

**ROLE OF VOLUNTARY AGREEMENTS IN THE
U.S. INTELLECTUAL PROPERTY SYSTEM**

HEARING

BEFORE THE

SUBCOMMITTEE ON
COURTS, INTELLECTUAL PROPERTY,
AND THE INTERNET

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

—————
SEPTEMBER 18, 2013
—————

Serial No. 113-49

—————

Printed for the use of the Committee on the Judiciary



Available via the World Wide Web: <http://judiciary.house.gov>

ROLE OF VOLUNTARY AGREEMENTS IN THE U.S. INTELLECTUAL PROPERTY SYSTEM

ROLE OF VOLUNTARY AGREEMENTS IN THE U.S. INTELLECTUAL PROPERTY SYSTEM

HEARING BEFORE THE SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY, AND THE INTERNET OF THE COMMITTEE ON THE JUDICIARY HOUSE OF REPRESENTATIVES ONE HUNDRED THIRTEENTH CONGRESS FIRST SESSION

SEPTEMBER 18, 2013

Serial No. 113-49

Printed for the use of the Committee on the Judiciary



Available via the World Wide Web: <http://judiciary.house.gov>

U.S. GOVERNMENT PRINTING OFFICE

82-846 PDF

WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON THE JUDICIARY

BOB GOODLATTE, Virginia, *Chairman*

| | |
|---|--|
| F. JAMES SENSENBRENNER, Jr., Wisconsin | JOHN CONYERS, JR., Michigan |
| HOWARD COBLE, North Carolina | JERROLD NADLER, New York |
| LAMAR SMITH, Texas | ROBERT C. "BOBBY" SCOTT, Virginia |
| STEVE CHABOT, Ohio | MELVIN L. WATT, North Carolina |
| SPENCER BACHUS, Alabama | ZOE LOFGREN, California |
| DARRELL E. ISSA, California | SHEILA JACKSON LEE, Texas |
| J. RANDY FORBES, Virginia | STEVE COHEN, Tennessee |
| STEVE KING, Iowa | HENRY C. "HANK" JOHNSON, JR., Georgia |
| TRENT FRANKS, Arizona | PEDRO R. PIERLUISI, Puerto Rico |
| LOUIE GOHMERT, Texas | JUDY CHU, California |
| JIM JORDAN, Ohio | TED DEUTCH, Florida |
| TED POE, Texas | LUIS V. GUTIERREZ, Illinois |
| JASON CHAFFETZ, Utah | KAREN BASS, California |
| TOM MARINO, Pennsylvania | CEDRIC RICHMOND, Louisiana |
| TREY GOWDY, South Carolina | SUZAN DeBENE, Washington |
| MARK AMODEI, Nevada | JOE GARCIA, Florida |
| RAUL LABRADOR, Idaho | HAKEEM JEFFRIES, New York |
| BLAKE FARENTHOLD, Texas | |
| GEORGE HOLDING, North Carolina | |
| DOUG COLLINS, Georgia | |
| RON DeSANTIS, Florida | |
| JASON T. SMITH, Missouri | |

SHELLEY HUSBAND, *Chief of Staff & General Counsel*
PERRY APELBAUM, *Minority Staff Director & Chief Counsel*

SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY, AND THE INTERNET

HOWARD COBLE, North Carolina, *Chairman*
TOM MARINO, Pennsylvania, *Vice-Chairman*

| | |
|---|--|
| F. JAMES SENSENBRENNER, JR., Wisconsin | MELVIN L. WATT, North Carolina |
| LAMAR SMITH, Texas | JOHN CONYERS, JR., Michigan |
| STEVE CHABOT, Ohio | HENRY C. "HANK" JOHNSON, JR., Georgia |
| DARRELL E. ISSA, California | JUDY CHU, California |
| TED POE, Texas | TED DEUTCH, Florida |
| JASON CHAFFETZ, Utah | KAREN BASS, California |
| MARK AMODEI, Nevada | CEDRIC RICHMOND, Louisiana |
| BLAKE FARENTHOLD, Texas | SUZAN DeBENE, Washington |
| GEORGE HOLDING, North Carolina | HAKEEM JEFFRIES, New York |
| DOUG COLLINS, Georgia | JERROLD NADLER, New York |
| RON DeSANTIS, Florida | ZOE LOFGREN, California |
| JASON T. SMITH, Missouri | SHEILA JACKSON LEE, Texas |

JOE KEELEY, *Chief Counsel*
STEPHANIE MOORE, *Minority Counsel*

CONTENTS

SEPTEMBER 18, 2013

| | Page |
|---|------|
| OPENING STATEMENTS | |
| The Honorable Howard Coble, a Representative in Congress from the State of North Carolina, and Chairman, Subcommittee on Courts, Intellectual Property, and the Internet | 1 |
| The Honorable Melvin L. Watt, a Representative in Congress from the State of North Carolina, and Ranking Member, Subcommittee on Courts, Intellectual Property, and the Internet | 2 |
| The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, Ranking Member, Committee on the Judiciary, and Member, Subcommittee on Courts, Intellectual Property, and the Internet .. | 3 |
| WITNESSES | |
| Jill Lesser, Executive Director, Center for Copyright Information | |
| Oral Testimony | 7 |
| Prepared Statement | 9 |
| Cary H. Sherman, Chairman and CEO, Recording Industry Association of America | |
| Oral Testimony | 12 |
| Prepared Statement | 15 |
| Randall Rothenberg, President and CEO, Interactive Advertising Bureau | |
| Oral Testimony | 25 |
| Prepared Statement | 27 |
| Gabriel Levitt, Vice President, PharmacyChecker.com | |
| Oral Testimony | 35 |
| Prepared Statement | 37 |
| Robert C. Barchiesi, President, The International AntiCounterfeiting Coalition | |
| Oral Testimony | 50 |
| Prepared Statement | 52 |
| LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING | |
| Prepared Statement of the Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, Ranking Member, Committee on the Judiciary, and Member, Subcommittee on Courts, Intellectual Property, and the Internet | 5 |
| Material submitted by the Honorable Judy Chu, a Representative in Congress from the State of California, and Member, Subcommittee on Courts, Intellectual Property, and the Internet | 64 |
| Material submitted by the Honorable Doug Collins, a Representative in Congress from the State of Georgia, and Member, Subcommittee on Courts, Intellectual Property, and the Internet | 85 |
| APPENDIX | |
| Material Submitted for the Hearing Record | 121 |

ROLE OF VOLUNTARY AGREEMENTS IN THE U.S. INTELLECTUAL PROPERTY SYSTEM

WEDNESDAY, SEPTEMBER 18, 2013

HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY,
AND THE INTERNET

COMMITTEE ON THE JUDICIARY

Washington, DC.

The Subcommittee met, pursuant to call, at 2:03 p.m., in room 2141, Rayburn House Office Building, the Honorable Howard Coble (Chairman of the Subcommittee) presiding.

Present: Representatives Coble, Marino, Goodlatte, Smith of Texas, Poe, Collins, Watt, Conyers, Johnson, Chu, Jeffries, and Lofgren.

Staff Present: (Majority) Joe Keeley, Chief Counsel; Olivia Lee, Clerk; and (Minority) Stephanie Moore, Minority Counsel.

Mr. COBLE. The Subcommittee on Courts, Intellectual Property and the Internet will come to order. Without objection, the Chair is authorized to declare recesses of the Subcommittee at any time. We welcome all of the witnesses and others in the audience for today's very important hearing I will now give my opening statement.

Good afternoon, and welcome again to today's Subcommittee hearing on the Role of Voluntary of Efforts in the U.S. Intellectual Property System. Copyright owners have been dealing with the increasing acts of power sales of their property that is often aided by groups and Web sites that glorify theft. This Subcommittee has dealt with the issue for some time.

The Congressional Creative Rights Caucus which I Chair with the gentlelady from California, Ms. Chu, has also heard from artists impacted by the outright theft of their works. I am pleased to learn today of the voluntary efforts now underway to reduce piracy. These good works are the result of several companies and trade associations that have invested their time and effort to cultivate best practice principles that help direct consumers to legitimate content while making it more difficult for pirates to operate. These agreements are a step in the right direction. They promote intellectual property, they improve the Internet marketplace for consumers and they have been established through a voluntary process.

I want to especially highlight the efforts by the Center for Copyright Information as an example of what can be done. By letting

ISP customers know about piracy that may be occurring using their Internet connections, ISP's consumers may find that the wireless network has been hacked, or that their teenager needs to join a family meeting about responsible Internet usage. I am also pleased that the Center has taken a thoughtful approach to implementing an appeals system as well as creating an oversight panel of consumer groups.

While much work has been done, more work is required from other groups. I am interested in hearing how existing voluntary agreements can be utilized to foster new agreements in new areas, and if there is anything we can do to help promote the best practices. As most of us know, private sector actions are oftentimes more efficient and effective than some regulation handed down by the Federal Government.

Thank you, again, for being here, and I look forward to hearing the testimony from our witnesses on today's panel.

I am now pleased to recognize the Ranking Member from North Carolina, Mr. Mel Watt for his opening statement.

Mr. WATT. Thank you, Mr. Chairman.

Two years ago, this Subcommittee held several hearings to address possible legislative solutions to the epidemic of online piracy and sale of counterfeit goods over the Internet. Although the Stop Online Piracy Act was itself stopped, the problem of piracy was not, as I have noted on a number of occasions.

We are certainly not here to relitigate SOPA, but I do believe that the SOPA debate we had helped motivate an important shift in the willingness of some parties to engage more aggressively in negotiating to develop some of the best practices we are considering here today.

Indeed, some of the entities that fought vigorously to defeat SOPA are now constructive parties to voluntary agreements designed to combat the drain on our economy and the potential harm to consumers that online piracy and counterfeiting represent.

Over the past 2 years, government entities, nonprofit organizations, academic institutions and industry stakeholders have all issued studies evaluating the problem. Recent examples include the July 2013 Department of Commerce Internet Policy Task Force report on copyright policy, creativity and innovation in the digital economy in which the task force noted "while the extent of the losses caused by online infringement is hard to calculate with certainty, the proliferation of unlicensed sites and services making content available without restriction or payment impedes the growth of legitimate services."

In February, the Administration also reported on the cyber theft of trade secrets, and in May, the Nonprofit Commission on the Theft of American Intellectual Property found that the scale and complexity of the international theft of American intellectual property is unprecedented, including the rapid growth in online sales of counterfeit goods.

Earlier this year, Carnegie Mellon professor Michael Smith released his findings on the impact of the Department of Justice enforcement against the notorious MegaUpload site. In general, Professor Smith suggested that providing legitimate avenues to obtain content online, coupled with effective anti-piracy policies, rep-

resents the best recipe for combating IP theft online. However, yesterday a report entitled “Sizing the Piracy Universe” by NetNames painted a bleak picture regarding Internet-based infringement. The report, commissioned by NBC Universal, found that piracy of entertainment content has increased dramatically despite the growing number of legal options available to consumers.

Google also released a report last Friday entitled “How Google Fights Piracy,” outlining its efforts to curtail piracy and highlighting how its services provide enhanced opportunities for creators. However, this morning the Motion Picture Association of America, together with Chairman Coble and our colleague on the Committee, Ms. Chu, unveiled a study by Compete, “Understanding the Role of Search in Online Piracy,” which reportedly details how search engines like Google introduce consumers to Web sites dedicated to infringement.

The single common thread throughout each of these reports is the recognition that there is an ongoing vulnerability for U.S. intellectual property in the online environment. That threat is not only economic and is not limited to specific industries represented here. Counterfeit hard goods, especially pharmaceuticals, may pose an additional threat to safety risk for American consumers.

Futile efforts to curtail online infringement and counterfeiting does more than deplete the profits of U.S. companies and negatively affect the U.S. economy. It also opens our citizens to a variety of predictable harms like identity theft, fraud, sickness or even death. Failure to address the problem may also make our cyber infrastructure less secure and facilitate individual criminal activity or encourage criminal enterprises.

So it is important that these voluntary agreements and best practices are meaningful endeavors, not just window dressing. It is also important that our values of privacy, free speech, competition and due process are honored. But it is also important that those values are not fraudulently turned against us to invite or justify legislative paralysis.

I applaud the voluntary efforts of the various industry stakeholders both to confront the challenge and to embrace the opportunities that permeate the digital era. While these cooperative measures may or may not be enough, I believe that our Subcommittee, which has jurisdiction over both intellectual property and the Internet, should encourage these collaborations, but it is also our responsibility to consider whether additional oversight or legislative action is warranted as well.

I welcome the witnesses and look forward to the testimony.

Mr. Chairman, I yield back.

Mr. COBLE. Thank you, Mr. Watt.

The Chair now recognizes the distinguished gentleman from Michigan, the Ranking Member for the full Judiciary Committee, Mr. Conyers, for his opening statement.

Mr. CONYERS. Thank you, Chairman Coble, and we join in welcoming our distinguished witnesses today.

Voluntary agreements, intellectual property law, should facilitate technological advances, while at the same time, protecting creators, I think that is what the hearing is all about, and we must continue ways to examine how we can prevent piracy and fight violations of

copyright law. I think that is a worthwhile issue to examine here today in the Judiciary Committee.

Although these voluntary agreements have been a positive step, we must continue to develop solutions to address digital piracy. A primary goal is that we should have to continue to inform and change the behavior of the majority of users who want to enjoy content legally, and I am hoping that these issues will be examined with the care and experience of our distinguished witnesses today.

I will put the rest of my statement in the record. Thank you very much, Chairman Coble.

Mr. COBLE. Thank you, Mr. Conyers.

[The prepared statement of Mr. Mr. Conyers follows:]

Statement of the Honorable John Conyers, Jr.
for the Hearing on the
Role of Voluntary Agreements in the U.S. Intellectual Property System
before the
Subcommittee on Courts, Intellectual Property, and the Internet

Wednesday, September 18, 2013 at 2:00 p.m.
2141 Rayburn House Office Building

The purpose of this hearing is to examine the role that voluntary initiatives have played in protecting copyright in the digital age.

Content is available in many more ways than it was in recent years and this change is affecting how companies participate in the digital marketplace.

We must ensure that illegal activity does not undermine new legitimate technologies. The change in the way that content is available is having an impact on the type of innovation that is happening on the Internet and within the content community.

The voluntary agreements we will discuss today are a step in the right direction. However, I believe more must be done to ensure that products and services are not used in an illegal manner.

First, voluntary agreements and intellectual property law should facilitate technological advances while at the same time protecting creators.

We must make sure that the voluntary initiatives are flexible over time to adopt to the changing marketplace.

One of the most high-profile voluntary agreements that we will discuss today is the Copyright Alert System.

The Copyright Alert System, which was implemented in 2013, provides a way to inform users of their activity. The Copyright Alert System allows copyright holders to notify consumers when their Internet accounts have alleged illegally downloaded and shared copyrighted music, movies or television shows.

I want to hear the witnesses discuss whether the creation of the Copyright Alert System has helped to influence the thinking of consumers about digital piracy. And I am interested to hear whether the Copyright Alert System has also been able to help consumers find content legally.

Second, we must continue to examine ways that we fight violations of copyright law.

The Internet has regrettably become a cash-cow for the criminals and organized crime cartels who profit from piracy.

Piracy is both a domestic and international issue. And, it is an issue that should encourage cooperative efforts between Internet Service Providers (ISPs), payment processors, advertisers and advertising intermediaries, and the movie and music industries.

With an estimated 2 billion people accessing the Internet annually: this translates to a devastating amount of property theft and job-destruction.

In addition, a study by the Institute for Policy and Innovation found that there are \$12.5 billion dollars in losses to the United States economy and more than 70,000 lost jobs annually by American workers due to piracy of sound recordings.

Those are not insignificant statistics.

We need to explore ways to make them even better.

Third, although these voluntary agreements have been a positive step, we must continue to develop solutions to address digital piracy.

I am happy to see that the Copyright Office as well as the Patent and Trademark Office have taken the lead in helping to develop these voluntary agreements.

The IPEC should continue to work with advertisers to establish best practices to reduce advertising revenue from online infringement.

The IPEC should also work internationally with other countries on the development of voluntary initiatives that are in line with United States policy.

I look forward from hearing the witnesses discuss these issues and I encourage all parties to continue to pursue more voluntary agreements in the future.

Mr. COBLE. We have a very distinguished panel today, and I will begin by swearing in our witnesses before introducing them. If you would, please, all rise.

[Witnesses sworn.]

Mr. COBLE. Let the record show that each of the panelists responded in the affirmative.

As I said before, we have a distinguished panel before us, and I am pleased to introduce them now. Our first witness today is Ms. Jill Lesser, Executive Director at the Center for Copyright Information. Ms. Lesser is a long-time consumer protection, technology and copyright expert, and also serves as a board member for the Center For Democracy and Technology. She received her J.D. from the Boston University School of Law, and her B.A. in political science from the University of Michigan.

Our second witness is no stranger on Capitol Hill, Mr. Cary Sherman, Chairman and Chief Executive Officer for the Recording Industry Association of America, the organization representing the Nation's major music labels. Mr. Sherman received his J.D. from Harvard School of Law and his B.S. from Cornell University.

Our third witness today is Mr. Randall Rothenberg, President and Chief Executive Officer of the Interactive Advertising Bureau, a trade association representing over 500 leading interactive companies that are responsible for selling more than 86 percent of on-line advertising in the United States. Mr. Rothenberg received his B.S. in classics from Princeton University.

Our fourth witness today is Mr. Gabriel Levitt, Vice President of PharmacyChecker.com. Mr. Levitt helped found the company in 2002, and is responsible for all business and research operations. Mr. Levitt received his Master's Degree in International Relations from the American University, and his bachelor's degree from Roger Williams University.

Our final witness today, Mr. Robert Barchiesi, is President of the International AntiCounterfeiting Coalition. Mr. Barchiesi received his M.A. from the University of Alabama and his B.A. from the John Jay College of Criminal Justice. It is good to have all of you with us today, gentleman and lady.

There is a timer on the desk that will alert you when your time is waning, rapidly vanishing. We try to employ the 5-minute rule. When the green light on the panel turns to amber, that is your warning that you have 1 minute to wrap up. Now, you won't be keelhauled if you violate that rule, but try to wrap up on or about 5 minutes if you would do so.

Ms. Lesser, we will begin with you. I repeat, it is good to have all of you with us.

**TESTIMONY OF JILL LESSER, EXECUTIVE DIRECTOR,
CENTER FOR COPYRIGHT INFORMATION**

Ms. LESSER. Chairman Coble, Ranking Member Watt, Ranking Member Conyers, and Members of the Subcommittee, my name is Jill Lesser and I am the Executive Director of the Center For Copyright Information. I am pleased to be testifying on the issue of voluntary initiatives aimed at protecting copyright in a digital age, a new area of cooperation and progress in a policy debate that has long been characterized by sharp differences of opinion.

The Center for Copyright Information was established in 2011 as part of a groundbreaking initiative among the Nation's five leading Internet service providers and virtually the entire movie and music industries. The agreement set out to stem the tide of digital piracy by accomplishing two goals: One, establishing the copyright alert system or CAS; and, two, creating an organization that could educate users about the importance of protecting digital content while offering them a better way to find movies, TV and music online safely and legally.

In the two short years since CCI's formation, we have successfully implemented the Copyright Alert System and have begun a series of educational efforts aimed at helping users make better choices about the way they enjoy creative content. Still in its early stages, this initiative illustrates the importance of multi-stakeholder, market-driven solutions, and more generally serves as a model for addressing challenging technology policy issues through collaboration.

I have addressed the negotiations that led to the creation of CCI in my written testimony. Therefore, I will focus here on CCI's current and future work in bringing our voluntary initiatives to life.

The Copyright Alert System is an educational program that enables copyright holders to notify consumers when their Internet access accounts are alleged to have been used illegally to download and share movies, music or TV shows over peer-to-peer networks. CAS notices are designed to be sent in a manner that respects users' privacy, educates them about how to correct behavior, and offers them an independent review process to ensure that users accounts are not inadvertently misidentified as having been used to engage in digital piracy.

Each of the participating ISP's CAS implementation has unique elements, but there are several common components. Notices of alleged infringement are generated by copyright owners using a methodology that has been reviewed and validated by technology experts to capture whole works and avoid false positives. The copyright owners forward notices to participating ISPs who, in turn, pass on individual notices to account holders in the form of copyright alerts. Each alert is one way and no information about individual account holders is shared with content owners.

The program includes up to six alerts with a 7-day grace period between each, offering consumers time to identify the source of and take steps to correct infringing behavior. If a user reaches the final or what we call the mitigation stage, he or she becomes eligible to seek an independent review of alerts received. Administered by the American Arbitration Association, the process offers users the ability to challenge alerts they believe were sent in error.

And finally, all of the alerts sent to consumers and CCI's Web site offer information about how users can find content through the many legal services now available.

The CAS began operating early this year after nearly 18 months of research and development. Our research helped us understand what consumers do and do not know about peer-to-peer technology, and their level of understanding about copyright laws. We found that most consumers do not understand or appreciate concepts that many of us take for granted, and our mandate includes trying to

enhance consumer understanding and change the conversation about digital copyright.

Our research indicates that one of the most important audiences for our educational effort is young people, and we have just completed development of a new copyright curriculum that is being piloted during this academic year in California. The kindergarten through sixth grade curriculum is as a result of CCI's partnership with the California School Libraries Association and iKeepSafe, a leading digital reading literacy organization. It introduces concepts about creative content in innovative and age appropriate ways to help children understand they can be both creators and consumers of artistic content.

A critical element of this entire initiative is our Consumer Advisory Board. The associations and companies that created CCI recognize the importance of—that the success of the program, I am sorry, would depend in large part on whether it was fair to consumers.

Our advisory board provides an important oversight role and advises the CCI board on consumer privacy, transparency and due process. Now that we have completed the challenging task of initial implementation, we are working on a system to evaluate the program's impact and over the coming months we will look internally at the CAS and evaluate user response to the program. We will also look more broadly at the impact on peer-to-peer piracy and our educational initiatives.

We hope these self-assessments will allow the CCI to continue to enhance the effectiveness of the CAS and our central mission of promoting lawful ways to find and consume copyrighted content and educating users about the importance of respecting copyrights.

Once again, thank you for the opportunity to appear before the Subcommittee, and provide information on this unique effort among content owners and ISPs in consultation with consumer advocates. The creation of the Copyright Alert System marks the beginning of a new age of cooperation and innovation.

