyright compliance and make it easier to establish and maintain an environment that is conducive to copyright compliance.

As noted above, SIIA also makes available several buying guides to help online shoppers be on the lookout for pirated software and content. These guides can be found on SIIA's website, eBay, Craigslist, SIIA-member sites and various other online locations. Many of SIIA's members also provide excellent videos and other educational materials, including CCC,³⁵ Symantec,³⁶ Intuit³⁷ and Adobe.³⁸

Certification Programs: Lastly, SIIA certifies resellers through its Premiere Reseller Program,³⁹ to help companies and individuals find trusted third parties who can help them comply with the copyright law and software licenses. SIIA also provides links to many of SIIA software members' authorized resellers.⁴⁰ Software purchasers can access the list if they want to be sure to purchase only legal software.

³⁵ See <http://www.copyright.com/viewPage.do?pageCode=pu3-n>

³⁶ See <http://www.symantec.com/about/profile/antipiracy/index.jsp>.

³⁷ See <http://about.intuit.com/piracy/>

³⁸ See <http://www.adobe.com/aboutadobe/antipiracy/>

³⁹ See http://www.sii.net/index.php?option=com_content&view=article&id=83&Itemid=36.

⁴⁰ *Id.*

What are stakeholders' experiences with the awareness and appropriate use by Internet users of the counter-notification mechanism? What are stakeholders' experiences regarding inappropriate use by Internet users of the counternotification mechanism, if any? What are stakeholders' experiences with the volume of counter-notices filed?

SIIA's experiences with counternotices has varied over the years. Shortly after the DMCA was enacted and we began sending DMCA takedown requests we would regularly receive counternotices. These counternotices were often filed merely as a way for the person filing the counternotice to continue to keep their website, auction, ad, or link active and online without regard to whether the underlying action that was the subject of the takedown request was actually legal or not.⁴¹ The people filing these counternotices were educated about the DMCA and understood that the only way for us to respond to the counternotice was to file a complaint within 10 days of receipt of the counternotice. They knew that we were unable to move that quickly in filing a lawsuit, which would have the result of allowing the infringing activity to continue. That changed, however, when we began our Anti-Piracy Litigation Program (ALP) (as explained above). Once we began suing infringers under the ALP program the counternotices generally stopped.

Today, apart from takedown notices that we send to eBay to remove the auction of illegal software or content, we almost never receive counternotices. For takedown notices sent to eBay sellers, we receive counternotices in response to only about 10% of all takedowns notices we send to these sellers. SIIA immediately follows up with those sellers and takes the opportunity to educate them by explaining to them why their auction was illegal. We are usually able to resolve the problem within a matter of hours or days.

What are stakeholders' experiences in foreign countries and on university campuses in reducing online copyright infringement?

SIIA's experience with foreign countries differ greatly depending on the specific country. We have had success in Canada and in many European countries in bringing civil suits to enforce our members' rights against infringers and, more generally, in getting material taken down off websites that reside in those countries. Because the DMCA has no applicability outside the United States, we usually rely on some combination of the country's domestic copyright law and/or the ISP enforcing its own terms and conditions to get the offending material taken down.

Our experiences outside of Canada and Europe differ greatly depending upon the specific country in which the infringement is taking place. It is most difficult to get results through litigation or other self-help measures (such as notice and takedown) against websites residing in China and Russia.

⁴¹ For example, on May 30, 2007, in *FileMaker v. Simpson*, a jury in U.S. Federal District Court in Santa Ana, California concluded that the defendant, Bryan Simpson, had been selling pirated FileMaker software on eBay and awarded FileMaker \$380,000 in damages. The other defendants in the case settled with FileMaker prior to the trial and, as a result paid over \$200,000 in total damages. Simpson conducted over 14,000 eBay transactions and filed over 30 counternotices. The jury found Simpson liable on two counts of willful trademark infringement, two counts of willful copyright infringement, and one count of trafficking in counterfeit labels.

Our experiences with universities also differ depending on the specific university and, more specifically whether the university is a state entity or not. In general, we have found universities have been quite slow in responding to our takedown requests. State universities in particular have proven to be problematic and can take as long as a couple of months to takedown the offending material.

The lag time with State Universities may be in large part due to state sovereign immunity. In 1999, the U.S. Supreme Court in the *Florida Prepaid* decisions,⁴² and the lower court decisions that have followed, created a major loophole in our laws that reduces the effectiveness of our copyright laws by immunizing state entities from monetary damages for copyright infringement. As a result, there is no effective deterrent to prevent states from infringing either intentionally or unintentionally copyrighted software, content and other copyrighted products. If and when state agencies and entities are discovered to be infringing, the best we can hope for is to get them to stop. This is having a detrimental effect on the protection afforded to copyright holders.

The impact on SIIA's members is not a constitutional abstraction. It involves real cases with meaningful financial consequences. During the six years leading up to issuance of the *Florida Prepaid* decision in 1999, SIIA identified at least 77 matters involving infringements by State entities. Of these 77 matters, approximately 50% involved State institutions of higher learning. (The other 50% consisted of State hospitals, bureaus, public service commissions, and other instrumentalities.)

Yet, while state universities are immune to damages for infringing the intellectual property rights of others, they remain free to sue private sector (both for-profit and non-profit) organizations under Federal intellectual property laws for alleged infringements of their patents, copyrights and trademarks and collect damages. State universities are themselves major owners of intellectual property and have benefited from Federal law and policy to achieve this result. States are increasingly seeing their intellectual property as strategic assets and utilizing sophisticated licensing management strategies to commercialize their portfolio.

It is essential that State universities and agencies act as model "good citizens." One concrete step would be to implement executive level policies and procedures that lay out in clear terms that intellectual property must be used and licensed consistent with the requirements of our nation's laws and spirit of respecting the intellectual property of creators. This would include abiding by the terms of any relevant license agreements. State governments need to do more to communicate that message throughout its departments and agencies, and to individual employees.

⁴² In *Florida Prepaid Postsecondary Education Board v. College Savings Bank*, 527 U.S. 627 (1999) the Supreme Court invalidated the Patent and Plant Variety Protection Remedy Clarification Act, a law analogous to the Copyright Remedy Clarification Act (CRCA) in the patent field. The holding in the case has been applied in the copyright context to immunize states from incurring copyright infringement liability.