[The prepared statement of Ms. Lesser follows:]

**Prepared Statement of Jill Lesser, Executive Director,
The Center for Copyright Information**

Chairman Coble, Ranking Member Watt, Chairman Goodlatte, Ranking Member Conyers, Members of the Subcommittee, I appreciate the opportunity to testify today on the important issue of digital copyright. My name is Jill Lesser and I am the Executive Director of the Center for Copyright Information. I am particularly pleased to be testifying on the issue of voluntary initiatives aimed at protecting copyright in the digital age, a new area of cooperation and progress in a policy debate that has long been characterized by sharp differences of opinion.

The Center for Copyright Information (CCI) was established in 2011 as part of a ground-breaking voluntary initiative among the nation's five leading internet service providers (ISPs) and virtually the entire movie and music industries. The agreement among the parties set out to stem the tide of digital piracy by accomplishing two goals: 1) establishing the Copyright Alert System (CAS); and 2) creating an organization that could educate users about the importance of protecting digital content, while offering them a better way to find movies and music online safely and legally. In the two short years since CCI's formation, we have successfully implemented the CAS and have begun a series of educational efforts aimed at helping users make better choices about the way they enjoy digital creative content, while enhancing the ability of recording artists, filmmakers and television producers to be compensated for the compelling and creative programming they deliver.

Still in its early stages, this voluntary cooperative initiative illustrates the importance of multi-stakeholder, market-driven solutions to address the problem of digital piracy, and more generally, CCI and its members believe it can be a model for addressing challenging technology policy issues through collaboration.

BACKGROUND

As the Members of the Subcommittee know well, the last 15 years have witnessed a sea of change in the creation and delivery of all manner of content to consumers. After many decades of distribution through channels easily managed by content owners, like records, DVDs and on-air broadcasting, the digital revolution has turned distribution models—and the ability to protect content against piracy—on their heads. While this wave of innovation in digital delivery wasn't designed to undermine copyright protection, an unfortunate side effect has been the dramatic rise in piracy. Exacerbating the effects of these technological innovations has been the perception by a generation of consumers that content distributed over the internet is or should be free, and that the rules that apply to the physical world don't apply to the virtual world.

Against this backdrop, representatives of the movie and music industries and major ISPs came together in 2009 to begin discussions that ultimately led to the creation of the CAS and the CCI. Those ground-breaking discussions focused on what the parties could do to stem the tide of piracy online, particularly through the growing use of peer-to-peer file sharing systems. After three years of negotiations, the nation's largest ISPs—AT&T, Cablevision, Comcast, Time Warner Cable and Verizon—along with the Motion Picture Association of America (MPAA) and the Recording Industry Association of America (RIAA), and their member companies¹ signed the Memorandum of Understanding (the MOU) that established the framework for the CAS and the structure of CCI. The MOU was the first, and remains the only, purely voluntary, industry-led agreement of its kind.

THE COPYRIGHT ALERT SYSTEM

The CAS, which is overseen by CCI, is an entirely voluntary educational initiative that enables copyright holders to notify consumers when their internet access accounts are alleged to have been used illegally to download and share copyrighted movies, music or TV shows. Such notices are sent in a manner that respects users' privacy, educates them about how to correct their behavior and offers them an independent review process to ensure that users' accounts are not inadvertently misidentified as having been used to engage in digital piracy.

Importantly, the CAS is intended to educate consumers and is largely targeted to the casual infringer. Indeed, large-scale pirates looking to game the system will undoubtedly be able to find other ways to engage in illegal activity. Our system, instead, seeks to inform and change the behavior of the vast majority of users who want nothing more than to enjoy the content they love when and how they desire. It is not intended to be punitive in nature but to assist users in finding digital content legally and understanding the consequences of sharing content illegally over P2P networks.²

While each participating ISP's CAS implementation has unique elements, the key common components of the CAS present in each program are as follows:

- Copyright owners use a methodology that has been reviewed and validated by technology experts to identify instances of copyright infringement over P2P networks and generate notices associated with particular IP addresses;
- Copyright owners forward those notices to the ISP to which the IP address has been assigned;
- The ISP, in turn, matches the identified IP address to a particular account holder and passes on the copyright owner notice to the primary account holder in the form of a Copyright Alert (Alert). Each Alert is a one-way notice and no information about the individual account holders is sent back to the content owners;

¹In partnership with MPAA and RIAA, the Independent Film and Television Alliance (IFTA) and the American Association of Independent Music (A2IM), the representatives of the independent music and film distributors are also participants in the CAS.

²The CAS as an educational program does not require any ISP to terminate any account holder's internet service. However, the program does not affect any obligations ISPs may have pursuant to the DMCA, nor does it alter existing provisions in ISPs' terms-of-service relating to illegal behavior using their accounts.

- Primary account holders may receive up to six Alerts with a seven-day grace period in between each Alert to allow the consumer time to correct his or her behavior or to identify who in the household (or through an external hack of the account) might be intentionally or unintentionally engaging in copyright infringement;
- Within those six Alerts, there are three levels of notice—Educational, Acknowledgement and Mitigation—each designed to offer increasingly clear educational messages about how the user can ensure his or her account is not used for illegal purposes and where and how to find legitimate, licensed sources of movies, music and TV shows;
- If a user reaches the Mitigation Stage, (which happens after receiving either three or four previous Alerts) he or she becomes eligible to seek an independent review of the Alerts received. Our review process, administered by the American Arbitration Association, offers users the ability to challenge the Alerts they received if they believe the Alert were sent in error.

The CAS began operating early in 2013, after 18 months of research and development. Each ISP invested significant resources to design its implementation of the CAS, including the creation of consumer interfaces that would not simply identify instances of digital piracy, but help users understand how P2P technology works, when its use might be illegal and how to find content legally and safely.

To support the companies' work, the CCI engaged in consumer research that helped us understand what consumers do and do not know about P2P technology and their level of understanding about the copyright laws. We found that most consumers do not understand or appreciate concepts that many of us in the policy and legal communities take for granted—like the meaning of copyright. This research is helping us to better understand the drivers of consumer behavior around piracy and, we hope, will help us to improve the CCI's effectiveness in communicating our messages and ultimately reduce the level of online piracy and increase content consumption through legal means.

CONSUMER ADVISORY BOARD

Another very important aspect of the CAS is our consumer advisory board. The member associations and companies that designed the CAS recognized that the success of the program would depend, in large part, on whether the program was fair to consumers and was *perceived* as such by the user community. While, the MOU signatories had worked hard to build in strong privacy protections, and to make each stage of the program (including the independent review process) fair, accurate and impartial, the participants recognized that external review and validation was critically important. Thus, the MOU provided for the establishment of a consumer advisory board, to be comprised of outside industry experts and consumer advocates, who would work with the CCI and its members to ensure that the interests of consumers were adequately considered and protected as the CAS was implemented. The consumer advisory board has provided and continues to provide an important oversight role and valuable advice to the CCI board on consumer privacy and other issues, including the building of a fair independent review mechanism for challenging Alerts.

CCI'S EDUCATIONAL ACTIVITIES

CCI's initial work has focused on implementation of the CAS and the creation of online support for the CAS, including helping users find better ways to access movies, music and television programming. However, an equally important part of our mandate includes helping to change the conversation about digital copyright—to enhance consumer understanding of and respect for creative content in the digital age.

Based on our research, we believe one of the most important audiences for our educational efforts is young people. As a result, we have developed a new copyright curriculum that is being piloted during this academic year in California. The kindergarten through sixth grade curriculum, entitled "Be A Creator"TM, is the result of CCI's partnership with the California School Libraries Association and iKeepSafe, a leading digital literacy organization. The curriculum introduces concepts about creative content in innovative and age-appropriate ways. The curriculum is designed to help children understand that they can be both creators and consumers of artistic content, and that concepts of copyright protection are important in both cases. We hope to use this pilot period to enhance the curriculum and ultimately encourage schools across the country to integrate it into their digital literacy programs.

EVALUATION

Now that we have completed the challenging task of the initial implementation of the CAS and begun expanding our educational initiatives, we are working on a system to evaluate the impact of this innovative partnership among content owners and ISPs. Over the coming months, we will look internally at the CAS in order to evaluate user response to the program, including the impact it is having on the behavior of those receiving Alerts. We will also look more broadly at the impact on P2P piracy of the CAS and our broader educational activities. We hope these self-assessments will allow the CCI to continue to enhance the effectiveness of the CAS and our central mission of promoting lawful ways to find and consume copyrighted content and educating users of all ages about the importance of respecting copyrights.

We are aware that stakeholders around the world are watching the program with interest and we have been sharing our lessons-learned so far when asked. We also stand ready to expand here in the U.S. to additional members and will continue to look for additional opportunities to raise awareness and that our educational messages will expand consumers' respect for copyrights beyond P2P software to other methods of online piracy.

Once again, thank you for the opportunity to appear before the Subcommittee and provide information on this unique effort among content owners and ISPs, in consultation with consumer advocates. The creation of the Copyright Alert System marks the beginning of a new age of cooperation and innovation, as we all work to stem the tide of digital piracy and enhance consumers' ability to find the movies, music and TV shows they love in a safe and legal manner.

Mr. COBLE. Thank you, Ms. Lesser.
Mr. Sherman.

**TESTIMONY OF CARY H. SHERMAN, CHAIRMAN AND CEO,
RECORDING INDUSTRY ASSOCIATION OF AMERICA**

Mr. SHERMAN. Thank you. Chairman Coble, Ranking Member Watt, Ranking Member Conyers, Members of the Subcommittee, thank you for inviting me to testify today. I am Cary Sherman, Chairman and CEO of the Recording Industry Association of America.

The creative industries are undergoing a complete digital transformation. It was not long ago the consumers had limited choices for accessing the music they wanted. Today, the music industry is leading the way beyond the physical CD, licensing hundreds of services worldwide offering tens of millions of songs with digital now making up nearly two-thirds of our revenue.

For the digital marketplace to truly work, we must ensure that these vibrant new services are not undermined by illegal activity. Voluntary initiatives with Internet businesses are a key component of that objective.

So what has been done? First, as Jill Lesser just discussed, the content community and major Internet service providers collaborated to address infringing activity over peer-to-peer networks, resulting in a new Copyright Alert System administered through the Center For Copyright Information.

Second, as Bob Barchiesi will describe, Visa, MasterCard, American Express, Discover and PayPal and now others have collaborated with content and product owners to establish a process for terminating relationships with Web sites that persist in selling illegitimate products.

Third, with regard to advertising on the Internet, Randall Rothenberg will discuss the IAB's new quality assurance guidelines for ad networks and exchanges. We applaud IAB for this effort, al-

though we are a little disappointed that complaints about IP infringement do not yet affect certification.

Grand advertisers and their ad agencies and several ad networks have also established best practices to deter the advertising of products on rogue sites. Information from companies such as Mark Monitor, Double Verify and White Bullet can provide useful data and metrics to measure the effectiveness of these programs.

Fourth, as part of the rollout of new generic top-level domain names, ICANN recently passed a resolution requiring registrars to prohibit domain name holders from engaging in trademark or copyright infringement or other deceptive practices and to impose consequences if they do, including suspension of the domain name.

Fifth, a series of principles relating to user generated content were negotiated by leading commercial copyright owners and UGC services. The parties addressed such issues as the use of effective content identification technology to eliminate infringing uploads, removing or blocking links to sites that are clearly dedicated to infringement, all while accommodating fair use.

So what is missing? Search engines are the roadmaps, indeed, the turn-by-turn directions to rogue sites online. They can be a key partner in addressing infringing activity, and yet there is no voluntary agreement regarding search results. There is certainly many actions that could be taken. Google has tools in its Chrome browser to warn users if they are going to sites that may be malicious. Perhaps that technology could be used to warn users of rogue sites. Imagine if search results linking authorized content were labeled with a certification mark or badge indicating that the site is licensed and actually pays royalties to creators. That educational message could have a profound impact on user behavior.

Similarly, there are no best practices for storage or locker services. Unfortunately, some storage companies appear to be the go-to host for rogue Web sites, and some locker services have an abundance of infringing content available for distribution.

The notice and take-down process under the DMCA would also benefit from collaboration. As interpreted by service providers and the courts, the law requires copyright owners to monitor millions of Web sites and networks every day and send detailed notices to all of them specifically identifying each and every individual infringing file and requesting that each be removed with nothing to prevent the same works from being immediately reposted.

Shouldn't stakeholders sit down and negotiate practical solutions that will make notice and takedown more meaningful and effective? For more stringent repeat infringer policies to takedowns that don't automatically repopulate, many programmatic solutions can be devised. Also, voluntary activities today to focus on Web and wire line activity. With the rapid adoption of mobile devices, we need to focus our efforts on the mobile space and deal with unique challenges it presents.

We are encouraged by the growing support for voluntary initiatives. We are grateful for this hearing which shines light on the current efforts underway. We urge the Subcommittee to do even more; to further encourage collaborations by using its good auspices to monitor data from ad verification companies to see whether the programs are working effectively, monitor best practices that may

develop among registries and registrars to implement the ICANN resolution; encourage and facilitate discussions with search engines and locker services leading toward voluntary best practices; and convene discussions of practical means to improve the notice and takedown process under the DMCA.

Implementing voluntary initiatives will never be a silver bullet, but as reports have shown, taking action against infringing services can have a major positive impact on the usage of licensed services. Working together, we can grow legitimate commerce for everyone.

We look forward to working with this Subcommittee and all our partners in the Internet marketplace to make these initiatives a success. Thank you.

[The prepared statement of Mr. Sherman follows:]

Statement of Cary H. Sherman
Chairman and CEO
Recording Industry Association of America

U.S. House of Representatives
Committee on the Judiciary
Subcommittee on Courts, Intellectual Property, and the Internet

September 18, 2013

Chairman Coble, Ranking Member Watt, Chairman Goodlatte, Ranking Member Conyers, and members of the Subcommittee, thank you for inviting me to submit this statement. I serve as Chairman and CEO of the Recording Industry Association of America. The RIAA is the trade organization that supports and promotes the creative and financial vitality of the major music companies. Its members are the music labels that comprise the most vibrant record industry in the world. RIAA members create, manufacture and/or distribute approximately 85% of all legitimate recorded music produced and sold in the United States.

There can be no doubt that the creative industries are undergoing a complete digital transformation. In the case of the music industry, it was not long ago that the CD was the dominant format and consumers had a relatively limited set of choices for accessing the music they wanted. Today, the music industry is leading the way beyond the physical format with digital sales making up nearly two-thirds of our revenue. There are now literally hundreds of authorized services worldwide offering tens of millions of songs.

We, like others in the creative communities, are working very hard to grow this digital marketplace, driving new technologies and services, and entering into new licenses and partnerships. But in order to make this digital marketplace truly work, we must ensure that these vibrant new legitimate and authorized technologies are not undermined by those engaged in illegal activity. Voluntary initiatives with Internet intermediaries are a key component of that objective.

We are encouraged by the growing awareness of, and support for, these efforts. The Copyright Office in the legislative branch and the Intellectual Property Enforcement Coordinator (IPEC) and Patent and Trademark Office (PTO) in the executive branch have taken active roles in fostering and building these voluntary initiatives, with the IPEC specifically highlighting them in her 2013 Joint Strategic Plan. The recent report by the PTO and Department of Commerce's Internet Policy Task Force repeatedly refers to the "great promise" of voluntary initiatives and best practices. The PTO is currently studying the efficacy of these initiatives. We greatly appreciate the ongoing recognition of the importance of best practices and voluntary agreements by the Administration and Congress, and this hearing, along with the copyright review being conducted by this Subcommittee, helps to shine light on the current initiatives underway as well as encouraging agreements where there is still work to do.

What's been done?ISPs

After several years of discussions, the content community and major Internet service providers (ISPs) collaborated to address the serious problem of infringing activity over peer-to-peer (P2P) networks. The resulting Copyright Alert System (CAS), administered through the Center for Copyright Information (CCI) and officially implemented in early 2013, provides a means to inform users of their activity, to educate them on appropriate and legal ways to access the content they seek, and to implement reasonable mitigation measures when necessary.¹

The system enables content owners, after confirming a work has been illegally shared, to inform the relevant ISP so that the ISP can then pass on the notice to the corresponding subscriber, without revealing the subscriber's name or information to the copyright owner. Multiple notices to a subscriber result in "escalating" alerts by the ISP. The first one or two alerts provide the user with an online educational message about their activity and copyright. Alerts 3 and 4 provide a mechanism for acknowledging receipt. Alerts 5 and 6 implement a mitigation measure to deter future content theft. The CAS is intended to provide enforcement through a consumer-friendly approach:

- Consumers have a right to know when their Internet accounts are being used for content theft and the system provides information on steps consumers can take to identify and stop such activity.
- The multiple alerts and grace periods provide consumers with time to change their behavior before the next alert is sent and before any mitigation is imposed.
- No personal information about subscribers is exchanged between content owners and ISPs without subscriber consent, and then only in connection with certain challenges under an independent review.
- ISPs are not required to impose any mitigation measure that could disable a subscriber's essential services, such as telephone service, email, or security or health service.

The CAS is still in the initial implementation stages and proper metrics are being determined. But feedback so far has been positive and it is worth noting that P2P content protection programs in other countries have been found to have an impact on either the amount of unauthorized P2P activity or on sales.

Payment Processors

In 2011, the IPEC helped finalize a set of best practices among Visa, MasterCard, Amex, Discover and PayPal, and content and product owners, in which these payment processors

¹ See www.copyrightinformation.org for more information.

agree to terminate their relationship with a website if the site persists in intentionally selling illegitimate products.² Payment processors have implemented the agreement with members of the International Anti-Counterfeiting Coalition (IACC) through a mechanized process for submitting secure and valid evidentiary requests for ending affiliation with rogue sites. Some data on the impact of this program has already been provided by IACC.³ Per the IACC, as of August 21, 2013, nearly 7,000 websites had been referred via IACC's portal for investigation, resulting in termination of over 1,500 individual merchant accounts. Perhaps more importantly, as IACC notes, the collaboration resulting from the portal will likely result in "systematic long term improvement in addressing the trafficking of counterfeit goods online".⁴

Advertisers and Advertising Intermediaries

There have been three significant developments on voluntary initiatives with regard to advertising. First, the Association of National Advertisers (ANA) and the American Association of Advertising Agencies (4A's) established best practices by brand owners and their agencies to deter advertising on rogue sites.⁵ These best practices define rogue sites as those dedicated to infringement because they have no significant or only limited use or purpose other than engaging in, enabling or facilitating infringement. These best practices and their implementation would be more effective if they required ANA Members and 4A Members to include in their insertion orders to ad networks that such networks comply with IAB's Quality Assurance Guidelines (QAG).

The IAB established these network and exchanges quality assurance guidelines in 2010, and recently updated the QAG this year to include other online ad intermediaries.⁶ The QAG prohibits the sale of any ad space inventory on sites that infringe on copyrights, or are warez sites, including illegal streaming sites, torrent sites, illegal music download sites, etc. Unfortunately, while complaints regarding QAG non-compliance may affect QAG certification, the QAG makes clear that IP infringement complaints do not.

² See U.S. Intellectual Property Enforcement Coordinator, 2013 Joint Strategic Plan on Intellectual Property Enforcement. June 2013, p. 36, available at <http://www.whitehouse.gov/sites/default/files/omb/IPEC/2013-us-ipec-joint-strategic-plan.pdf> ("IPEC 2013 Report").

³ See Comments submitted by the International AntiCounterfeiting Coalition re: Request of the Patent and Trademark Office for Public Comments: Voluntary Best Practices, Study, Docket No. PTO-C-0036-02, dated August 21, 2013, available at <http://www.uspto.gov/ip/officechiefecon/PTO-C-2013-0036.pdf#page=33>. See also International AntiCounterfeiting Coalition. IACC Payment Processor Portal Program: First Year Statistical Review, October, 2012, available at <http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf>.

⁴ Id.

⁵ See ANA press release about Pledge to Deter Advertising on Rogue Sites, May, 2012, with link to pledge, available at <http://www.ana.net/content/show/id/23408>.

⁶ Available at http://www.iab.net/QAGInitiative/overview/quality_assurance_guidelines and http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-072513.

Third, several ad networks established a set of best practices to reduce the amount of ad revenue that funds, and largely enables, pirate and counterfeit sites.⁷ These best practices categorize rogue sites as those principally dedicated to selling counterfeit goods or engaging in copyright piracy and have no substantial non-infringing uses. They require the establishment of policies prohibiting such sites from participating in the ad network's advertising program, that the ad network be QAG certified (though as noted above, IP complaints do not affect QAG certification), and that the ad network maintain a complaint procedure.

Reports such as those from the USC Annenberg Innovation Lab, as well as information from companies such as MarkMonitor, DoubleVerify, Integral Ad Science and WhiteBullet, can provide useful data and metrics to determine the effectiveness of these programs on the placement of ads on rogue sites.

Domain Name Registries/Registrars

As part of the roll-out of new generic Top Level Domains, ICANN recently passed a resolution that, among other provisions, provides that a "Registry Operator will include a provision in its Registry-Registrar Agreement (RRA) that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name."⁸

While the practical impact of this resolution remains to be seen (few if any new gTLDs will "go live" before the end of this year), it will be worth monitoring what best practices, if any, develop among registries, registrars and right holders to implement this resolution. It would also be useful to track how this provision is implemented in the new gTLD space as compared with controls chosen from existing gTLDs whose operators are not parties to the updated registry-registrar agreement.

UGC Principles

Leading commercial copyright owners and services providing user-uploaded and user-generated audio and video content ("UGC services") collaborated to establish principles to foster an online environment that promotes the promises and benefits of UGC Services while protecting the rights of copyright owners.⁹ Published in 2007, these were one of the first multi-stakeholder negotiated voluntary initiatives established to address copyright issues in the digital environment.

⁷ See <http://www.whitehouse.gov/blog/2013/07/15/coming-together-combat-online-piracy-and-counterfeiting-and>
<http://www.2013ippractices.com/bestpracticesguidelinesforadnetworkstoaddresspiracyandcounterfeiting.html>.

⁸ See <http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-25jun13-en.htm>.

⁹ See www.cgcprinciples.com.

Copyright owners and UGC services recognized that they share several important objectives: (1) the elimination of infringing content on UGC Services; (2) the encouragement of uploads of wholly original and authorized user-generated audio and video content; (3) the accommodation of the fair use of copyrighted content on UGC Services; and (4) the protection of legitimate interests of user privacy.

To achieve these objectives, the parties agreed to:

- during the upload process on UGC sites and services, prominently inform users that they may not upload infringing content according to the services' terms of use;
- use effective content identification technology to eliminate infringing user-uploaded audio and video content for which Copyright Owners have provided detailed reference material;
- to work together to identify sites that are clearly dedicated to, and predominantly used for, the dissemination of infringing content or the facilitation of such dissemination;
- to remove or block links to such sites; to provide commercially reasonable enhanced searching and identification means to Copyright Owners;
- to accommodate fair use; to use reasonable efforts to track infringing uploads of copyrighted content by the same user and to use such information in the reasonable implementation of a repeat infringer termination policy; and
- to use reasonable efforts to prevent a terminated user from uploading audio and/or video content.

The UGC principles serve as a model of intermediaries and content owners working together voluntarily to assure that the provisions of the Digital Millennium Copyright Act (DMCA) have meaning and are adapted to new technological advancements. They should serve as a blueprint for new voluntary agreements between content owners and Internet intermediaries to carry out the intent of the DMCA to protect both copyright owners and intermediaries (see "Notice and Takedown Under the DMCA," below.)

What's missing?

Search Engines

If ISPs can be considered the gateway by users to rogue sites online, search engines may be considered the roadmaps or, more directly, the turn-by-turn directions and door-to-door service to these sites. There can be no doubt that search engines play a considerable role in leading users to illicit services and can be a key part of addressing infringing activity online.

Unfortunately, while there has been some action and steps taken by search engines under the notice and takedown system of the DMCA, there has been little movement toward finding tools that have the impact of actually reducing theft and damage. One reason for this

may be the failure by these intermediaries to measure whether actions taken are, and have been, effective. The result is at its best wasted effort on a solution that doesn't work and at worst lip service that merely buys time and, often, money from the advertising revenue such linking generates.

There have been occasional instances of progress, but with disappointing outcomes. For example, Google announced in August 2012 that:

"Starting next week, we will begin taking into account a new signal in our rankings: the number of valid copyright removal notices we receive for any given site. Sites with high numbers of removal notices may appear lower in our results. This ranking change should help users find legitimate, quality sources of content more easily—whether it's a song previewed on NPR's music website, a TV show on Hulu or new music streamed from Spotify."¹⁰

But several months later, our studies, which we have shared with Google and Congress, indicate that sites for which Google has received hundreds of thousands of infringement notices are still appearing at the top of search returns.¹¹ Worse still, users are being directed to these sites through the use of "autocomplete" features, which purport to predict what users are looking for after merely a few keystrokes.

We believe it would be useful to see voluntary initiatives by search engines that take into account whether or not a site is authorized to provide the content at issue in determining search result rankings for searches to consume that content. This could take into account not only the absolute number of copyright removal requests sent about a site to trigger demotion of that site, but also whether the site is authorized to provide the content to trigger a higher search rank for that site.

There are certainly other voluntary actions that could be taken by search engines to stop encouraging and directing users to illegitimate sources of copyrighted material, and to evaluate whether such measures could have a demonstrable impact, possibly by proxy to similar efforts with other content. For example, Google has announced that it intends to develop and deploy technology to eradicate links to child pornography images from the web. Certainly similar technology can be used to remove links to other illegal content. Also, Google has tools in its Chrome browser to warn users if they are going to sites that may be malicious. Shouldn't that technology be used to warn users of rogue sites? Or better yet, can Google use similar technology to highlight or identify sites that are authorized? Imagine if links to content on legitimate sites were labeled – directly in the search result –with a certification mark

¹⁰ See <http://insidesearch.blogspot.com/2012/08/an-update-to-our-search-algorithms.html>.

¹¹ See RIAA, "Six Months Later – A Report Card on Google's Demotion of Pirate Sites", Feb. 21, 2013, available at <http://76.74.24.142/3CF95FD1-3836-E6CD-A470-1C2889DF9723.pdf>. Also, on a search conducted August 29, 2013 for mp3s or downloads of the recent top 50 billboard tracks, www.mp3skull.com, a site for which Google has received over 1.25 million copyright removal notices, showed up in the top 5 search results 42 times.

indicating that the site is licensed and actually pays royalties to creators. That educational message could have a profound and positive impact on user behavior.

Storage Services

Today, there does not seem to be any form of best practices for storage services when it comes to protecting works online – whether for technical hosting providers that maintain the servers where content is hosted or for locker services that interact directly with the user. Unfortunately, some storage services – whether unwittingly or not – appear to be the “go to” services for rogue websites, and some locker services have an abundance of infringing content available via their service. It would be helpful to engage these services in developing best practices for deterring infringement on their services.

As a first step, it may be useful to measure if any U.S.-based technical hosting storage services host a concentration of sites that engage in widespread infringement. To determine which sites to include in such a study, one could look at those sites for which Google has received multiple notices of infringement, as indicated on the Google Copyright Removal Transparency Report, or engage website reputation services, such as WhiteBullet or Veri-Site. Of course, it is always beneficial to consult copyright holders directly.

For lockers services that are known to be used for infringing activity, best practices should involve more than notice and take-down. For example, a German Court recently ordered RapidShare to scan for incoming infringing links. This and/or other tools should be considered to deter infringing activity over locker services.

Notice and Takedown Under the DMCA

When Congress passed the DMCA in 1998, it intended to protect copyright owners from widespread infringement made possible by the Internet, and to protect Internet intermediaries from liability for illegal acts committed by their users. At the time, several cases had already detailed the potential ease with which new methods of digital dissemination could facilitate massive amounts of content theft. Congress sought to create a partnership between content creators and Internet intermediaries to make the Internet a safe place for legitimate commerce, providing the public with access to legitimate high-quality works.

Congress's stated objective was to “preserve strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment.”¹²

Unfortunately, while the liability limitations have, in large part, worked to protect intermediaries, copyright owners have not received meaningful protection. Courts have often failed to apply the statute in a practical manner, effectively requiring copyright owners to

¹² S. Rep. No. 105-190, at 40 (1998).

monitor millions of websites and networks every day and send detailed notices to all of them specifically identifying every individual infringing item and requesting that the items be removed. Moreover, even if a copyright owner takes on this challenge, the courts have eliminated any expectation that any removed infringing items will not be immediately re-posted.

As was done with the UGC Principles, there is an opportunity for intermediaries and content owners to sit down and negotiate practical solutions that will make the “notice and takedown” system more meaningful and effective. From more stringent repeat infringer policies to takedowns that don’t automatically repopulate, many practical solutions can be adopted that would assure the intent of the DMCA is carried out. We hope the relevant parties will join together to start this process and we need Congress to encourage and facilitate such a process.

Mobile

As noted above, the voluntary initiatives to date have focused on web and wireline based activity and services. With the beneficial and rapid adoption of mobile devices, we need to focus our efforts on the mobile space as well, and deal with the unique challenges that ecosystem presents.

What works best?

The established best practices and voluntary agreements outlined above represent a considerable positive step in the evolution of the legitimate digital marketplace. The true goal should not only be to enable content owners to discover and inform intermediaries of illegal use of their works, but also for intermediaries to take active steps themselves to ensure that their products and services are not being used to engage in illegal behavior. Intermediaries increasingly understand that cooperating in efforts to prevent infringement redounds to their benefit as well as to the owners of the content they serve, host, transmit, or otherwise handle. But beyond the security and integrity such engagement provides, establishing best practices and voluntary agreements provides an opportunity to form lasting and meaningful partnerships that will benefit businesses, creators, and consumers alike.

Of course, these initiatives are very much in their infancy and we will have to give them appropriate time to operate and be properly evaluated. But there are some considerations we should keep in mind going forward:

- The initiatives must be flexible to adapt over time.
- True goals of the initiatives should be determined.
- Initiatives must go beyond what is already done or expected of intermediaries under existing law.

- Baseline measurements should be taken to measure the impact of initiatives and to determine whether the private sector can adequately “self-regulate” to deter infringing and other abusive behavior.
- Academic and research papers should be considered in determining whether initiatives are effective and what can be done differently.
- Qualitative impacts should be considered – raising awareness among consumers, other stakeholders, and other governments, and should consider any changing attitudes towards infringement.
- Each initiative should be evaluated separately, and direct stakeholders/participants should be consulted.

In addition, it is worth noting that best practices and voluntary agreements negotiated and agreed to among all stakeholders are more promising than those that are established unilaterally. For example, ICANN’s Registry-Registrar Agreement could be very effective because it binds anyone who wants to operate a new gTLD or sell registrations in the new registries as an ICANN-accredited registrar. CCI’s Copyright Alert System and the payment processor agreement required both sides to compromise and work together toward a solution. While unilateral principles and public commitments such as the ad networks’ are valuable, they do not offer the same promise of effectiveness since they don’t have the same buy-in from both sides and may not lead to a common process or solution.

This point has been made particularly clear by Google’s recent report entitled “How Google Fights Piracy”. As we noted in a blog on the report, we are grateful for the efforts Google has taken, and there is much to applaud. However, as much as Google may be doing, as Benjamin Franklin cautioned, we must “never confuse motion for action.” While we have seen some measurable impact in Google’s AdSense based initiatives, we cannot say the same for its other anti-piracy activities.

We invite Google and the other major search engines to sit down with us to formulate a plan that goes beyond promises of action and actually serves its intended purpose of deterring piracy and giving the legitimate marketplace an environment to thrive.

Certainly, no one has claimed that implementing voluntary initiatives with Internet intermediaries is a single silver bullet to stop piracy online. But in fulfilling the promise of a healthy and growing legitimate digital marketplace, enforcement in any form is worth considering. As reports by the NPD Group have shown, taking legal action against infringing services, such as unauthorized activity on p2p networks and digital locker sites, can have a major impact on usage of licensed music services. Implementing voluntary initiatives in a thoughtful manner compliments prior enforcement initiatives and helps fulfill that promise.

Again, we thank the Subcommittee for holding this hearing. While unilateral enforcement efforts and legislative options have played a large part in our past and may necessarily play a role going forward, we truly believe that strengthening our partnerships and mutual efforts through voluntary initiatives is preferable and can be much more effective.

Voluntary initiatives can address new and changing situations and adapt easily to new business models. They can set industry standards that form norms in the Internet eco-system. And importantly, they help build necessary trust and cooperation among content owners, intermediaries, and consumers.

We appreciate the attention brought to the development of voluntary initiatives, and look forward to working with you and all our partners in the Internet marketplace to determine how to make them most effective.

Mr. COBLE. Thank you, Mr. Sherman.
Mr. Rothenberg.

**TESTIMONY OF RANDALL ROTHENBERG, PRESIDENT
AND CEO, INTERACTIVE ADVERTISING BUREAU**

Mr. ROTHENBERG. Chairman Coble, Ranking Member Watt, Senior Member Conyers, Members of the House Judiciary Subcommittee on the Courts, Intellectual Property and the Internet, thank you for the opportunity to testify at this important hearing. My name is Randall Rothenberg and as you heard, I am the President and Chief Executive Officer of the Interactive Advertising Bureau and I am very honored to be here.

IAB is the trade association for ad-supported digital media in the United States. IAD's more than 500-member companies account for 86 percent of the interactive advertising sold in the U.S. Our members include many of the recognized names, most of the recognized names of the media world, AOL, CBS, Facebook, Google, Microsoft, The New York Times, Time, Inc., Walt Disney, Yahoo among them, as well as scores of smaller publishers, advertising networks and specialists in such areas as digital video advertising and mobile advertising.

I am also here for a personal reason. Prior to joining the IAB, I spent the first two-thirds of my career as an author and writer. I have written several books, hundreds of newspapers and magazine articles. I own hundreds of copyrights. I continue to be a contributor to many publications.

Having spent my career in the creation of intellectual property, I firmly believe the meaningful protection of intellectual property rights is the foundation on which the U.S. economy depends. As the Framers of the U.S. Constitution understood, if we wish to remain the world's leader in innovation and entrepreneurship, we must reward both hard work and risk-taking through the protection of intellectual property.

On behalf of our member companies, IAB is dedicated to the growth of the interactive advertising marketplace. IAB drives toward this end by educating marketers, advertising agencies, media companies and the wider business community about the value of interactive advertising, and we recommend technical standards and best practices for this evolving marketplace.

In this regard, we are proud of our efforts to bring together the most significant representatives of this digital marketing supply chain to develop strong protections for intellectual property and greater trust in the digital advertising marketplace.

The vibrant online advertising ecosystem that was created by innovative and legitimate individuals and companies has gained the attention of illegitimate actors that wish to undercut the market for creative content through the illegal activity of copyright infringement. This is a major reason, a foundation reason, the IAB developed the quality assurance guidelines that Mr. Sherman referred to.

The guidelines were created to help establish trust between the buyers and sellers of advertising in a very complex and ever-evolving digital advertising ecosystem. The program helps promote the flow of advertising budgets into digital advertising by establishing

industry principles that offer a framework for increasing brand safety.

We consider the piracy of intellectual property antithetical to the concept of brand safety. For that reason, the IAB guidelines provide specific prohibitions against selling certain types of advertising inventory, including ad inventory on sites involved in intellectual property violations such as Web sites hosting and streaming infringing copyrighted content, torrent sites and peer-to-peer sites.

In April of 2013, IAB released an update to the guidelines for public comment. This revision focuses on increasing the applicability, visibility and influence of the guidelines program as well as the advancement of other vital program elements. I would like to identify three important changes we made.

First, we took a program that was originally designed for ad networks and exchanges solely and expanded it into a true multi-stakeholder process by including all buyers and sellers of digital advertising. The program will now represent the full diversity of the industry and reinforce the role all parties play in building a more accountable, transparent and safe marketplace.

Second, the guidelines now explicitly include an option for the lodging of intellectual property infringement complaints by rights holders to the IAB which will then direct the complaint to the relevant contact at each company participating in the guidelines. The IAB is committed to working with all parties to strengthen the protection of intellectual property rights through the guidelines including through a strengthened complaints process.

Third, the program was also strengthened with the introduction of the option of independent third party validation of a company's certification to create a new level of trust in the marketplace.

Going forward, we will continue to evolve, strengthen and drive adoption of the guidelines. The program has received a tremendous amount of exposure because of recent acknowledgments by Victoria Espinel, the former U.S. Intellectual Property Enforcement Coordinator. We would welcome additional public support from you and other Members of Congress.

Thank you for considering the views of the IAB on these issues. We greatly appreciate your focus on our work and the work of all the others on this panel to strengthen the protection of intellectual property and understanding the role of the advertising industry in creating additional strengths to those protections. Thank you.

[The prepared statement of Mr. Rothenberg follows:]

BEFORE THE
SUBCOMMITTEE ON COURTS, INTELLECTUAL PROPERTY AND
THE INTERNET
OF THE
HOUSE JUDICIARY COMMITTEE

HEARING ON
THE ROLE OF VOLUNTARY AGREEMENTS IN THE U.S. INTELLECTUAL
PROPERTY SYSTEM
SEPTEMBER 18, 2013

TESTIMONY OF
RANDALL ROTHENBERG
PRESIDENT AND CEO
INTERACTIVE ADVERTISING BUREAU

I. Introduction

Thank you for the opportunity to testify at this hearing of the House Judiciary Committee's Subcommittee on the Courts, Intellectual Property and the Internet. I would like to thank Chairman Coble and Ranking Member Watt for holding this important hearing.

My name is Randall Rothenberg and I am the President and Chief Executive Officer for the Interactive Advertising Bureau (IAB). IAB is the trade association for ad-supported interactive media in the United States. IAB's more than 500 member companies account for 86 percent of the interactive advertising sold in the United States. Our members include the great names of the online and offline media world – AOL, CBS, Facebook, Google, Microsoft, The New York Times, Time Inc., Walt Disney, and Yahoo! among them – as well as scores of smaller publishers, advertising networks, and specialists in such areas as digital video advertising and mobile advertising.

Prior to joining the IAB, I spent many years a journalist at the *New York Times* and *Advertising Age*, a magazine on marketing and media. I am also an author and a frequent guest contributor to various publications. Having spent my career promoting the creation of quality, original content, I firmly believe that meaningful protection of intellectual property rights is the foundation on which the U.S. economy depends. As the framers of the U.S. Constitution understood, if we wish to remain as the world's leader in innovation and entrepreneurship, we must reward hard work and risk-taking through the protection of intellectual property.

On behalf of our member companies, IAB is dedicated to the growth of the interactive advertising marketplace. IAB drives toward this end by educating marketers, agencies, media companies and the wider business community about the value of interactive advertising, and

recommending standards and practices for this evolving marketplace. I believe that in order for the online advertising industry to continue growing, advertisers and marketers must have confidence that their brands will be protected in the digital ecosystem. We are proud of our efforts to bring together the most significant representatives of this digital marketing supply chain to develop strong protections for intellectual property and greater trust in the online advertising marketplace.

Mr. Chairman, my testimony will describe how the IAB, in partnership with both buyers and sellers of online advertising, has helped to create safeguards and enforcement mechanisms against online copyright piracy and counterfeiting. IAB's enforcement mechanisms are important tools in reducing the economic incentive of intellectual property theft, and illustrate the broad support and adoption for self-regulation in online advertising.

II. Interactive Advertising Is Important to the U.S. Economy

Before explaining the online advertising industry's efforts to combat intellectual property theft, let me first explain the role of advertising in today's digital marketplace.

In 2012, a study commissioned by the IAB and conducted by researchers at the Harvard University Business School found that the ad-supported Internet contributed over \$530 billion to the U.S. economy, making it one of the most dynamic sectors in the U.S. economy.¹ Over 5.1 million, or roughly 3 percent, of American jobs are directly or indirectly created by the Internet. These jobs are highly dispersed across the U.S., with more jobs being created in small businesses across every state than in large internet companies.

¹ Professors John Deighton and Harold Brierley, Economic Value of the Advertising-Supported Internet Ecosystem (October 1, 2012), available at <http://www.iab.net/economicvalue>.

210 million people in the United States spend, on average, 38 hours a month on the Internet for work and leisure. This is unsurprising, for the Internet offers original creators of news, business information, entertainment, maps, and self-help resources, an ability to connect directly with consumers around the world. For example, education and information-gathering tools, including search engines, have helped to remove geographic and economic barriers and democratized the availability and accessibility of educational content. The Web is a communications lifeline for an enormous number of people. There are an estimated 1 billion users of free email services worldwide. Over 72 percent of Americans keep in touch with family and friends through social networking sites. In July, 187 million Americans viewed 48 billion videos online that were uploaded by others.

Nearly all of these services, information, and entertainment are free. Although, as you and I know, they are not really free: They are supported by advertising.

This is not surprising. For centuries, advertising has been at the center of a vital value exchange between businesses and consumers. We provide quality news, information, entertainment, and other services, in return for which consumers give us their time and attention. That time and attention, in turn, allows businesses to communicate the availability of goods and services to consumers and customers. Advertising is the heart of the U.S. consumer economy.

III. Self-Regulation is Combatting Intellectual Property Theft

The vibrant online advertising ecosystem that was created by innovative and legitimate individuals and companies has gained the attention of nefarious actors who wish to undercut the market for creative content through the illegal activity of copyright infringement. This abuse

hurts the brand integrity of advertisers and slows legitimate growth and job creation in the Internet economy.

IAB strongly believes in the importance of intellectual property protection for a functioning economy and the sustainability of the online advertising industry. This is one reason the IAB developed the Quality Assurance Guidelines (“Guidelines”).² The Guidelines were created to help establish trust between buyers and sellers in a complex and ever-changing digital advertising ecosystem. The program helps promote the flow of advertising budgets into digital advertising by establishing industry principles that offer a framework for increasing brand safety. We consider piracy of intellectual property antithetical to the concept of brand safety: Consumer brands depend on the integrity of their own copyrights, trademarks, and patents, as well as on their distinctive brand reputations, and would not want to be associated with digital environments that persistently pirate others’ intellectual property. For that reason, the IAB Guidelines provide specific prohibitions against selling certain types of advertising inventory, including ad inventory on sites involved in intellectual property violations, such as websites hosting and streaming infringing copyrighted content, torrent sites, and peer-to-peer sites.

On April 18, 2013, IAB released an update to the Guidelines for public comment. This revision focuses on increasing the applicability, visibility, and influence of the program, as well as the advancement of other vital program elements. Principally, we expanded the program to include all buyers and sellers of digital advertising. Originally, the Guidelines were targeted solely to ad networks and exchanges. The program will now represent the full diversity of the industry and reinforce the role all parties play in building a more accountable, transparent, and safe marketplace. This means that any seller of digital advertising, including premium

² Interactive Advertising Bureau, Quality Assurance Guideline (July 25, 2013) Available at <http://www.iab.net/QAG>

publishers, can now certify to be compliant with the Quality Assurance Guidelines which allows them to more formally shape and strengthen the guidelines. Intellectual property protection remains a centerpiece of the expanded Guidelines. The updated Guidelines now explicitly include an option for the lodging of Intellectual Property Infringement complaints by rights holders to the IAB, who will then direct the complaint to the relevant contact at each company participating in the Guidelines. The IAB is committed to working with all parties to strengthen the protection of intellectual property rights and improving the Guidelines complaint process. In addition, the program was also strengthened with the introduction of the option of independent third-party validation of companies' certification to create a new level of trust in the marketplace.

This program is driven by consensus amongst the participating companies. Representatives from companies that are in compliance or have committed to becoming compliant with the Guidelines shape the process. With the expanded representation across the digital advertising supply chain, we recognize there will be challenges to reaching consensus; therefore we have incorporated several procedural changes to encourage swifter action on high priority issues. For example, IAB is working to expand involvement in the decision making bodies of the program to include a much wider array of companies, including rights holders and premium publishers as well as representatives of buyers. IAB is also establishing a working group to research and analyze technological solutions across the ecosystem. IAB strives to provide a fertile environment for the finding of majority-supported resolutions, and to then act promptly and diligently to bring them to market. Opening up the Guidelines program to content owners will allow for their direct influence in future iterations of the Guidelines. They will be

able to help define how the Guidelines protect their intellectual property. The program and their interests are now more closely aligned than ever.

IAB remains committed to further developing and expanding the Guidelines. We proactively educate our members and the public about the program through consistent promotion and outreach. Members learn about and are encouraged to adopt the Guidelines through email, attendance at events such as the IAB Advertising Tech Marketplace, and regularly scheduled committee and board meetings. We inform the greater industry and the public about the Guidelines through social media and press outreach. I have spoken often at our events, including our IAB Annual Leadership Meeting this year, which drew nearly 1,000 senior industry executives, about the importance of industry-wide action and individual company commitment to combatting intellectual property piracy.

Going forward, we will continue to drive adoption of the Guidelines through marketing efforts, as well as by our expansion of the program to involve more stakeholders. The program has received a tremendous amount of exposure because of recent acknowledgments by Victoria Espinel, former U.S. Intellectual Property Enforcement Coordinator. We would welcome additional public support from you and other members of Congress.

IV. IAB Continues to Explore New Solutions

IAB continues to explore other avenues to combat online piracy and counterfeiting. In July, 24/7 Media, Adtegrity, AOL, Condé Nast, Google, Microsoft, SpotXchange, and Yahoo!, in coordination with IAB and the Office of Management and Budget, agreed to participate in voluntary Best Practices and Guidelines for Ad Networks to Address Piracy and Counterfeiting

("Best Practices").³ These eight companies are leaders in the advertising industry. By agreeing to the Best Practices, they have committed to "maintain policies prohibiting websites that are principally dedicated to selling counterfeit goods or engaging in copyright piracy and have no substantial non-infringing uses from participating in the Ad Network's advertising programs." Further, the advertising networks agreed to continue the dialogue with content creators, rights holders, consumer organizations, and free speech advocates, regarding the best practices for enforcing intellectual property rights. The Obama Administration's Office of the U.S. Intellectual Property Enforcement Coordinator recently offered support for the self-regulatory Best Practices, stating that it was "a good example of how the public and private sector can work to combat piracy and counterfeiting while protecting and, in fact, further encourag[ing] the innovation made possible by an open Internet." IAB is educating other ad networks about the Best Practices. We are also exploring the possibility of inclusion of the Best Practices in the next version of the Quality Assurance Guidelines. As you can see, Mr. Chairman, IAB continues to explore creative solutions to address the problem of intellectual property theft.

V. Conclusion

Thank you for considering the view of IAB on these issues. We greatly appreciate your focus on our work to protect the value of original content and the advertising industry that supports its creation. We welcome your observations as the Guidelines progress, and urge you to continue to engage in fruitful dialogue that will lead to truly implementable and successful outcomes for the creative industries impacted by online theft.

³ Best Practices and Guidelines for Ad Networks to Address Piracy and Counterfeiting (July 15, 2013), available at <http://2013ippractices.com/>

Mr. COBLE. Thank you, Mr. Rothenberg.
Mr. Levitt.

**TESTIMONY OF GABRIEL LEVITT, VICE PRESIDENT,
PHARMACYCHECKER.COM**

Mr. LEVITT. Chairman Coble and Ranking Member Congressman Watt and Ranking Member Conyers, I am Gabriel Levitt, the Vice President of PharmacyChecker.com, which for the past 10 years, has been helping Americans find affordable medication from safe online pharmacies by checking and verifying the credentials of these pharmacies and posting price comparisons.

We believe that voluntary agreements can be a useful tool in protecting Americans from counterfeit products, but they can also be misused in anti-competitive ways which scare and thwart Americans from accessing affordable medications. This leads to poor medication compliance with negative health consequences and also goes against the Administration's desire that voluntary agreements not be used to impede competition. I will present recommendations which can keep this from happening.

Last year, 50 million Americans, ages 19 to 64, did not fill a prescription due to cost, up from 48 million in 2010, according to the Commonwealth Fund. We also know that nearly 5 million Americans have been buying their medication from outside the U.S. in order to get affordable prices because the cost to buy brand name medicine is often 80 percent lower in other countries than in the U.S.

Independent studies and over a decade of experience have demonstrated the safety of domestic and international online pharmacies approved in rigorous programs such as PharmacyChecker's. A voluntary agreement of particular concern is one established by a group of Internet and credit card companies called the Center For Safe Internet Pharmacies, or CSIP. While CSIP has been effective at taking down some rogue pharmacies, it also acts to discourage Americans from accessing safe affordable medications outside the United States.

CSIP uses a company called Legit Scripts to help it identify rogue sites for takedown and to power an online tool for consumers to look up the status of an online pharmacy. Unfortunately, if you use this tool to look up any online pharmacy operating in any country other than the U.S., such as Canada, it will tell you that the pharmacy is unapproved, regardless of the fact that it may be licensed, require a prescription and safely selling only genuine medication.

The CSIP Web site has become a clearinghouse for information from the pharmaceutical-funded groups such as the Partnership For Safe Medicine and the National Association of Boards of Pharmacy with scare campaigns conflating all non-U.S. pharmacies with rogue pharmacies. In fact, any pharmacy outside the U.S. which sells to Americans is labeled by NABP as a rogue.

To keep voluntary agreements from misleading Americans, we ask that your Committee make sure that CSIP does not discourage Americans from accessing safe and affordable medication online. In particular, we would urge that the basis for defining a rogue pharmacy include any of the following, but not simply whether or not it is licensed in the U.S. It intentionally sells adult rated or coun-

terfeit medication; sells prescription medication without requiring a prescription; engages in fraudulent and deceptive business practices; does not follow generally accepted safety standards of pharmacy practice; and sells medication that is not regulated.

We would also like to see CSIP and other institutions established under voluntary agreements be more transparent by providing the following information: Clearly state what recourse companies and people have if their businesses are shut down by actions taken by CSIP; provide information on those sites that were shut down and the reasons they were shut down based on applicable intellectual property laws and identify the precise public health risk of the Web site.

Last, it is important to recognize that voluntary agreements are being afforded considerable market power. To ensure these powers are used properly, we recommend the appointment of an independent ombudsman to oversee these agreements. The ombudsman would analyze voluntary agreements to make sure private sector actions aren't blocking Internet competition and are consistent with the Administration's other goals of due process, free speech and transparency.

I have provided the Committee with a transcript of this presentation and included our public comments submission to the U.S. PTO in Exhibit A. Thank you for your time.

[The prepared statement of Mr. Levitt follows:]



PharmacyChecker.com, LLC
 333 Mamaroneck Avenue
 White Plains, NY 10605
 p: 718.554.3067
 f: 718.715.1033

Testimony of Gabriel Levitt
 Vice President, PharmacyChecker.com (www.pharmacychecker.com)

House Judiciary Committee, Subcommittee on the Courts, Intellectual Property and the Internet
 Hearing on "The Role of Voluntary Agreements in the U.S. Intellectual Property System"

September 18th, 2 pm, 2141 Rayburn House Office Building

Chairman Goodlatte and Ranking Member Congressman Watt, thank you for inviting me here today.

I am Gabriel Levitt, the vice president of PharmacyChecker.com, which, for the past 10 years, has been helping Americans find affordable medication from safe online pharmacies by checking and verifying the credentials of these pharmacies and posting price comparisons.

We believe that voluntary agreements can be a useful tool in protecting Americans from counterfeit products, but they can also be misused in anti-competitive ways which scare and thwart Americans from accessing affordable medication. This leads to poor medication compliance with negative health consequences and also goes against the Administration's desire that voluntary agreements not be used to impede competition.¹ I will present recommendations which can keep this from happening.

Last year, fifty-million Americans ages 19-64 did not fill a prescription due to cost, up from 48 million in 2010, according to the Commonwealth Fund.¹¹ We also know that nearly five million Americans have been buying their medication from outside the U.S. in order to get affordable prices, because the cost to buy brand-name medicine is often 80% lower in other countries than in the U.S.^{12,13} Independent studies and over a decade of experience have demonstrated the safety of domestic and international online pharmacies approved in rigorous programs such as PharmacyChecker's.¹⁴

A voluntary agreement of particular concern is one established by a group of Internet and credit card companies called the Center for Safe Internet Pharmacies, or CSIP. While CSIP has been effective at taking down some rogue pharmacies, it also acts to discourage Americans from accessing safe, affordable pharmacies outside the United States. CSIP uses a company called LegitScript to help it identify rogue sites for "take down" and to power an online tool for consumers to look up the status of an online pharmacy. Unfortunately, if you use this tool to look up any online pharmacy operating in any country other than the U.S., such as Canada, it will tell you that pharmacy is "unapproved," regardless of the fact that it may be licensed, require a prescription, and safely selling only genuine medication. The CSIP website has become a clearing house for information from pharmaceutical industry-funded groups such as The

¹ of 10- Gabriel Levitt, Vice President, PharmacyChecker.com, LLC, Subcommittee on Courts, Intellectual Property and the Internet, September 18th, "Role of Voluntary Agreements in the U.S. Intellectual Property System."

Partnership for Safe Medicines and the National Association of Boards of Pharmacy (NABP) with scare campaigns conflating all non-U.S. pharmacies with rogue pharmacies. In fact, any pharmacy outside the U.S. which sells to Americans is labeled by NABP as a rogue.

To keep voluntary agreements from misleading Americans, we ask that your committee make sure that CSIP does not discourage Americans from accessing safe and affordable medication online. In particular, we would urge that the basis for defining a “rogue pharmacy” include any of the following, but not simply whether or not it is licensed in the U.S.:

- Intentionally sells adulterated and/or counterfeit medication
- Sells prescription medication without requiring a prescription
- Engages in fraudulent and deceptive business practices
- Does not follow generally accepted safety standards of pharmacy practice
- Sells medication that is not regulated, i.e., not registered by a drug regulatory authority

We would also like to see CSIP and other institutions established under voluntary agreements be more transparent by providing the following information:

- clearly state what recourse companies and people have if their businesses are shut down by actions taken by CSIP;
- provide information on those sites that were shutdown, and the reasons they were shutdown based on applicable intellectual property laws; and
- identify the precise public health risk of a website.

Last, it is important to recognize that voluntary agreements are being afforded considerable market power. To ensure these powers are used properly, we recommend the appointment of an independent Ombudsman to oversee these agreements. The Ombudsman would analyze voluntary agreements to make sure private sector actions aren't blocking Internet competition and are consistent with the Administration's other goals of due process, free speech, and transparency.^{vi}

I have provided the Committee with a transcript of this presentation and included our public comments submission to the United States Patent and Trademark Office in **Exhibit A**.

Thank you for your time.

¹ See Request of the United States Patent and Trademark Office for Public Comments: Voluntary Best Practices Study. 78 FR 37210. <https://www.federalregister.gov/articles/2013/06/20/2013-14702/request-of-the-united-states-patent-and-trade-mark-office-for-public-comments-voluntary-best> [Last accessed online 9-17-2013].

ⁱⁱ “The Commonwealth Fund 2012 Biennial Health Insurance Survey”. *The Commonwealth Fund*. See <http://www.commonwealthfund.org/Publications/Fund-Reports/2013/Apr/Insuring-the-Future.aspx> (Last accessed 7/22/2013).

ⁱⁱⁱ Cohen RA, Kirzinger WK, Gindi RM. Strategies used by adults to reduce their prescription drug costs. NCHS data brief, no 119. April 2013. Hyattsville, MD: National Center for Health Statistics. 2013. See <http://www.cdc.gov/nchs/data/databriefs/db119.pdf>. (Last accessed 7/22/2013).

^{iv} See “Savings on Brand Name Drugs Rise to 85% Using Verified Online Pharmacies Outside the U.S., According to PharmacyChecker.com — Consumers Told How to Avoid Rogue Pharmacies <http://www.pharmacychecker.com/news/online-pharmacy-prescription-savings-2012.asp>.”

^v See Bate, Roger and Ginger Zhe Jin, Aparna Mathur. “Unveiling the Mystery of Online Pharmacies: An Audit Study.” *The National Bureau of Economic Research*. March 2012. See <http://www.nber.org/papers/w17955>. [Last accessed 8/10/2012]

^{vi} Ibid.

Exhibit A



August 20th, 2013

Teresa Stanek Rea
Acting Under Secretary of Commerce for Intellectual Property and Acting Director of the United States Patent and Trademark Office

RE: Request of the U.S. Patent and Trademark Office for Public Comments: **Voluntary Best Practices Study**

Docket #PTO-C-2013-0036

Gabriel Levitt, Vice President, PharmacyChecker.com, LLC

Founded in 2003, PharmacyChecker.com verifies online pharmacies, provides drug price comparisons among verified online pharmacies, and advocates for expanding access, online and off, to safe and affordable medication. Our main mission is to help Americans find the lowest prescription drug prices offered by safe online pharmacies or discount cards offered by U.S. pharmacy benefit managers. We are a stakeholder in the online business community seeking an open Internet environment that promotes innovation and new business models, especially those that serve the public health. Thus, the main focus herein is to examine the effectiveness of cooperative voluntary initiatives (CVIs) encouraged by the White House Office of the Intellectual Property Enforcement Coordinator (IPEC) as they relate to online pharmacies. The formation of the Center for Safe Internet Pharmacies (CSIP) is often noted as one of IPEC's achievements in encouraging and facilitating the development of CVIs to protect intellectual property on the Internet and its operation will be discussed accordingly.

Reducing intellectual property infringement (IPI) is the goal of IPEC, and CVIs are a part of its strategy to curtail IPI on the Internet. Generally, effectiveness of such efforts is defined by whether or not CVIs are actually reducing IPI. However, it's more complex when it comes to online prescription drug sales than for other types of Internet commerce. For instance, counterfeit handbags do not impact the public health, whereas counterfeit or real medication, which can kill or save lives, respectively, can have a great public health impact. That's why IPEC's main focus when it comes to online pharmacies appears to be protection of the public health, not IPI. The excerpt below, from a March 2011 IPEC document, exemplifies this public health focus:

"On December 14, 2010, White House Intellectual Property Enforcement Coordinator, Victoria Espinel, announced that GoDaddy, Google, Microsoft, Yahoo!, Network Solutions, Neustar, eNom, PayPal, MasterCard, Visa, and American Express have agreed to support an initiative which will start taking voluntary action against illegal Internet pharmacies.

"This fall, Espinel challenged the private sector to voluntarily address the health and safety issues presented by rogue online pharmacies...These discussions culminated in a well-attended, cross-industry meeting at the White House on November 9th, 2010. At that meeting, GoDaddy and Google took the lead on proposing the formation of a private sector 501 (c)(3) non-profit organization dedicated to promoting information sharing, education, and more efficient law enforcement of rogue online internet pharmacies".¹

From this excerpt it's clear that the basis for IPEC's "challenge" and the subsequent formation of CSIP was predicated on "health and safety issues." We believe that this is the proper focus for engaging the private sector to deter and shutdown online pharmacies that intentionally sell counterfeit, adulterated, or substandard medications, or sell real medications but without requiring a prescription. In addition to protecting the public health, violations of intellectual property rights will be curtailed by curtailing online sales of counterfeit drugs.

CVIs against online pharmacies should, at a minimum, *do no harm*, the philosophical foundation of medical ethics. Harm can be caused by CVIs that curtail or block online access by consumers to safe and affordable medication. In fact, any actions that block access to safe and affordable medication are harmful ones. The public health importance of incorporating this truism into metrics for effectiveness of CVIs dedicated to infringing online pharmacies merits a full explanation.

There is a vast and well documented crisis of prescription drug non-compliance in our country, and, according to a CVS/Caremark study the main cause is the cost of medication in the United States.ⁱⁱ Fifty-million Americans ages 19-64 did not fill a prescription due to cost in 2012, up from 48 million in 2010, according to the Commonwealth Fund.ⁱⁱⁱ An analysis of a 2005 study by Kaiser, USA Today, and the Harvard University School of Public Health, found that approximately twenty-five million Americans became sicker from not taking their medications due to cost.^{iv} The FDA estimates \$290 billion in added annual healthcare costs due to prescription non-compliance.^v

Other documented adverse effects from prescription non-compliance include the death of 125,000 Americans who were not adhering to their prescribed heart medication.^{vi} It's likely that hundreds of thousands more die each year from prescription non-compliance for other medications. The numbers above suggest that high drug prices are a major factor in these deaths.

Almost five million Americans personally import medication because of more affordable prices abroad.^{vii} Over the past decade, tens of millions of prescriptions have been ordered online and filled internationally through which Americans have received safe and effective medication: the same medications sold in the United States but at a much lower price. Empirical studies and over a decade of experience show the high degree of safety of personally imported medication from properly credentialed online pharmacies. This remains an inconvenient truth for those who seek to curtail access to such safe online pharmacies. Countless Americans would have gone without needed medication if not for these international and online sources.

A study published in the National Bureau of Economic Research in 2012 called "In Whom We Trust: The Role of Certification Agencies in Online Drug Markets" demonstrates the safety of properly credentialed online pharmacies. The study tracked 370 prescription orders placed with online pharmacies, *both foreign and domestic*. The population of online pharmacies included international and domestic ones credentialed by PharmacyChecker.com, international ones who are members of the Canadian International Pharmacy Association (CIPA), and domestic ones in the National

2 of 10- Gabriel Levitt, Vice President, PharmacyChecker.com, LLC, Subcommittee on Courts, Intellectual Property and the Internet, September 18th, "Role of Voluntary Agreements in the U.S. Intellectual Property System."

Association of Boards of Pharmacy's (NABP) Verified Internet Pharmacy Practice Sites and LegitScript.com programs. The study concluded that all credentialed online pharmacies, foreign and domestic, required a prescription and passed all drug authenticity tests. Of those drugs ordered from non-credentialed online pharmacies, 9% of products were fake or counterfeit medication, all of those for Viagra only.^{viii}

The real health and safety *threat* stems from domestic and international prescription drug orders that are filled by *un-credentialed online pharmacies*, many of which are not safe.

Thus, to maximize positive public health outcomes, CVIs should endeavor to encourage access to *all safe online pharmacies for Americans, including international online pharmacies, while preventing access to dangerous online pharmacies.*

From here we try to address the USPTO's questions in the "Supplementary Information" section:

1. *How should effectiveness of cooperative voluntary initiatives (CVIs) be defined?*

Effectiveness is the degree to which CVIs can reduce and stop access to dangerous online pharmacies while encouraging access to safe online pharmacies, specifically those credentialed by PharmacyChecker.com, Canadian International Pharmacy Association, LegitScript.com and the NABP.

Dangerous and fraudulent online pharmacies are often referred to as "rogue online pharmacies." Unfortunately, the NABP, which represents U.S. pharmacy boards and pharmacists, defines any online pharmacy that is based outside the United States and sells to Americans as "rogue," regardless of its credentials. NABP publishes a "Not Recommended" list that includes fraudulent and dangerous online pharmacies but also includes some safe international online pharmacies approved in the PharmacyChecker.com Verification Program because they are not based in the U.S.^{ix} We believe this conflates the problem of "real" rogue online pharmacies (which hurt consumers) with the practice of safe personal drug importation (which helps consumers). As a practical and ethical matter we believe IPEC should reject NABP's definition of "rogue online pharmacy."

LegitScript.com comes closer to the right classification system for "rogue online pharmacy," but it suffers from too much ambiguity and potential for overreach. Like the NABP, LegitScript.com's program does not allow for the approval of non-US, international, online pharmacies that sell to consumers in the United States. However, to its credit, safe international online pharmacies are *not* classified as "rogue" by LegitScript.com. Instead, safe international online pharmacies, such as those approved by PharmacyChecker.com are generally categorized as "unapproved." The "unapproved" designation is misleading, as it scares consumers who are seeking safe and affordable medication away from safe sources, but at least it distinguishes safe international online pharmacies from "rogue online pharmacies".

A reasonable definition of "rogue online pharmacy" is any website that:

3 of 10- Gabriel Levitt, Vice President, PharmacyChecker.com, LLC, Subcommittee on Courts, Intellectual Property and the Internet, September 18th, "Role of Voluntary Agreements in the U.S. Intellectual Property System."

- 1) Sells prescription medication without requiring a prescription;
- 2) Engages in fraudulent and deceptive business practices;
- 3) Does not follow accepted safety standards of pharmacy practice;
- 4) Intentionally sells adulterated and counterfeit medication.

This definition would certainly describe most online pharmacies that are dangerous but not sweep into its ambit ones that are safe. CVIs are effective when they reduce the volume of, and access to, dangerous online pharmacies.

2. *What type of data would be particularly useful for measuring effectiveness of voluntary initiatives aimed at reducing infringement and what would the data show?*

The answer depends in part on how “infringement” is defined. In the case of online pharmacies “infringement” should be defined within the framework of IPEC’s main goal of protecting the public health. By defining “infringement” as “the intentional sale of counterfeit or adulterated medication, or the sale of genuine and safe medication but without a prescription,” CVIs would target not only the worst offenders, such as criminal networks known to sell counterfeit drugs, but the large majority of websites that the U.S. Food and Drug Administration (and the pharmaceutical industry) seek to put out of business and, in some cases, prosecute.

Using the definition of “infringement” above, the data needed to measure effectiveness would show on a year-to-year basis the reduction in the number of infringing online pharmacies *caused by CVIs* – private sector actions that led to the shutdown of a website that *did not entail any corresponding government action*. It would also show if any non-infringing sites – safe online pharmacies – were inadvertently shutdown by CVIs.

Useful data could be obtained by working with companies, organizations and associations that currently verify online pharmacies, including our company, PharmacyChecker.com, as well as LegitScript, NABP, and CIPA. More data to determine how to classify an online pharmacy could be obtained by conducting mystery purchases from online pharmacies to show if they are rogue or not, such as by using the methods of the National Bureau of Economic Research study mentioned above.

A national survey on consumer purchases of prescription medication would also be helpful in determining the public safety and health ramifications of online pharmacies (good and bad). This would help identify the types of websites that help and hurt the public health. Considering the public health threat that federal authorities see from online pharmacies it should engage the U.S. Centers for Disease Control and Prevention (CDC) by asking CDC to include questions relating to online pharmacy purchases in their National Health Interview Survey. In its last such survey, the following questions were asked of 33,014 Americans ages 18 and over:

“DURING THE PAST 12 MONTHS, are any of the following true for you? ...You skipped

medication doses to save money ...You took less medicine to save money ...You delayed filling a prescription to save money ...You asked your doctor for a lower cost medication to save money ...You bought prescription drugs from another country to save money ...You used alternative therapies to save money.”^{vii}

A survey to determine public health ramifications of online pharmacies could ask: “are any of the following true for you? You ordered medication from another country through an online pharmacy to save money. You ordered medication from a U.S. online pharmacy to save money. You ordered from an online pharmacy that required a prescription from your doctor. You ordered from an online pharmacy that issued you a prescription based on an online questionnaire. You ordered from an online pharmacy that did not require a prescription at all. You received the medication that you ordered. The medication you ordered online worked as you expected. The medication you ordered did not work as expected. You experienced negative health effects after taking the medication ordered online.

LegitScript.com's online pharmacy database already contains tens of thousands of websites identified as “rogue” that can be used as a baseline to measure progress. Encouragingly, its data shows that the number of “not legitimate” sites has decreased over the past year by 10,240 or 23.7%.

| June 24, 2013 | July 23, 2012 |
|--|---|
| 43,075 Internet pharmacies | 32,835 are active Internet pharmacies |
| 225 are legitimate (0.5%) | 279 are legitimate (0.8%) |
| 1,210 are potentially legitimate (2.8%) | 1,512 are potentially legitimate (4.6%) |
| 41,640 are not legitimate (96.7%) | 31,204 are not legitimate (94.6%) |
| Source: LegitScript.com Home Page as viewed on June 24 th , 2013. | Source: LegitScript.com's home page on July 23 rd , 2012, as crawled by Alexa.com. |

The question is how many of these were actually shut down by CVIs, rather than from government actions. The answer is simply those cases where a private company’s action effectively shut down the rogue online pharmacy. Private company actions include refusal of service to rogue online pharmacies by payment processors, domain registrars, and search engines. A LegitScript press release claims that LegitScript has “dismantled over

5 of 10- Gabriel Levitt, Vice President, PharmacyChecker.com, LLC, Subcommittee on Courts, Intellectual Property and the Internet, September 18th, “Role of Voluntary Agreements in the U.S. Intellectual Property System.”

40,000 rogue Internet pharmacies since 2009.”⁶ Since LegitScript doesn’t have legal authority to “dismantle” a company we believe that it has influenced domain registrars to end service to rogue online pharmacies: In other instances, LegitScript may identify for federal agencies those websites that ought to be seized by the government.

To determine what techniques are most effective, Center for Safe Internet Pharmacies, LegitScript.com, or both should enumerate the number of rogue online pharmacies shut down by the different private actions mentioned above.

To prevent inadvertently shutting down safe online pharmacies, and to better assist the Center for Safe Internet Pharmacies and the public, LegitScript.com should provide a breakdown of the number of sites that are classified as *not legitimate* by “rogue” and “unapproved,” since the latter designation, as per the discussion above, usually refers to safe online pharmacies that require a prescription, follow the laws where they operate, and provide affordable medication to Americans.

Effectiveness should also be measured in line with the Obama Administration’s goals that CVIs are “consistent with due process, free speech, privacy of users, and competition” while being as “transparent” as possible. CSIP should make public its protocols for action against infringing online pharmacies and the due process available to those websites targeted for takedown. When a website is shutdown through CVIs it should be informed of the legal basis for the action. CSIP’s website, for example, should:

- 1) clearly state what recourse companies and people have if their businesses are shut down by actions taken by CSIP;
- 2) provide information on those sites that were shutdown, and the reasons they were shutdown;
- 3) identify the precise public health risk of a website; and
- 4) provide the legal basis for determining intellectual property infringement activities of those websites which are shut down, if there are any.

One of the Obama Administration’s goals for CVIs is that they do not stifle competition. There’s an inherent risk in “deputizing” private companies for law enforcement-type activities when such activities could curtail competition and business innovation. Thus, the degree to which CVIs curtail competition and business innovation, especially if such curtailment threatens the public health, must be factored in measuring effectiveness.

Online pharmacies are a relatively new business model for distributing medications and offer a good example to show how CVIs could stifle competition. Online pharmacies provide significant benefits to consumers in terms of cost and convenience. They make it easier for consumers to find companies in different states and countries that operate mail-order pharmacies, providing them more choices and lower prices. Their operations, which can greatly benefit consumers and the public health, challenge existing pharmacy business models. Entrenched business interests often seek to stifle new competition. For example,

⁶ of 10- Gabriel Levitt, Vice President, PharmacyChecker.com, LLC, Subcommittee on Courts, Intellectual Property and the Internet, September 18th, “Role of Voluntary Agreements in the U.S. Intellectual Property System.”

on behalf of U.S. chain pharmacies, the National Association of Chain Drugstores has lobbied the government to stop Americans from buying lower cost medication from Canada and other countries for over a decade^{xi}. For drug companies it's a commercial imperative to segment national markets by preventing them from parallel trade of pharmaceuticals, especially in protection of the U.S. market from which they derive the greatest profits. Furthermore, international drug price transparency serves to advantage consumers vis a vis drug companies as it gives rise to the former's advocacy for lower domestic drug prices. Like U.S. pharmacies, but for somewhat different reasons, the pharmaceutical industry lobbies the U.S. government to prevent Americans from buying lower cost medication from licensed Canadian or other international pharmacies for their personal use.^{xii}

The discussion above is necessary because drug companies and U.S. pharmacies are lobbying the government to promote CVIs that stifle the development of international online pharmacies. In the case of the Center for Safe Internet Pharmacies, some of its member companies pay LegitScript.com to assist them in taking actions against online pharmacies. However, LegitScript.com is a steering committee member of the Alliance for Safe Online Pharmacies, a group that is funded by the NACDS and Eli Lilly;^{xiii} both are engaged in lobbying Congress and federal agencies to stop Americans from personal drug importation. This interplay of private action to bring about CVIs will no doubt disadvantage consumers in areas other than online pharmacy.

To prevent CVIs from anticompetitive policies and actions, we recommend an **independent** ombudsman. For example, the CVI ombudsman would be someone with neither a financial interest nor alignment with pharmacy or pharmaceutical companies nor a federal or state regulator. The CVI Ombudsman will analyze CVIs to make sure private sector actions aren't blocking Internet competition and innovation. As part of his or her efforts the CVI Ombudsman would determine the negative effects to the public health of CVIs.

We understand that while the main goal of IPEC in combatting rogue online pharmacies is protecting the public health it's also concerned with online IPI. For the sake of effectiveness and transparency, IPEC should clearly, and with the greatest specificity, identify what practices by rogue or other online pharmacies constitute intellectual property violations. Only then can we measure how effectively CVIs are protecting intellectual property rights.

3. If the data is not readily available, in what ways could it be obtained?

LegitScript's data is useful for measuring a reduction in the number of active rogue online pharmacies. As stated above, it should go one step further and show the number of "illegitimate" online pharmacies that are not rogue but classified as "unapproved" since many of those are safe and should not be subject to takedown actions by CVIs.

Please also refer to the recommendation above for the CDC to conduct a national survey of Americans who buy medication online.

7 of 10- Gabriel Levitt, Vice President, PharmacyChecker.com, LLC, Subcommittee on Courts, Intellectual Property and the Internet, September 18th, "Role of Voluntary Agreements in the U.S. Intellectual Property System."

4. Are there particular impediments to measuring effectiveness, at this time or in general, and if so, what are they?

There may be a lack of political will to actually determine the public health effects of online pharmacies because they are inconveniently positive. Indeed, millions of prescriptions have been safely filled internationally by Americans through online pharmacies, despite the fact that under most circumstances they may have broken the law or violated intellectual property rights. Keeping in mind the tens of millions of Americans who skip filling prescriptions due to cost, what are the public health effects if such access is blocked?

The dangers of rogue online pharmacies – “rogue” as defined by LegitScript.com – are very clear and compelling. Publicizing patient harm from such websites would 1) deter Americans from buying from them, and 2) clarify those sites that need to be shutdown to protect the public health.

5. What mechanisms should be employed to assist in measuring the effectiveness of voluntary initiatives?

As stated above, identifying the specific private actions taken under CVIs that led to the shutdown or dismantlement of rogue online pharmacies will be helpful. For example, out of the 40,000 rogue online pharmacies dismantled by LegitScript.com, it should be determined how many such takedowns occurred via domain registrars refusing service to rogue online pharmacies vs. payment processors refusing to service them.

6. Is there existing data regarding efficacy of particular practices, processes or methodologies for voluntary initiatives, and if so, what is it and what does it show?

The number of rogue online pharmacies has diminished, according to LegitScript.com, and many through CVIs. The processes include identifying rogue online pharmacies to domain registrars, payment processors and search engines and asking them to refuse service to such websites, effectively dismantling them.

ⁱ “Counterfeit Pharmaceutical Inter-Agency Working Group Report to the Vice President of the United States and Congress.” Executive Office. Prepared by the Office of the Intellectual Property Enforcement Coordinator. March 2011, page 9. See http://www.whitehouse.gov/sites/default/files/omb/IPEC/Pharma_Report_Final.pdf [Last accessed 8/14/13].

ⁱⁱ “CVS Caremark Study Says Cost is Biggest Barrier to Prescription Adherence”. 2012. CVS Caremark Cooperate: <http://www.cvs-caremarkfyi.com/blogs/cvs-caremark-survey-says-cost-biggest-barrier-prescription-adherence>. (Last accessed 7/22/13).

ⁱⁱⁱ “The Commonwealth Fund 2012 Biennial Health Insurance Survey”. *The Commonwealth Fund*. See <http://www.commonwealthfund.org/Publications/Fund-Reports/2013/Apr/Insuring-the-Future.aspx> (Last accessed 7/22/2013).

^{iv} “USA Today/Kaiser Family Foundation/ Harvard School of Public Health Care Costs Survey, 2005”. *The Kaiser Family Foundation*. See <http://www.kff.org/newsmedia/upload/7371.pdf> (Last accessed 8/10/2012). Twenty percent of survey respondents reported not filling a prescription due to cost; and 54% of those said their condition got worse as a result. Extrapolated to the 2012 population of adults 18 and older, which is 234,564,071, the number is 25 million.

^v U.S. Food and Drug Administration. 76 FR 12969. March 2011. Campaign To Improve Poor Medication Adherence: <https://www.federalregister.gov/articles/2011/03/09/2011-5287/campaign-to-improve-poor-medication-adherence-u18>. (Last accessed 8/10/12)

^{vi} McCarthy, R. “The Price You Pay for the Drug Not Taken”. *Business Health 1998*. See http://findarticles.com/p/articles/mi_m0903/is_n10_v16/ai_n27541896/. (Last accessed 8/10/2012)

^{vii} Cohen RA, Kirzinger WK, Gindi RM. Strategies used by adults to reduce their prescription drug costs. NCHS data brief, no 119. April 2013. Hyattsville, MD: National Center for Health Statistics. 2013. See <http://www.cdc.gov/nchs/data/databriefs/db119.pdf>. (Last accessed 7/22/2013).

^{viii} Bate, Roger and Ginger Zhe Jin, Aparna Mathur. “Unveiling the Mystery of Online Pharmacies: An Audit Study”. *The National Bureau of Economic Research*. March 2012. See <http://www.nber.org/papers/w17955>. (Last accessed 8/10/2012)

^{ix} National Association of Boards of Pharmacy publishes a list of “Not Recommended Sites” found here: <http://www.nabp.net/programs/consumer-protection/buying-medicine-online/not-recommended-sites> (Last accessed 8/12/2013). All sites on the list are defined as “rogue”. The definition of “rogue” can be found here: <http://www.nabp.net/programs/consumer-protection/buying-medicine-online/why-not-recommended/>. Online pharmacies that are safe and approved by PharmacyChecker.com appear on this list alongside dangerous websites that intentionally sell counterfeit and adulterated medication and/or do not require a prescription.

^x “LegitScript Shuts Down 6,700 Rogue Internet Pharmacies.” LegitScript Press Release dated June 28th, 2013. See <http://online.wsj.com/article/PR-CO-20130628-909470.html> (Last accessed 8/12/2013)

^{xi} Kocot, S. Lawrence, Senior Vice President and General Counsel, National Association of Chain Drug Stores. April 5th, 2004. Statement on Importation of Prescription Drugs Prepared for United States Department of Health and Human Services Task Force on Drug Importation. <http://archive.hhs.gov/importtaskforce/session2/presentations/NACD.pdf> [Last accessed 8/13/13].

9 of 10- Gabriel Levitt, Vice President, PharmacyChecker.com, LLC, Subcommittee on Courts, Intellectual Property and the Internet, September 18th. “Role of Voluntary Agreements in the U.S. Intellectual Property System.”

^{xii} Ismail, M. Asif. "Drug Lobby Second to None: How the Pharmaceutical Industry Gets its Way in Washington." July 7th, 2005. The Center for Public Integrity. <http://www.publicintegrity.org/2005/07/07/5786/drug-lobby-second-none> [Last accessed 8/13/2013]. Also: Peter Baker. "Obama Was Pushed by Drug Industry, E-Mails Suggest." June 6, 2009. New York Times. <http://www.nytimes.com/2012/06/09/us/politics/e-mails-reveal-extent-of-obamas-deal-with-industry-on-health-care.html?pagewanted=all&r=0> (Last accessed 8/12/2013)

^{xiii} See Alliance for Safe Online Pharmacies "Who We Are" web page: <http://safeonlinerx.com/about-us/who-we-are/> [Last accessed 8/14/2013].

Mr. COBLE. Thank you, Mr. Levitt.
Mr. Barchiesi.

**TESTIMONY OF ROBERT C. BARCHIESI, PRESIDENT,
THE INTERNATIONAL ANTICOUNTERFEITING COALITION**

Mr. BARCHIESI. Chairman Coble, Ranking Member Watt, Members of the Subcommittee, thank you for the opportunity to appear before you today. I am proud to be representing the Intellectual AntiCounterfeiting Coalition and our partners from the financial industry. My testimony today will address our ongoing collaboration regarding the trafficking of counterfeit and pirated goods online.

With over 230 members that span across industries, the International AntiCounterfeiting Coalition is one of the world's largest organizations representing the interests of companies concerned with trademark counterfeiting and intellectual property theft.

While legitimate retailers increasingly leverage the Internet as a platform for sales, the same is true of counterfeiters. Once confined to brick and mortar shops, the Internet has created new opportunities for the sale of illegal goods as well as an ever-widening pool of customers. Additionally, the shift to online distribution has raised a variety of practical difficulties for our enforcement against criminals who operate with anonymity and beyond the jurisdiction of U.S. courts or law enforcement.

The proliferation of this illicit trade threatens consumer confidence in the legitimacy of the Internet as a commercial platform. Consumers expect and deserve the honest cooperation of all of the players in the e-commerce ecosystem. That point of view has driven our partnership with the financial industry and informed the development of our ongoing collaboration.

In January 2012, the IACC launched its payment processor program in collaboration with some of the largest multi-national brands and leading financial companies. This launch followed the establishment of a set of best practices facilitated by the Administration's Intellectual Property Enforcement Coordinator, Victoria Espinel.

The program is, in laymen's terms, a "follow the money" approach that seeks to diminish the ability of criminal counterfeiters to turn a profit. Our program is dependent on the financial partners' policies which prohibit merchants from using financial services for illegal transactions. Merchants that sell counterfeit goods violate those policies and as such, subject themselves to remedial action, including termination of their merchant accounts. Because those policies apply to merchants regardless of their jurisdiction, the program has a global reach.

At its inception, the IACC and its partners identified several goals for the IACC payment processor program. These include increasing the cost of doing business for and decreasing the profits to the counterfeiters; shrinking the universe of merchant banks willing to do business with those sellers; facilitating an efficient use of resources by both rights holders and our financial partners; and dismantling counterfeit networks by developing deeper intelligence on those networks' methods of operating.

In the context of these goals, the program has been a resounding success. We have referred nearly 7,500 Web sites for investigation, resulting in the termination of over 2,100 individual counterfeiters' merchant accounts which likely correspond to a much higher number of affected sites.

The collaboration between the IACC and its partners has resulted in opportunities to provide training to banks and others all around the world. While there remain challenges to quantifying the impact of this program on the overall availability of counterfeit and pirated goods online, there is significant anecdotal evidence that online sales of such illicit product are becoming more difficult.

Further, the program has created a growing pool of data that may be leveraged by both public and private sectors. Since the launch of our program, we have seen a number of trends, including a decline in the use of traditional credit card payments in favor of alternate payment methods; the misuse of anti-fraud measures in an attempt to thwart legitimate investigations by law enforcement and private industry; and the shift from the use of individual merchant accounts to reliance on illegitimate and sophisticated payment service providers who provide full service infrastructure for illegal sales and promise bulletproof processing.

It is our hope that this paves the way for further cross-industry collaboration. The success of this program proves that when rights holders and others work side-by-side to ensure a safe and trusted marketplace, everyone wins.

[The prepared statement of Mr. Barchiesi follows:]

Written Testimony of
Robert C. Barchiesi
President

On Behalf of
The International AntiCounterfeiting Coalition

The Role of Voluntary Agreements
in the U.S. Intellectual Property System

United States House of Representatives
Committee on the Judiciary
Subcommittee on Courts, Intellectual Property, and the Internet

September 18, 2013

Chairman Coble, Vice Chairman Marino, Members of the Subcommittee:

Thank you for the opportunity to appear before you today. I am proud to be representing the International AntiCounterfeiting Coalition (“IACC”) and our partners from the financial industry. My testimony today will address our ongoing collaboration regarding the trafficking of counterfeit and pirated goods online.

With a membership composed of over 230 corporations, trade associations, and professional firms, and founded over 30 years ago, the International AntiCounterfeiting Coalition is one of the world’s oldest and largest organizations representing exclusively the interests of companies concerned with trademark counterfeiting and the related theft of intellectual property. The members of the IACC represent a broad cross-section of industries, and include many of the world’s best-known companies in the apparel and luxury goods, automotive, software, tobacco, electronics, consumer goods, entertainment, pharmaceutical, and other product sectors. The IACC is committed to working with government and industry partners in the United States and abroad to strengthen IP protection and enforcement, and to raise awareness regarding the range of harms caused by counterfeiting and piracy.

Our current financial industry partners include: MasterCard, Visa International, Visa Europe, PayPal, American Express, Discover / PULSE / Diners Club, MoneyGram, and Western Union. In addition, there are currently thirty-three rights-holder participants from a variety of product sectors, including apparel, footwear, and luxury goods, electronics, automotive, tobacco, pharmaceutical, business and entertainment software, and consumer products.

Background

While legitimate retailers increasingly leverage the Internet as a platform for sale and distribution of their goods to consumers, the same is true of counterfeiters. Where such illicit activity was once confined to brick-and-mortar shops, the Internet's maturation as a commercial platform has created new opportunities for sales and advertising of illegal goods, as well as an ever-widening pool of potential customers. According to data provided by MarkMonitor, in the past decade, there have been approximately 2 billion new Internet users, representing a 425% growth since 2000. In 2010, 1 in 4 consumers reported that they had used the Internet for shopping. It is anticipated that the number of Internet users, and accordingly, the number of Internet shoppers, will only continue to grow in the coming years.

As the Committee is well aware, the shift to online distribution has raised a variety of practical difficulties for those seeking to enforce their rights against individuals who are able to operate with relative anonymity, and beyond the jurisdiction of U.S. courts or law enforcement. The proliferation of this illicit trade online poses a threat to consumers' confidence in the legitimacy of the Internet as a commercial platform. As such, addressing these problems is in everyone's interest, and is the responsibility of all of the players in the e-commerce ecosystem. Consumers expect, and deserve, the honest cooperation of all of the parties involved in the online market. That point of view has driven our partnership with the financial industry, and informed the development of our ongoing collaboration.

Voluntary Collaborative Efforts Between the IACC and Financial Industry

In January 2012, the IACC launched its Payment Processor Program in partnership with some of the world's largest multinational brands and leading financial companies. This launch followed the establishment of a set of best practices, facilitated by the Administration's Intellectual Property Enforcement Coordinator, Victoria Espinel. The program was developed with the recognition that e-commerce involves a number of

natural choke-points that can be effectively targeted to combat illegal activities. The program is, in layman's terms, a "follow-the-money approach" that seeks to diminish the ability of criminal counterfeiters to process online payments, thereby decreasing the profitability of their illicit businesses.

The main objective of the Payment Processor Program is to provide a streamlined, simplified procedure that allows rights-holders to report online sellers of counterfeit or pirated goods directly to financial companies in a more time- and cost-efficient manner, thereby facilitating action against the corresponding merchant accounts and diminishing the ability of such sellers to profit from their illicit sales. To implement this program, the IACC has developed an access-controlled portal system to facilitate the flow of information between and among participating rights-holders, the IACC, the National Intellectual Property Rights Coordination Center (the "IPR Center"), and financial partners, utilizing a master IACC portal as the clearinghouse for such information. The portal system contains analytical tools, as well as a reporting mechanism that provides disposition results and statistical data to the reporting rights-holders.

Our program is dependent on the financial partners' policies, which prohibit merchants from using financial services for illegal transactions. Merchants that sell counterfeit goods violate those policies, and as such, subject themselves to remedial action, including termination of their merchant accounts. Because those policies apply to merchants regardless of their jurisdiction, the program has global reach.

Evaluating Effectiveness

At its inception, the IACC and its partners identified several goals for the IACC Payment Processor Program. These include: increasing the cost of doing business for, and decreasing the profits to, the counterfeiters; shrinking the universe of third-party acquiring banks willing to do business with known, high-risk merchants; facilitating an efficient use of resources by both rights-holders and our financial partners – for

example, by providing a standardized format for reports and deduplicating multiple reports by more than one rights-holder; and disrupting and dismantling counterfeit networks by developing deeper intelligence on those networks' methods of operating.

In the context of these goals, the IACC Payment Processor Program has proven to be a resounding success since its launch in 2012. To date, participants in the program have referred nearly 7,500 websites for investigation, resulting in the identification of over 26,000 payment channels, and the termination of over 2,100 individual counterfeiters' merchant accounts. Because counterfeiters frequently use a single merchant account to accept payments for multiple sites, the number of affected sites is likely significantly higher. In addition to such data, the collaboration between the IACC and its partners in the program has resulted in several opportunities to provide training to banks and others around the world on relevant issues.

While there remain obvious challenges to quantifying the impact of this program on the overall availability of counterfeit and pirated goods for sale online, there is significant anecdotal evidence that online sales of such illicit products are becoming more difficult. Further, the program has created a growing pool of empirical data that may be leveraged by both the public and private sectors to more effectively target their efforts in terms of traditional enforcement and to develop appropriate policy responses to such trafficking. For example, since the launch of our program, we've seen a number of trends including: a shift away from the use of traditional credit card payment systems to alternate payment methods, and in some cases to the use of virtual currencies; the misuse of anti-fraud measures in an attempt to thwart legitimate investigations by law enforcement and private industry; and a shift from the use of individual merchant accounts to reliance on illegitimate and sophisticated payment service providers who provide full-service infrastructure for illegal sales and promise "bullet-proof processing."

It is our hope that this paves the way for further cross-industry collaboration. The success of the program proves that when rights-holders and others work side-by-side to ensure a safe and trusted marketplace, everyone wins.

For a more in-depth discussion of the LACC Payment Processor Program, including a review of the first year statistics and an evaluation of the successes and challenges of the program to date, see

<http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf>.

Mr. COBLE. Mr. Barchiesi, I know you weren't advised that you were going to be here until rather late in the game, but you brought it up to speed. Folks, we try to apply the 5 minute rule to ourselves so I will keep my questions in a very terse way.

Mr. Sherman, are voluntary agreements a better approach to solving issues in lieu of legislation for companies that want to do the right thing on the one hand in contrast to companies that simply want to take advantage of intellectual property owners?

Mr. SHERMAN. I am sorry, I heard the first part of the question but not the last.

Mr. COBLE. Are voluntary agreements a better approach in resolving these problems?

Mr. SHERMAN. I have been a big fan of voluntary agreements. We have seen what happens with legislation. We are carving in stone certain standards, certain processes, certain expectations, and everybody gets nervous on each side. It becomes very, very difficult to agree on that.

With voluntary agreements, you can be flexible. You can agree on things, knowing that they can change without going back to Congress. You have the ability to learn from the marketplace what is working and what is not and modify the agreement, so there is flexibility, there is an ability to change as you go, and there is an ability to learn from experience. I think it makes people a lot more willing to try things and it begins to build trust.

So, yes, I think that for a start, voluntary measures are a great way to begin basically closing the gap between the business side of the Internet and the content side of the Internet.

Mr. COBLE. Thank you, Mr. Sherman.

Ms. Lesser, what role, if any, should the U.S. Government agency exercise with these arrangements are being negotiated while they are in effect?

Ms. LESSER. I am sorry, Mr. Chairman, what role are the agencies playing now?

Mr. COBLE. What role should there be, if any, for U.S. agencies while these agreements are playing out or are in effect?

Ms. LESSER. As several of the witnesses have said, you know, the leadership of Victoria Espinel, when she was the Intellectual Property Enforcer at the White House, was very, very important and continued to be important not only as the negotiators came up with this agreement, but as we moved toward implementation.

I think as Federal agencies, Congress has a very important oversight role in helping us do what we want to do well. At the same time, as we look to evaluating the program and what changes need to be made, we are doing that on an ongoing basis, and as Mr. Sherman just said, we are very able to be very nimble and respond to the needs of the program on really a regular basis.

So I think oversight should continue. There should be hearings like this. I don't think there should be a rubric where there are consistent requirements for voluntary programs to report to the government however.

Mr. COBLE. Mr. Rothenberg, what say you to this?

Mr. ROTHENBERG. It would be very hard for me to improve on the way Mr. Sherman articulated, although I am forced to try a little bit. But the voluntary agreement, self-regulation by industry has

the benefit of being able to be more flexible in the pursuit of its objectives. Legislation and regulation have a tendency to fix in stone certain methods by which infringements have to be identified and punished. And technology, especially the infringers and especially those infringers outside our borders, will find new ways to evade them. It can be much, much more effective, certainly in the short and medium term, to get widespread adoption of voluntary agreements, in turn, industry participants, especially the largest and the most legitimate industry participants, into the police of the industry itself. We think that could uncover lots of infringements and help create a self-reinforcing system of abeyance.

Mr. COBLE. I thank you for that. Mr. Levitt, do you want to weigh in on this?

Mr. LEVITT. Once again, I think that commonsense voluntary agreements can be helpful. I come with a perspective that over time you could see entrenched interests who come together in carrying out these voluntary agreements could take actions that will stifle the emergence of other companies if there is not oversight. So I think that all of the people here have given good examples of how voluntary agreements can work and have worked, but there is an inherent risk when you deputize the private sector to take on a roll that I think you guys, I am sorry, you had tried to do through passing other laws, and I think there should be some oversight, there should be an independent ombudsman who is reviewing all of these voluntary agreements to make sure that they are transparent and not stifling competition.

Mr. COBLE. Well, my red light has illuminated, so I will recognize Mr. Watt from North Carolina.

Mr. WATT. Thank you, Mr. Chairman. As has been my practice, I am going to defer and go last in the queue and defer to Mr. Johnson. Mr. Conyers disappeared on me. He was there and then he disappeared.

Mr. JOHNSON. Well, your pause gave me a moment of concern.

Mr. WATT. You mean, you thought I had forgotten your name?

Mr. JOHNSON. Or something worse.

Mr. WATT. I defer to whoever this guy is. I defer to Mr. Johnson and I will go last in the queue.

Mr. JOHNSON. Thank you, Mr. Ranking Member, and thank you, Mr. Chairman.

Today's hearing represents another opportunity for this Subcommittee to discuss how innovative market-place solutions are protecting copyright holders. Recently the White House Office of the IP Enforcement Coordinator joined with Google, Yahoo, AOL, Microsoft and the Interactive Advertising Bureau and other ad networks to announce the completion of voluntary best practices guidelines for ad networks to address piracy and counterfeiting. These industry guidelines are also the product of several years of coordinated efforts and represent a follow-the-money approach to stopping rogue sites dedicated to intellectual property theft.

To demonstrate the magnitude of this problem, in 2012, Google disabled ads that served 46,000 sites for violating Google's policies on copyright infringing content. Google shut down more than 82,000 accounts for attempting to advertise counterfeit goods,

which were almost entirely discovered through Google's engineering to protect copyrighted works.

So I want to—and I also commend Victoria Espinel, the former U.S. Intellectual Property Enforcement Coordinator, on her hard work during her tenure.

Needless to say, copyright theft hurts everyone. Songwriters and artists depend on royalties for their livelihood and companies depend on protection so that they can make new content and products, and consumers want to know that when they purchase a good that it isn't counterfeit.

Alarmingly, a recent study commissioned by NBC Universal indicates that copyright infringement grows proportionally with Internet usage. But this isn't altogether surprising. There is a strong temptation to illegally download a copyrighted work without accessible alternatives to infringement. Regardless, there are serious challenges that continue to face movie studios, music companies and other industries.

Mr. Sherman, please describe some of the challenges facing artists, producers and songwriters, and also how does copyright infringement affect the ability for music labels to cultivate new and unproven talent?

Mr. SHERMAN. Well, the challenge is how you make a living when one of the basic forms of revenue for musicians, songwriters, publishers, labels is basically going away as people are able to get for free what they previously had to pay for. It just means that you are going to be doing a lot more live touring. You are going to be looking at alternative revenue streams. You are no longer going to be relying on CD sales or downloads in order to make a living. And because live touring is a hard life and because these alternative revenue streams are growing very slowly, it means the opportunities to be able to make a living in music is compromised.

Hopefully it will get better, and certainly the Internet has provided a level playing field where any musician can find a world-wide audience, so there is great opportunity. There is just a lot of difficulty in monetizing that opportunity so that you can actually eat and raise a family and send your kids to college.

So it is tough. And the labels, which are now 40 to 50 percent the size that they used to be, and about 40 percent the number of employees, have less money to invest in new artists. They have less money to promote them, less money to market them and less money to keep them on the label hoping that the next album will do a little bit better or the third album will do a little bit better. It is just a much tougher business.

Mr. JOHNSON. I see. So becoming a full-time musician, songwriter, performer, is getting much more difficult, and for the labels to be able to exploit that talent, it is very difficult to do when all of your product is being distributed in a way that you cannot collect any revenue from?

Mr. SHERMAN. Exactly right.

Mr. JOHNSON. So how has this access to illegitimate means of capturing this content, explain the consumer behavior that is behind that?

Mr. SHERMAN. Consumers, especially the younger generation, have grown up to believe that anything on the Internet is free. It

is the way it started and it has become an expectation. It is something that has to change over time, not only for music, but for all the content industries to be able to flourish, and I think it will change over time, but it will take awhile until there is a cultural shift on that.

So at this point the ease with which a music fan can get an illegal copy of music or illegal streams of movies or television shows has basically changed the expectation with respect to the value of music and entertainment. And that is a devastating thing when the value of music and other forms of entertainment are killed off because at that point, the pricing that legitimate services can charge becomes not enough to support the infrastructure necessary for investment and artists, new content, movies, television shows and the like.

Mr. JOHNSON. Thank you, Mr. Chairman.

Mr. COBLE. The gentleman's time has expired.

The distinguished gentleman from Texas, Mr. Poe, is recognized for 5 minutes.

Mr. POE. Thank you, Mr. Chairman. Thank you all for being here.

There is a phrase that brings fear and trepidation into the hearts and souls of men and women across the country and that is "We are from the government and we are here to help you." Whether it is a business or whether it is an individual, I mean, I have always thought that and I am part of the government and I really think that now, that that is a great concern among people.

We have in your all's situation a process that is working where different entities get together and follow contract law, something that is preserved in the Constitution, the right to contract.

I think it is working fairly well in your situation.

My question is does the government—should we legislatively now jump in the middle and sort things out and make it better? I mean, by "better," I mean that factiously. Would it make it worse, or would it make it better? Or should we continue to encourage the ability to contract and work out in the marketplace disagreement and compromise, something that we don't do too well here, Congress, compromise.

So I just kind of open that question up, and I would like to hear all five of your opinions on that role of government, if any. Ladies first.

Ms. LESSER. Well, I will speak from the perspective of my program, which, as I said during my testimony, has only been in operation for 6 months. I think what we found during the implementation process, which took more than 18 months, was that the negotiators who were at the table for 3 years coming up with the framework for our contract, our Memorandum of Understanding, and for the copyright alert system, didn't really know all of the elements that should ultimately go into the program. And so the 18 months we spent doing research, looking at the implementation, looking at the words in the contract, and in some cases changing those words so that we could make sense of the implementation, I think shows me that that collaborative process really allowed us to respond to the needs of the marketplace, to be flexible, and, most importantly, to work with our consumer advisory board.

Many people on that advisory board were really the people sitting across the table from the content industry during the renowned SOPA debate, and here they were at a table with us envisioning and constructing a program that we think is working well.

Now, we only have 6 months under our belt, so the next part of the answer is that we have to wait and see. We are already—I will give you an example. We have, as I said, an appeal process. The American Arbitration Association is overseeing that process. So if a consumer thinks that an alert has been sent in error, and they file an appeal, the American Arbitration Association is assigning copyright lawyer neutrals to adjudicate that appeal, not in a traditional sense of adjudication, but within the confines of our program. What we found early on is that indications were that our defense explanations were not that clear. And so immediately—

Mr. COBLE. Ms. Lesser, if you could wrap it up.

Ms. LESSER. Within a month we went back in and redid those defense explanations. So we are changing the program as we go.

Mr. POE. I want everybody to answer that question. Now, you all are down to a minute, 25 seconds apiece or so. So, Mr. Sherman.

Mr. SHERMAN. Do not underestimate the value of government encouragement. I certainly understand the difference between legislation and the imposition of rules. But the role of encouragement can be very, very helpful in getting parties together.

Mr. POE. Get it done, or we are going to do it. And then everybody's going to be—

Mr. SHERMAN. That often helps. Hopefully it won't be necessary, but it does help. So encouragement is important.

Mr. POE. Okay. Mr. Rothenberg.

Mr. ROTHENBERG. Sir, the ad-supported Internet contributes \$530 billion to the U.S. economy. It is responsible for about 5.1 million jobs. Those are based on platforms that have been built on the backbone of the Internet, platforms like eBay and Facebook and Google. They are responsible for jobs. One of most important things this Congress can do is promote our voluntary guidelines in global trade agreements to assure that the rest of the world doesn't shut down these platforms irresponsibly.

Mr. POE. Thank you.

Mr. Levitt.

Mr. LEVITT. I would like to answer that how I think a consumer will—what they might want you to hear. There is a group called RX Rights. That is RxRights.org. It is a coalition that has about 40- to 50,000 people, and they buy drugs, often from Canada, online from verified and safe sites. They don't want the government stopping them from being able to do that, because they know that it is safe because that is what they have been doing. And I think there has to be a balance when we are taking actions to shut down sites selling counterfeit drugs that we don't overreach where real people end up getting hurt because they can't afford their medications.

Mr. POE. Lastly.

Mr. BARCHIESI. We firmly believe in the efficacy of voluntary agreements and this proof of concept. What we do, it works. Our partnership with the financial industry works. But the operative word is it takes a willingness on the other party's side to work together, roll your sleeves up and get it done. We were able to go

over to China and recently put together an agreement with Tow Bow and Alibaba Group.

So I think there is a role with government. I am a bit frustrated that I can't go over to—in California to Google and do the same thing. So I agree with Cary Sherman that I think there is a role for government to play to help encourage these groups to get together and get it done.

Mr. POE. Thank you, Mr. Chairman.

Mr. COBLE. The gentleman's time has expired.

I am pleased to recognize the lady with whom I cochair the Creative Rights Caucus, the distinguished lady from California, Ms. Chu for 5 minutes.

Ms. CHU. Thank you, Mr. Chair.

Before I begin, I would like to submit testimony for the record on behalf of the Copyright Alliance on the role of voluntary agreements. The Copyright Alliance has been a great advocate for the rights of individual creators. So I am happy that they are weighing in on this very, very important hearing. And so that is this. And I would also like to submit for the record this study entitled "Understanding the Role of Search in Online Piracy," commissioned by the Motion Picture Association of America. This report indicates that search engines play a facilitating role, even if inadvertently.

Mr. COBLE. Without objection, they will be received.

[The information referred to follows:]



Testimony of Sandra Aistars, Executive Director, Copyright Alliance

Committee on the Judiciary

Subcommittee on Courts, Intellectual Property and the Internet

U.S. House of Representatives

“The Role of Voluntary Agreements in the U.S. Intellectual Property System”

September 18, 2013

**Testimony by Sandra Aistars, Executive Director, Copyright Alliance
The Role of Voluntary Agreements in the U.S. Intellectual Property System
Before the Judiciary Committee's Subcommittee on Courts, Intellectual Property and the
Internet**

September 18, 2013

The Copyright Alliance is a non-profit, public interest and educational organization made up of artists, creators, and innovators of all types. Our members include artist membership organizations and associations, unions, companies and guilds, representing millions of creative individuals. We also collaborate with and speak for thousands of independent artists and creators and small businesses who are part of our one voice activists network.

The Copyright Alliance welcomes this opportunity to submit testimony for the record of this hearing “The Role of Voluntary Agreements in the U.S. Intellectual Property System.”

The Copyright Alliance enthusiastically supports the use of cross-industry collaborative efforts to address the problem of online infringement. We are concerned, but not surprised by recently released studies such as the NetNames Report “Sizing the Piracy Universe” that reveal that the problem of online piracy is tenacious and persistent.¹ The anecdotal experiences of our members and grassroots members confirm this fact. We agree with the Intellectual Property Enforcement Coordinator (IPEC) that cooperative cross-industry measures are “an effective tool in our multi-faceted approach to fight infringement.”² And as the American Consumer Institute found in a survey of consumer attitudes toward intellectual property released this past July, a majority of the public supports the use of voluntary initiatives.³ The study found that 69% of Internet users supported ISPs voluntarily restricting access to sites involved in online infringement, while 76% of Internet users preferred to be notified by ISPs in the event they had mistakenly downloaded infringing content.

When such initiatives work well, they can reduce and equitably apportion the burden that would otherwise be placed on all stakeholders. Early signs suggest existing initiatives are having a positive effect on reducing infringement and educating users about legal alternatives. However, to date, most initiatives have focused mainly on the audiovisual and music sectors. We therefore encourage the expansion of such initiatives, or the creation of additional best practices that extend to other affected communities of creators and innovators.

¹ David Price, *Sizing the Piracy Universe*, NetNames (September 2013), http://www.netnames.com/Sizing_the_piracy_universe.

² U.S. Intellectual Property Enforcement Coordinator, 2013 Joint Strategic Plan on Intellectual Property Enforcement, p. 37 (June 2013), <http://www.whitehouse.gov/sites/default/files/omb/IPEC/2013-us-ipeec-joint-strategic-plan.pdf>.

³ Erwin A. Blackstone, et al., *Intellectual Property: Facts and Consumer Opinions on Counterfeit and Pirated Goods*, The American Consumer Institute Center for Citizen Research (July 25, 2013), <http://www.theamericanconsumer.org/wp-content/uploads/2013/07/Final-IP-Study-w-Cover.pdf>.

As it examines voluntary initiatives, the Subcommittee should keep the following principles in mind. First, initiatives should strive to be as open as practical to diverse sectors of creators and creative works. Initiatives should also strive to reach all needed participants in the online ecosystem; some notably important participants, such as search engines, remain unaccounted for. When the effectiveness of initiatives are measured, data should always be placed in the proper context; for one, copyright provides vital non-economic benefits to creators that are just as important as the economic benefits, and second, many of the indicators of a successful copyright framework are qualitative and subjective rather than quantitative and objective.

In addition, as ensuring appropriate copyright protections to artists and creators is one of the powers of Congress enumerated in the Constitution, it should play an important role in the oversight and encouragement of voluntary initiatives. Congress should continue to encourage the facilitation of discussions concerning the creation of initiatives through offices like IPEC and continue to monitor the effectiveness of existing initiatives.

The Copyright Alliance reiterates its call to keep the creator front and center during the copyright review process.⁴ As the Subcommittee takes a closer look at this issue, special attention should be placed on examining the viability of cooperative mechanisms for individual creators and small businesses. Remedies remain ineffective if they are out of the reach of these vital constituents. Such creators often lack the resources to seek judicial remedies and have no market leverage. Similarly, an initiative cannot be considered effective if the burden of action falls primarily on the creator; everyone in the online ecosystem has a role to play in creating a fair and sustainable marketplace.

The recently announced Best Practices for Ad Networks to Address Piracy and Counterfeiting illustrate this point well.⁵ Although the Practices are a welcome step in the right direction, we believe they would have benefited from the inclusion of creators — particularly individuals and small businesses — in the drafting process. For example, inclusion of the individual artist perspective in the discussion would have made clear that certain aspects of the procedure created by the Best Practices, such as the requirement for providing detailed data tracing information in order for a notice to be deemed effective, are burdensome for and beyond the reach of these creators, who may not have a working knowledge of technology practices that would be required by the procedures. More effective solutions for the full range of interested parties might be developed with broader participation of affected stakeholders.

Along with considering what specific initiatives do, the Subcommittee should consider what they *don't* do. Initiatives may contain notable gaps; for example, the Copyright Alert System only monitors P2P filesharing but not infringement occurring through cyberlockers or streaming piracy.⁶ Similarly, the Best Practices for Ad Networks only addresses display ads, not video and mobile ads (the latter of which constitute a growth sector in advertising spending), and

⁴ Sandra Aistars, Statement on Today's Hearing on "A Case Study for Consensus Building: The Copyright Principles Project" (May 16, 2013), https://copyrightalliance.org/sites/default/files/aistars_statement_re_judiciary_hearing_final.pdf.

⁵ Available at <http://2013ippractices.com>.

⁶ See Copyright Alert System, Final Memorandum of Understanding (July 6, 2011), available at <http://www.copyrightinformation.org/wp-content/uploads/2013/02/Memorandum-of-Understanding.pdf>.

it only applies to ad networks, not ad exchanges and other major participants in the online advertising sphere.⁷ Keeping such factors in mind when examining an initiative should not suggest that the initiative is ineffective, but may be an indication that if the first initiative has been worthwhile, it is worth examining how it can be adapted and expanded to address additional challenges.

Finally the Subcommittee should consider how closely the duties prescribed by best practices statements align with existing legal duties. Initiatives that spell out duties that are no more than what online actors should already be doing under existing law are little more than window-dressing. The goal of these initiatives should be to provide mechanisms that allow stakeholders to streamline their performance of existing legal duties and avoid unnecessary costs and inefficiencies that would come from enforcement of such obligations through judicial or administrative mechanisms. Effective best practices would be designed to make it as easy as possible for creators to file effective notices of infringement, and for other stakeholders to efficiently address them.

The architecture and scope of the Internet demand a multi-pronged approach to building an effective copyright framework, one in which voluntary initiatives unquestionably belong. The Copyright Alliance is glad to see the IP Subcommittee has recognized their importance and taken the time to examine such initiatives in detail. We look forward to participating in the Subcommittee's work whenever appropriate.

⁷ Best Practices Guidelines for Ad Networks to Address Piracy and Counterfeiting, <http://2013ippractices.com/> (last visited August, 14, 2013) (stating "[t]he term '[Ad Networks]' encompasses only services whose primary business is to broker for compensation the placement of website display advertisements and does not include services which are ad-serving platforms or ad exchanges").

Understanding the Role of Search in Online Piracy

Prepared by Millward Brown Digital for the MPAA



Introduction

The Motion Picture Association of America (MPAA) commissioned Compete to assess the role search plays in how US and UK consumers find copyright infringing copies of TV and film content on the internet. To accomplish the goal of the study, Compete used its online consumer panel to investigate how search is used in the discovery and navigational journey to these infringing content files located across the web. Compete also analyzed whether the algorithm change implemented by Google in August 2012, which incorporated copyright notice levels into its search engine ranking, caused any change in the role that search plays in access to copyright infringing content. The analysis included in this report is based on US and UK consumer data.

Executive Summary

The study identifies that:

- Overall, search engines influenced 20% of the sessions in which consumers accessed infringing TV or film content online between 2010 and 2012.¹
- Search is an important resource for consumers when they seek new content online, especially for the first time. 74% of consumers surveyed cited using a search engine as either a discovery or navigational tool in their initial viewing sessions on domains with infringing content.
- Consumers who view infringing TV or film content for the first time online are more than twice as likely to use a search engine in their navigation path as repeat visitors.
- The majority of search queries that lead to consumers viewing infringing film or TV content do not contain keywords that indicate specific intent to view this content illegally. 58% of queries that consumers use prior to viewing infringing content contain generic or title-specific keywords only, indicating that consumers who may not explicitly intend to watch the content illegally ultimately do so online. Additionally, searchers are more likely to rely on generic or title-specific keywords in their first visit than on subsequent visits.
- For the infringing film and TV content URLs measured, the largest share of search queries that lead to these URLs (82%) came from the largest search engine, Google.
- The share of referral traffic from Google to sites included in the Google Transparency Report remained flat in the three months following the implementation of Google's "signal demotion" algorithm in August 2012.

¹ Methodological detail: Both the relevance and recency of search queries were used to calculate this figure, versus solely attributing influence to the domains that a consumer visited immediately prior to viewing infringing content. This research methodology was used because consumer navigation to infringing content is complex and could include multiple search queries and visits to infringing websites before a user is able to find a working URL. Therefore direct referrals do not fully reflect consumers' navigation paths.

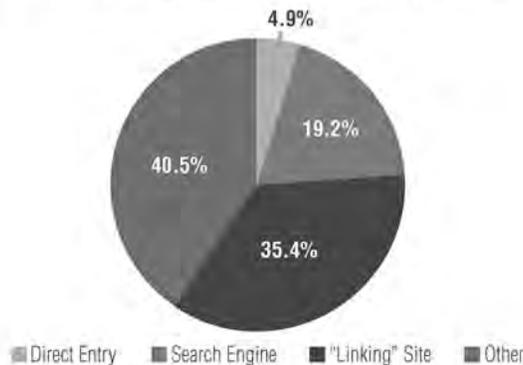
Analysis

The Role of Search

The goal for this study was to understand the role that search engines play in the discovery of and navigation to TV and film content online. Specifically, the study aimed to better understand the online paths consumers utilize when they find and view infringing content. As highlighted in the Methodology section at the end of the study, Compete used a hybrid approach to define the role of search, incorporating both the relevancy of keywords used and the recency of the query in relation to when the infringing content was viewed. The approach established instances of consumers visiting infringing content as endpoints, and then attributed search queries that included a related term and also occurred within a twenty-minute prior window as having influenced the path during which the infringing viewing behavior occurred. This methodology highlights the prevalence of consumers using search engines for content discovery. However, this method did not seek to indicate the degree to which infringing content appears on search engine results pages themselves.

Using this approach, Compete observed that on average, approximately 20% of all visits to infringing content were influenced by a search query from 2010-2012. The level was relatively flat between 2011 and 2012 and up from 2010 (16%). Meanwhile, 5% of sessions were driven by consumers who directly navigated to the website where the content is hosted. 35% of viewing sessions were referred by a linking site such as tv-links.eu, and 41% of these infringing viewing sessions resulted when a user clicked a link on any other type of website like a social network, forum, and blog or used a bookmark.

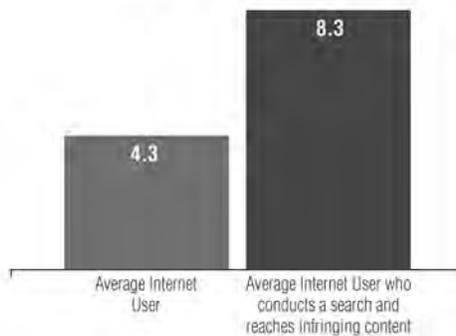
Share of Visits to Infringing Content by Entry Method
(% of Visits to Infringing Content URLs, 2010-2012 Monthly Average)



Search Behavior: How do searchers behave?

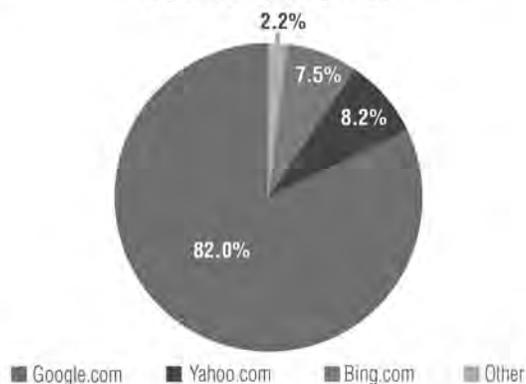
Consumers who use search as part of the path to viewing infringing TV or film content are heavier search users compared to the average internet user. These individuals conduct an average of 8.3 searches during their viewing session versus 4.3 searches for average internet users, equating to 2X more searches during sessions when infringing behavior occurred. While this analysis indicates that search behavior intensifies among consumers who view infringing content, it is also likely that this segment of consumers and this specific online activity are naturally prone to intensified search behavior since online video consumption is a more sophisticated behavior relative to simpler weather or news update searches.

Volume of Search Queries per Session
(Number of Queries per Session, 2010-2012 Monthly Average)



For consumers who conducted a search prior to viewing the infringing content analyzed, 82% navigated through to the content via Google, compared to 16% from Yahoo/Bing and 2% from other engines. Approximately half of consumers that used search to reach infringing content navigated to this content within two to seven minutes, and just under 10% reached the infringing content in less than a minute after conducting a search.

Search Engine Share
 (% of Search Influenced Visits to Infringing Content URLs Driven by Each Major Search Engine, 2010-2012 Monthly Average)



Search Term Analysis: What queries are consumers using to reach infringing content?

There are multiple ways consumers use search engines and reach infringing film and TV content online. This especially depends on the level of knowledge a given searcher has of the infringing ecosystem. This study analyzed the specific keywords used by consumers to reach infringing content, and classified them in the following categories:

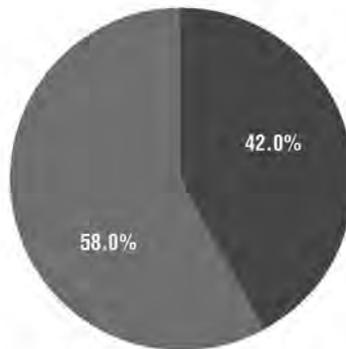
| SEARCH TERM CATEGORY | DEFINITION | EXAMPLES |
|----------------------|--|--|
| PIRACY DOMAIN | Searches that contain specific domains that are known to host or link to infringing content online | 10channel, Megavideo, tv-links, etc. |
| TITLE | Searches that contain titles of recent TV shows and films | Lost, Dark Knight Rises, Game of Thrones |
| GENERIC | Searches that contain phrases related to watching film/TV online | watch tv online, free movies, etc. |

Complete analyzed the role that "Generic Piracy" terms like "cam", "divx", "rip", etc. play in the consumer journey but found that it was not a significant category and did not warrant being broken out separately.

When looking at keyword types, the majority (58%) of searches by consumers who reach infringing URLs contain only "Generic" or "Title" keywords. These searches do not include specific infringing content websites, indicating that these consumers did not display an intention of viewing content illegally. Meanwhile, 42% of searches contain a "Domain" term, indicating that these users know which domains they intend to go to stream or download the content they are interested in. More granular analysis shows that 37% of searches are "Domain Keyword Only" implying that consumers are leveraging search as a navigational tool by inputting the domain name into the search box or URL bar instead of simply going to the site directly. While "Title Keyword Only" searches (8.8%) are not a primary driver to infringing content by themselves, consumers who used these terms (and may not have originally intended to find this type of content) subsequently navigated to a domain where they could view infringing material.

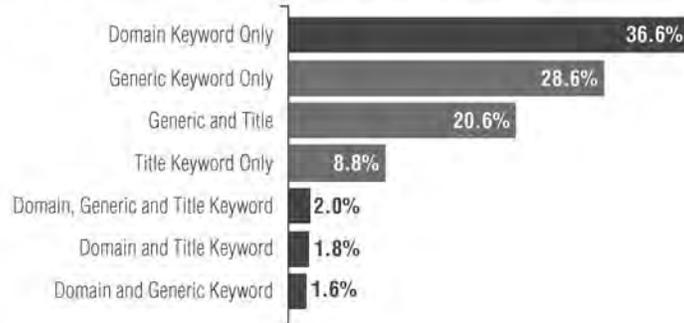
Search Term Keyword Type Distribution

(% of Visits to Infringing Content Referred by Search by Each Search Term Type, 3 Year Average, 2010-2012)



■ Contain "Title" or "Generic" Term Only ■ Contain any "Domain" Term

Search Term Keyword Breakdown
(% of Visits to Infringing Content Referred by Search by Each Search Term Bucket, 3 Year Average, 2010-2012)

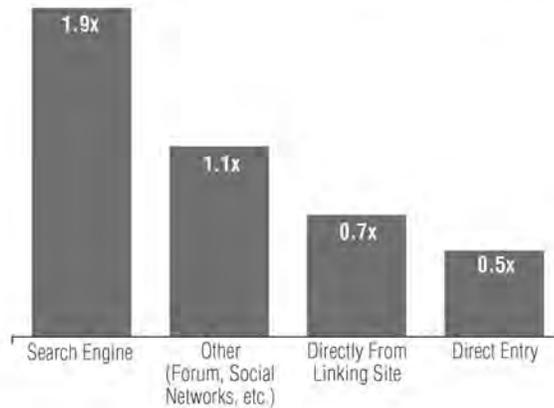


First Time vs. Repeat Infringing Viewing: Does the Role of Search Change?

One of the biggest goals of Compete's research was to understand the different role that search plays for first-time visitors to infringing domains compared to repeat visitors. Do first-time viewers leverage search more heavily in order to locate a site where they can stream or download content and then navigate directly to that site in the future? It is important to isolate these two segments as looking at an average rate of search influence could potentially be understating the real influence search engines play in this area. Repeat visitors could have been influenced by search at one point, but no longer use it. In our view the initial role of search needs to be assessed. To accomplish this goal, Compete used its longitudinal clickstream panel to segment consumers whose online activity was present in three consecutive months into two groups – First Time Viewers and Repeat Viewers.

First Time Views vs. Repeat Viewers

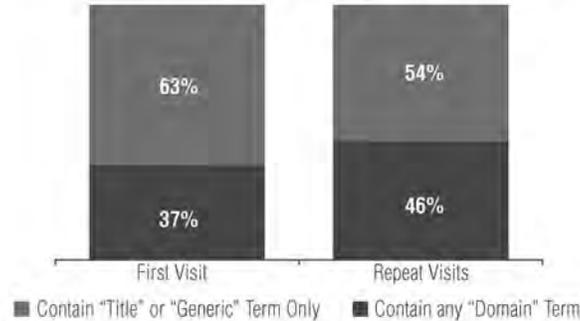
(Lift to each entry method among First Time Visits vs. Repeat Visits, 2010-2012 Monthly Average)



First-time visitors to infringing content were almost 2X more likely to use search on their first visit to infringing content compared to repeat visitors. This confirms that search is principally used for content discovery and is relatively more valuable to consumers who do not know where this content can be found online. This is not surprising and is consistent with other categories of search behaviors. As consumers become aware of content sites, search may play a less direct role than it did during their initial "discovery" session.

In addition to analyzing the clickstream patterns of infringing content viewers, Compele also surveyed consumers to better understand how they discover and navigate to this content and whether search influences their path. Attitudinal responses mirrored the behavioral data; first time visitors indicated that they were 1.6X more likely to use search on their first visit than on repeat visits. 74% of respondents reported that search played a role the first time they visited an infringing content domain, either as a tool for discovery (41%) or navigation (33%), compared to 47% of survey respondents who cited search as being used during later viewing sessions. Note that these responses were not constrained by the five-month window of the observed clickstream data, and represent the respondents' recollection of their first visit.

Search Term Keyword Type Distribution
 (% of Visits to Infringing Content Referred by Search by Each Search Term Type, First Time vs Repeat Visits, 3 Year Average, 2010-2012)



Comete also analyzed if the actual search terms used by consumers differed when comparing first time vs. repeat visitation to infringing content URLs. Analysis showed that first-time visitors were more likely to use generic or title-only keyword terms than repeat visitors (63% vs. 54%). Conversely, repeat visitors were more likely to use domain-specific search terms such as "1channel" or "watch-free-movies.com" on repeat visits at a rate of 46% compared to 37% among first-time visitors. This suggests that repeat visitors to infringing content often utilize "navigational" queries on search engines to arrive at domains where they have viewed infringing content in the past.

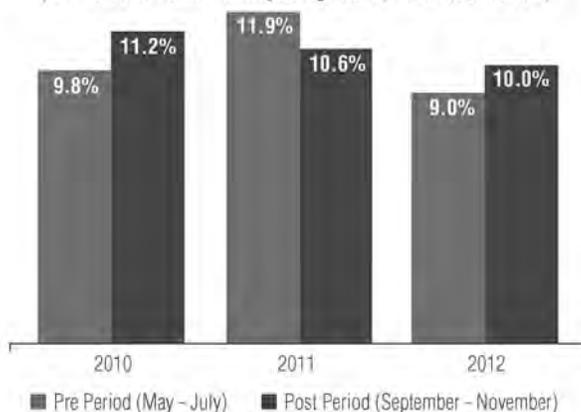
Google Transparency Report: Has it changed anything?

The study also analyzed the extent to which the "signal demotion" algorithm change implemented by Google in late 2012 impacted the role of search in consumer discovery and navigation to infringing content domains online. The stated goal of the algorithm change was to demote or remove search listings that were reported as hosting or linking to infringing content based on submissions sent to Google from content owners.

Other industry research has similarly analyzed the impact this algorithm change had on the infringing content ecosystem, but mostly from a "supply" perspective. These prior studies measured the presence and listing rank of various infringing sites on Google search result pages over time to identify any impact based on the volume of notices sent to Google for these same domains. Comete analyzed its clickstream panel to measure the consumer demand side of the Google change. This analysis sought to identify whether the number of consumers reaching infringing content sites from Google changed after the algorithm was released.

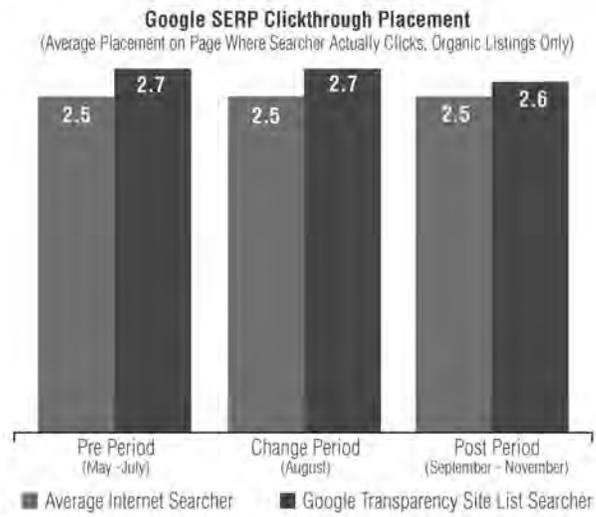
Google Transparency Report Site Visitation - Google Search Referred

(% of Visits to GTR Sites Referred by a Google Search, Pre vs. Post, 2010-2012)



For the two years prior to the study, Google directly referred between 8% and 12% of traffic to the sites analyzed in the Google Transparency Report ("GTR sites"). When comparing the three months before and after the algorithm was implemented in 2012, the share of direct referrals from Google to these sites increased slightly from 9% to almost 10%. Also, in comparison to the same periods from prior years (to isolate seasonality), the data indicate there was not a statistically significant change in direct referrals from Google to the GTR sites during the three months following the implementation of the algorithm.

In addition to analyzing referral volume, the study also measured the impact of the algorithm on consumer behavior. Specifically, the analysis gauged the extent to which consumers were required to find formerly higher-ranking results lower on search engines results pages or on subsequent pages due to the algorithm. This research indicates that among consumers who navigated from a Google search result page directly to a site listed on the GTR, the average listing placement decreased slightly from 2.7 to 2.6 when comparing the three months prior to and following the implementation of the algorithm (in this instance, a lower number translates into a higher ranking on search engine results pages, not a lower ranking). Therefore, the data do not indicate a significant change in listing placement; the search results consumers accessed were not lower in ranking than prior to the algorithm change.



Methodology

This study was based on the analysis of a database of 12 million film and TV content URLs that were known to host infringing content over the period 2010-2012. The URLs referred to the piece of content, not the site domain. The database was provided by two internet scanning vendors (DTecNet and IP Echelon) which on a regular basis scan websites for a list of MPAA member company titles, in order to find active infringing links and determine to which host sites the links direct. Note that these URLs are website-based and therefore the analysis based on these URLs does not include P2P sites or applications.

Using its robust clickstream panels in the U.S. and U.K. (2M and 200,000 members, respectively), Compete analyzed how many US and UK internet users reached the infringing URLs, how often and how long they visited for and most importantly, how they got there. In this study, Compete focused on the **role that search plays** in the consumer path to infringing content. Compete also identified other ways that consumers arrive to infringing content including by either directly going to an infringing domain or URL or by reaching that content via a "Linking" site like tv-links.eu. Compete's data was used to identify aggregate trends across different consumer segments and was not used to report individual infringing panelists.

Defining the Role of Search

Compete is able to measure how consumers use search engines in their online navigation process and is able to isolate the specific engine, term, what was displayed on a user's screen and what link they clicked. Consumers use search in two ways within the online piracy ecosystem: consumers can use search as a way to **discover websites** that link to or directly host the content they are looking for, or it can be used as a **navigational tool** to arrive at a known linking or hosting website instead of typing the URL into the browser.

Compete developed a customized, hybrid approach for this study to measure the impact that search plays in the path to infringing content as accurately as possible. This holistic approach contrasts with a more narrow definition that counts search only when a visit is preceded by a visit to a search engine. Compete defined a "search referral" to infringing content by:

- **Keyword Centric Component: A user must have conducted a relevant search query.** "Qualifying" search queries include all types of phrases that Compete has observed which online consumers use to find illegal TV and film content online. They include domain terms like "1Channel" and "sidereel", generic terms like "watch movies online" and movie and TV title-based terms like "Dark Knight Rises".
- **Time Centric Component:** In the same session (defined as a continuous period of internet activity without a 30 minute lapse) that a user visited an infringing content URL, users must have conducted a "qualifying" search on any major search engine within a 20 minute window before reaching that same infringing content URL.
 - » In order to capture the most relevant search queries yet also minimize the amount of noise in the data, Compete capped the time window at 20 minutes. Compete's analysis showed 20 minutes represents the most appropriate cutoff time as terms were still relevant to the content reached. After the 20 minute mark, Compete identified a sharp drop in level of relevancy the keywords had with watching or downloading content onlinewatching or downloading content online.

Defining First Time vs. Repeat Infringing Viewers

One the key components of the analysis completed by Compete was to understand if search plays a different role among consumers who are reaching infringing content on a site for the first time compared to those who have visited the site before. In order to accomplish this task, Compete segmented panelists who were in its panel for five consecutive months between August 2012 and December 2012 in order to perform a longitudinal analysis with a sufficient sample. The first visit to an infringing content domain within the time period was denoted as a "first-time" visit and all subsequent visits to that domain in that window were denoted as being "repeat" visits. Once the segmentation was defined, Compete was able to analyze the role that search played among the same group of consumers who visited infringing content at various times.

Survey Methodology

In tandem with its clickstream analysis, Compete conducted a quantitative survey to uncover additional learnings regarding how consumers use search in the steps leading up to watching or downloading infringing content. Additionally, Compete leveraged the survey to better understand the role that search plays for first-time infringing content consumers versus repeat visitors. Via email and an online survey, Compete interviewed 565 US and 500 UK panelists aged 18-54 who visited specific infringing URLs as well as known infringing domains in 2012. The survey was conducted between December 15th 2012 and January 7th 2013. Survey data was weighted on age and gender to represent the observed online infringing viewing population in each country.

Google Transparency Report Methodology

In order to understand if Google's "signal demotion" algorithm change had any impact on how consumers were reaching infringing sites, Compete retrieved the top 2,000 websites from the Google Transparency Report (GTR) website ranked by number of removal requests. We then isolated the share of traffic to these sites that were directly referred via a Google search result page before the change went into effect in August 2012 compared to afterwards in order to ascertain if the change had any effect. The pre-period of analysis consisted of the three months leading up to the change; May, June and July. The post-period was the three months following the change; September, October and November.

About Compete

Compete, Inc. is a Millward Brown Digital company based in Boston, MA. The company is a research and consulting firm that maintains an online behavioral database comprised of 2 million US internet users and 200,000 UK internet users. Compete uses its data to help brands, publishers and agencies understand how people use the web to communicate, shop, research, and consume content and media.

About MPAA

The Motion Picture Association of America, Inc. (MPAA), together with the Motion Picture Association (MPA) and MPAA's other subsidiaries and affiliates, serves as the voice and advocate of the American motion picture, home video and television industries in the United States and around the world. MPAA's members are the six major U.S. motion picture studios: Walt Disney Studios Motion Pictures; Paramount Pictures Corporation; Sony Pictures Entertainment Inc.; Twentieth Century Fox Film Corporation; Universal City Studios LLC; and Warner Bros. Entertainment Inc. MPAA is a proud champion of intellectual property rights, free and fair trade, innovative consumer choices, freedom of expression and the enduring power of movies to enrich and enhance people's lives.

Ms. CHU. Thank you.

This morning Mr. Coble and I did indeed participate in a press conference with the Motion Picture Association for the release of this study that found that search is a major gateway to the initial discovery of infringing content online. In fact, 74 percent of consumers surveyed cited using a search engine as the navigational tool that they use to find infringing content for the first time.

And so I would like to ask Mr. Sherman or Ms. Lesser, we know that the largest search engine, Google, made an effort last year to change the algorithm to take into account the number of copyright takedown notices the site has received, which is a positive step, but we have a long way to go. Unfortunately, there isn't anyone here today to represent them. But could you give your thoughts on what more search engines can do to reduce online infringement? What proactive steps do you think they could take?

Mr. SHERMAN. There are lots of practical steps that they could be taking when you think about the various ways in which search is leading people to infringing content. They did promise to demote sites that received a lot of takedown notices. We were very taken with that approach. We commended it. But 6 months, a year later, we have seen basically no difference whatsoever. The most rogue of rogue sites are still showing up on the first page of search results. We have sent about a million and a quarter notices on one site called MP3 Skull, yet it still shows up regularly on the first page of search results. Clearly, even though their intention was good, it hasn't been implemented well.

We also think they could be promoting more effectively, promoting the legitimate sites. I mentioned before the possibility of a certification mark or a badge. If we can provide a white list of sites that are licensed and actually pay creators, and they could put an indication like that in the search result, it could make a huge difference in the way that consumers use the search engine.

They could provide warnings about rogue sites. Just like they do when they encounter malware on a site in their own browser, they give a warning notice. Maybe they could do it with respect to rogue sites that are identified by third parties as sites they should be suspicious about.

They could also do things about autocomplete. Right now, if you enter in the name of an artist and a track, it will suggest to you MP3. And if you click on MP3, it will give you basically 6 to 8 illegal sites in the first 10 results.

And also the fact that we are sending millions of notices, and they are just going right back up again without any limitation. We send 100 notices about URLs with the same song on the same site, but you would think, therefore, that the other 1,000 songs on the same site would be taken down. But, no, we have to send each one individually.

We ought to be able to sit down and work out more efficient means for us and for them and for the piracy problem generally. There is a lot of motion, but what we need is impact.

Ms. LESSER. The only thing that I would add, since my program applies primarily—exclusively really at this point—to peer-to-peer is that I think when the negotiators who came up with this Memorandum of Understanding first sat down, there was very little opti-

mism about the ability to get not only to a sense of agreement, but also to actually create an existing real program that is changing consumer behavior. So I would say to Google and other search engines, it is important to come to the table and not see this as an “us versus them.” This is a problem that we all need to solve. And the 5-year dialogue and agreement among these parties is just evidence that can be done.

Ms. CHU. Let me follow up and talk about the copyright alert system, which is a successful voluntary system where ISPs alert Internet subscribers when they have downloaded pirated content and point them to legitimate sites. It is successful because, for one thing, the largest ISPs committed a significant amount of their own resources to this effort and invested significant resources to its design. And, secondly, the voluntary initiative took into account the views of all the key stakeholders.

While it is a great step forward, it does have limited impact unless other players like search engines get involved. How could they be integrated into this system? Mr. Sherman, you have ideas on that?

Mr. SHERMAN. Well, the copyright alert system is really based on peer-to-peer piracy, which is not something where search has a big role to play. So the ISPs are the appropriate party for that kind of operation. But because we have been more successful with peer-to-peer, because peer-to-peer has actually declined, other forms of piracy are increasing, Web site piracy, and certainly search engines would have a huge role to play there, one of the reasons we would like to be able to sit down with a multistakeholder process and see if we can come up with some improved mechanisms.

Ms. CHU. Thank you. I yield back.

Mr. COBLE. Gentlelady has expired—time is expired.

The distinguished gentleman from Georgia Mr. Collins is recognized for 5 minutes.

Mr. COLLINS. Thank you, Mr. Chairman. I appreciate the opportunity to be back here. And seeing this panel, it reminds me of one of my favorite movies of all time, “Groundhog Day,” because we see you here again as we go through this.

Mr. Chairman, I would ask unanimous consent to enter Google’s report on how they fight online piracy into the record.

Mr. COBLE. Without objection.

[The information referred to follows:]

HOW GOOGLE FIGHTS PIRACY



September 2013

Google

Contents

| | |
|--|----|
| Introduction | 2 |
| Better Legitimate Alternatives to Piracy | 4 |
| YouTube | 9 |
| Google Web Search | 13 |
| Advertising | 22 |

Introduction

In December 2012, a 34-year-old Korean artist made online video history when his viral video “Gangnam Style” smashed records and became the first YouTube video to reach a billion views. PSY was already popular in Korea, but he quickly launched an international career as his music spread from Seoul to North America, South America, and Europe.

In the past, music distribution had been mostly regional, making it difficult to hear great artists from around the world. But with a global platform like YouTube, which is owned and operated by Google, anyone is able to discover and share music from anywhere. This means new revenue opportunities for artists—according to outside estimates “Gangnam Style” generated over \$8 million in advertising deals in the first six months alone and has been purchased digitally millions of times.¹

The Internet has been a boon to creativity. Today, more music, more video, more text, and more software is being created by more people in more places than ever before.² Every kind of creative endeavor, both amateur and professional, is being transformed by the new opportunities and lower costs made possible by digital tools and online distribution.

Nevertheless, online piracy remains a challenge, and Google takes that challenge seriously. We develop and deploy anti-piracy solutions with the support of hundreds of Google employees. This report gathers and details those efforts, as well as how Google products and services create opportunity for creators.

GOOGLE'S ANTI-PIRACY PRINCIPLES

- ✓ **Create More and Better Legitimate Alternatives.** The best way to battle piracy is with better, more convenient, legitimate alternatives to piracy. By developing licensed products with beautiful user experiences, we help drive revenue for creative industries.
- ✓ **Follow the Money.** Rogue sites that specialize in online piracy are commercial ventures, which means the most effective way to combat them is to cut off their money supply. Google is a leader in rooting out and ejecting rogue sites from our advertising and payment services, and is raising standards across the industry.
- ✓ **Be Efficient, Effective, and Scalable.** Google strives to implement anti-piracy solutions that work. For example, beginning in 2010, Google has made substantial investments in streamlining the copyright removal process for search results. As a result these improved procedures allow us to process copyright removal requests for search results at the rate of four million requests per week with an average turnaround time of less than six hours.

Sources

1. NYMag, “Gangnam-Buster Profits,” December 2012 <<http://goonj/P412/>>
2. Techdirt, “The \$kyie Rising,” January 2012 <<http://goonj/P412/>>

- ✓ **Guard Against Abuse.** Unfortunately, fabricated copyright infringement allegations can be used as a pretext for censorship and to hinder competition. Google is committed to ensuring that, even as we battle piracy online, we detect and reject bogus infringement allegations, such as removals for political or competitive reasons.
- ✓ **Provide Transparency.** We disclose the number of requests we receive from copyright owners and governments to remove information from our services.³ We hope these steps toward greater transparency will inform ongoing discussions about content regulation online.

These principles guide the actions of Google employees, as well as our investment of tens of millions of dollars in new tools and systems to improve and expand our anti-piracy efforts. Some of the highlights, discussed in more detail in this report, include:

YOUTUBE PARTNER SUCCESS

More than one million partner channels are making money from their YouTube videos. More than four thousand rights holder partners use YouTube's content identification tool, Content ID, to manage their copyrights appearing within user-generated content on the site. These partners include network broadcasters, movie studios, songwriters, and record labels, and they are collectively making hundreds of millions of dollars by using YouTube's Content ID tools to monetize these videos.

GOOGLE PLAY

Google Play is a digital storefront where people can buy millions of songs and books, thousands of movies and TV shows, and much more content. All Access, a new monthly subscription service, also gives people another way to access music. For a monthly fee they can listen to millions of songs across their devices.

GOOGLE SEARCH

We process more takedown notices, and faster, than any other search engine. We receive notices for far less than 1% of everything we index, which amounts to four million copyright removal requests per week that are processed, on average, in less than six hours.

ADS

Our policies restrict infringing sites from using our advertising services. In 2012, Google disabled ad serving to 46,000 sites for violating our policies that prohibit the placement of ads on sites with infringing content, the vast majority being violations Google detected before we were notified.

Sources:

3. Google. "Transparency Report: Removal Requests." January 2013 <<http://goo.gl/pQOT>>



Piracy often arises when consumer demand goes unmet by legitimate supply. As services ranging from Netflix to Spotify to iTunes have demonstrated, the best way to combat piracy is with better and more convenient legitimate services. The right combination of price, convenience, and inventory will do far more to reduce piracy than enforcement can.

The music industry has demonstrated the effectiveness of this approach by licensing a variety of music services including free, advertising-supported streaming services (like Spotify and Pandora), download stores (like iTunes), and on-demand subscription products (like All Access). A survey recently released by the Swedish music industry shows that since 2009 the number of people who download music illegally in Sweden has decreased by more than 25 percent, largely as a result of greater availability of improved legal services such as Spotify.⁴ Similar trends were seen in a 2013 survey from NPD Group.⁵ And a recent study conducted by Spotify found that overall piracy rates in the Netherlands has declined dramatically thanks to the popularity of legitimate digital music services.⁶

Film and television have had success combating piracy with legitimate alternatives, as well. In a recent interview with Stuff magazine, Netflix's Chief Content Officer Ted Sarandos said that when Netflix launches in a new country, piracy rates in that country drop. In his opinion, the best way to reduce piracy is by "giving good options."⁷

Signs have been positive that the creative industries are growing around the world, thanks in large part to digitization. IFPI reported that the recording industry grew its revenue in 2012 for the first time in over a decade, to \$16.5 billion.⁸

Sources:

4. Mediavision, "Music Sweden File Sharing & Downloading," 2011 <<http://www.mediavision.se>>
5. NPD Group, "Music Filesharing declined significantly in 2012," February 2012 <<http://www.npd.com>>
6. Spotify, "New Spotify study sees encouraging downwards trend in music piracy in the Netherlands," July 2013 <<http://www.spotify.com>>
7. Stuff, "Netflix's Ted Sarandos talks Arrested Development, iK and reviving old shows," May 2013 <<http://www.stuff.co.nz>>
8. IFPI, "IFPI's Recording Industry in Numbers 2013," April 2013 <<http://www.ifpi.com>>

Nielson and Billboard reported that, in the same year, music purchases grew by 3.1% from the previous record high set in 2011, which was driven largely by digital purchases.⁹ A 2013 study by Booz & Co. in Europe also found that digital media was driving growth in the European creative sector.¹⁰

Google has been at the forefront of creating new, authorized ways for consumers to obtain digital content. We build platforms where our users can legitimately purchase, consume, and discover entertainment and culture. We also pioneer innovative new approaches to monetizing online media.

YouTube Partners

YouTube's community includes not only a billion individual users, but also more than a million partner channels from over thirty countries that earn money from their YouTube videos—from independent musicians and creators to some of the world's biggest record labels, movie studios, and news organizations. YouTube has developed a series of tools and programs to help content partners thrive, including partnerships with every major record label, as well as hundreds of collecting societies, independent labels, and music publishers to license recorded music on the site. As a result of partnerships like these, YouTube generates hundreds of millions of dollars each year for the content industry.

From musicians to athletes, teachers to comedians, tens of thousands of video creators are now part of the Partner Program established by YouTube in 2007, many thousands of them earning six-figure incomes from their YouTube channels. To further support this creative community, we have opened facilities like the new collaborative spaces in LA, London, and Tokyo as places for partners to shoot, edit and create their content. These facilities support the creative industry developing and monetizing their work through partner channels on YouTube.



Photos of the YouTube Space in Los Angeles. For more information, visit youtubespace.la.com.

Sources

⁹ Businesswire, "The Nielsen Company & Billboard's 2012 Music Industry Report," January 2013 <<http://goo.gl/2C18J>>

¹⁰ Booz & Co., "The Digital Future of Creative Europe: The Economic Impact of Digitization and the Internet on the Creative Sector in Europe," March 2013 <<http://goo.gl/255m0t>>

To give YouTube creators more flexibility in monetizing and distributing content, in May 2013 we launched a pilot program for certain partners that will offer paid channels on YouTube with subscription fees starting at \$0.99 per month. Our partners are experimenting with different pricing models to attract viewers, including offering 14-day free trials, and many offer discounted yearly rates.

Rentals are another option for content partners. Thanks to our partnerships with content creators, YouTube offers tens of thousands of movies and TV episodes to rent at standard industry pricing.

CELEBRATING THE NEXT GENERATION OF CREATIVE VIDEO

One of the most inspiring things about YouTube is the way people around the world use it to express their passion and creativity—and to turn it into a career. Thousands of channels are now generating six-figure revenue through the YouTube Partner Program, and there are more than one million channels earning revenue.

To shine a light on the many inspiring things happening on YouTube, we recently published a report sharing the stories of 20 YouTube Partners in the United States who are changing lives, businesses, and in some cases, history.



Read the full report at goo.gl/bMRy.

Thanks to the popularity of music videos and YouTube's agreements with record labels and music publishers to feature them, YouTube has become an important destination for music. So much so that, as of February 2013, Billboard magazine's Hot 100 chart now incorporates YouTube views when ranking a song's popularity. The 2013 Digital Music Report from IFPI,¹¹ an international association representing the recording industry, concluded that 90% of Internet users are aware of YouTube, and that the service attracts a large global audience.

Each time a music fan chooses YouTube over an unauthorized source for music, it's a victory against piracy—unlike previous generations of music fans who were raised on unauthorized sources for music, today's young fans have YouTube as a legal, compelling way to experience music online. And because of our licensing agreements with our partners in the music industry, rightsholders are compensated when fans visit YouTube to experience music videos.

Google Play

More than 900 million Android devices have been activated around the world, presenting a tremendous opportunity to creative industries. Google Play is a global service that helps rightsholders and creators sell their applications or content directly to Google users. It's a digital store where people can find, purchase, and enjoy entertainment for their devices—from computers to tablets to smartphones. We've partnered with all of the major record labels, publishers, and movie studios to offer millions of songs and books, thousands of movies and TV shows, and hundreds of magazines that can be enjoyed across devices. In the last year, Google Play digital content, including music and movies, has launched in 21 new countries, including India, Mexico and Russia.

MUSIC

Google Play also offers a store where users can purchase new music, a music locker to store existing collections of songs, and a subscription service to access millions of songs from the Google Play collection. Today there are more than 18 million songs available for purchase from Google Play. Google also has "scan-and-match" licenses that enable users to access their personal music collections from any connected device, without the time-consuming process of uploading those files. Our new music subscription service, All Access, lets users listen to millions of songs on-demand for a monthly fee.

These products are driving revenue for the music industry. And thanks to our partnerships with rightsholders around the world, Google Play Music is available to a global audience.

¹¹ IFPI, "IFPI Digital Music Report 2013," 2013. <<http://goo.gl/11624p>>

MOVIES AND TV SHOWS

Google Play has partnered with all of the major film studios in the U.S. and many local studios in countries overseas to offer thousands of movies and TV shows that can be rented or purchased. We also offer innovative features that take advantage of a digital format to drive user engagement, such as Info Cards that appear when a movie or TV show is paused and that give more information about the actors and music in a scene.

BOOKS AND MAGAZINES

Google Play is home to the world's largest selection of eBooks – with more than 5 million titles available. More than 48,000 publishers have joined the Partner Program to promote their books online, including nearly every major U.S. publisher. We have also partnered with major publishers to offer hundreds of magazines for purchase or subscription in the Google Play store, creating a new market for magazines and newspapers. Users are able to access their books and magazines on any of their devices.

APPS AND GAMES

Google Play is an engine of economic opportunity for application and game developers because it gives them a free platform to build on and reach millions of users. More than a million apps and games are available for sale or for free on Google Play, and they've been downloaded over 50 billion times.

Several of the most popular apps are delivering licensed music, movies, and TV shows to users.

- ✓ **Netflix** allows subscribers to stream popular TV and movies to Android devices. Its Android application launched in 2011.
- ✓ **Pandora** creates personalized music stations and streams songs directly to users.
- ✓ **Spotify** is an interactive music service allowing users access to a catalog of licensed music.

Google recently launched Google Play Games, an app that makes it easy to discover new games, track achievements and scores, and play games with friends around the world. Google Play is an opportunity for game developers to showcase their creativity and sell their apps directly to gamers.



More than one billion unique users visit YouTube each month and together watch more than six billion hours of video. And more than 100 hours of video are uploaded to YouTube every minute, spanning every conceivable topic from politics to comedy, from daredevil sports to religion. YouTube has been a transformational force in the world of creative expression, a global video platform at a scale never imagined.

Content ID: A Win-Win Solution

Beginning in 2007, YouTube developed and launched the most advanced content identification system in the world, called Content ID. With this system, rightsholders are able to identify user-uploaded videos that are entirely or partially their content, and choose, in advance, what they want to happen when those videos are found.

This is how it works: Rightsholders deliver YouTube reference files (audio-only or video) of content they own, metadata describing that content, and policies describing what they want YouTube to do when it finds a match. YouTube compares videos uploaded to the site against those reference files. Our technology automatically identifies the content and applies the rightsholder's preferred policy.

Rightsholders can choose among three policies when an upload matches their content:



Thanks to the options that Content ID affords to copyright owners, it's not just an anti-piracy solution, but also a new business model for copyright owners and YouTube alike. The majority of partners using Content ID choose to monetize their claims and many have seen significant increases in their revenue as a result.

Content ID is good for users as well. When copyright owners choose to monetize or track user-submitted videos, it allows users to continue to freely remix and upload a wide variety of new creations using existing works.



The majority of partners using Content ID choose to monetize their claims, and many have seen significant increases in their revenue as a result.



CONTENT ID STATS

Content ID is the premier automated video content identification system in the world. The following statistics provide a sense of the impressive scale and technical sophistication of the system:

More than

4,000 partners

use Content ID, including major U.S. network broadcasters, movie studios and record labels.

Content ID scans over

250 years

of video every day.

More than

200 million videos

have been claimed with the help of Content ID.

We have more than

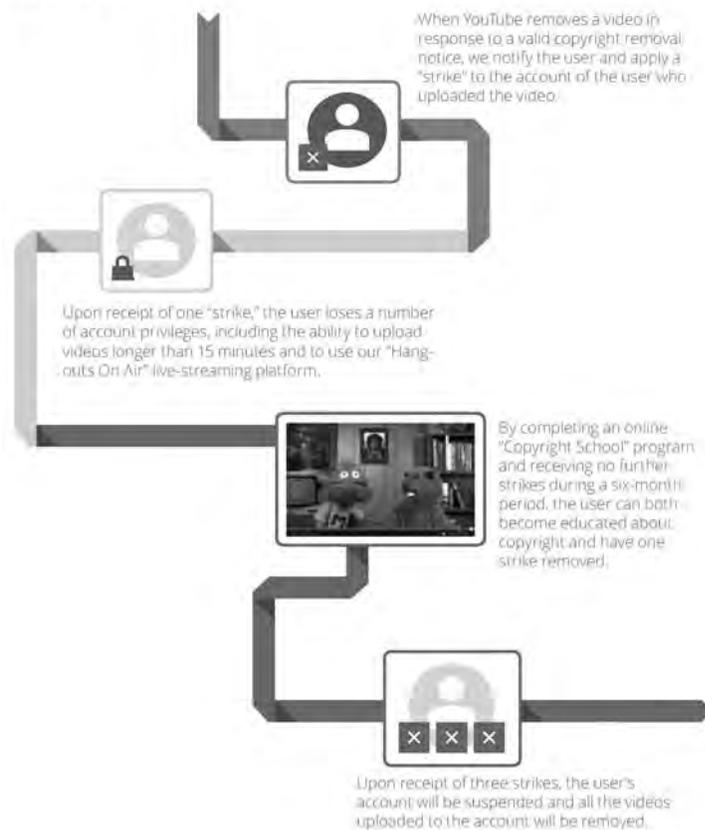
15 million active reference files

In the Content ID database, that's over 1.5 million hours of material.

YouTube Copyright Policies

The vast majority of the 100 hours of video uploaded to YouTube every minute will not infringe anyone's copyright. Nevertheless, YouTube takes seriously its role in educating YouTube users about copyright and creating strong incentives to discourage infringing activity. As a result, YouTube has a number of policies in place designed to discourage copyright infringement and terminate repeat offenders.

For example:



The YouTube Copyright Center

In addition to the Content ID system, copyright owners and their representatives can submit copyright removal notices through the YouTube Copyright Center, which offers an easy-to-use web form, as well as extensive information aimed at educating YouTube users about copyright. The Copyright Center also offers YouTube users a web form for “counter-noticing” copyright infringement notices that they believe are misguided or abusive.



Glove and Boots explains copyright in the YouTube Copyright Center: [youtube.com/ytc/copyright](https://www.youtube.com/ytc/copyright).

YouTube Content Verification Program

YouTube offers a Content Verification Program for rightsholders who have a regular need to submit high volumes of copyright removal notices and have demonstrated high accuracy in their prior submissions. This program makes it easier for rightsholders to search YouTube for material that they believe to be infringing, quickly identify infringing videos, and provide YouTube with information sufficient to permit us to locate and remove that material, all in a streamlined manner intended to make the process more efficient.



There are more than 60 trillion addresses on the web. Only an infinitesimal portion of those trillions infringe copyright, and those infringing pages cannot be identified by Google without the cooperation of rightsholders. Nearly every paragraph of text, photograph, video, sound recording, or piece of software is potentially protected by copyright law. Moreover, copyright laws generally permit some uses, such as parodies and quotation, even over a copyright owner's objection. So while we don't want to include links to infringing pages in our search results, Google needs the cooperation of copyright owners to separate the authorized or unobjectionable uses from infringing ones.

Google relies on copyright owners to notify us when they discover that a search result infringes their rights and should be removed. These notices are submitted through procedures that are consistent with the Digital Millennium Copyright Act (DMCA) and similar laws that apply to providers of online services.¹²

To help copyright owners submit these notices, Google has developed a streamlined submission process. There is no search engine that processes as many copyright removal notices as Google does, and none that process them more quickly.

For example:

- ✓ Copyright owners and their agents submitted more than 57 million web pages for removal in 2012

Notes:

¹² The DMCA is a U.S. law that provides qualifying online service providers like Google with a safe harbor from monetary liability for copyright infringement claims. One of the requirements of these safe harbor provisions is that the service provider (Google, in this case) remove or disable access to allegedly infringing material upon receiving a request that meets certain requirements. Laws governing other jurisdictions, such as Europe's E-Commerce Directive, have similar requirements for service providers.

- ✓ Between December 2011 and November 2012, we removed from search 97.5% of all URLs specified in copyright removal requests. For the remaining sites, we either needed additional information, were unable to find the page, or concluded that the material was not infringing
- ✓ Our average turnaround time for copyright notices is less than 6 hours.

In addition, Google incorporates the number of valid copyright removal notices we receive for any given site as a signal in our ranking algorithm, as described below.

Submitting Removal Notices

The fastest and most efficient way to submit a copyright removal notice to Google is through our content removal web form, which accepts many different kinds of removal requests, including copyright requests. Our web form is consistent with the DMCA and similar laws, and provides a simple and efficient mechanism for copyright owners from countries around the world. During 2012, approximately 16,000 different entities used our web form to submit copyright removal notices from search results.

In addition to the public content removal web form, for copyright owners who have a proven track record of submitting accurate notices and who have a consistent need to submit thousands of URLs each day, Google created the Trusted Copyright Removal Program for Web Search (TCRP). This program streamlines the submission process, allowing copyright owners or their enforcement agents to submit large volumes of URLs on a consistent basis. At the end of 2012, there were approximately 50 TCRP partners, who together submitted 95% of the URLs submitted during the year.

~~~~~

**At the end of 2012, there were approximately 50 Trusted Copyright Removal Program partners, who together submitted 95% of the URLs submitted during the year.**

~~~~~

REMOVAL REQUESTS FOR SEARCH SKYROCKET

Since launching new submission tools for copyright owners and their agents in 2011, we have seen remarkable growth in the number of pages that copyright owners have asked us to remove from search results. In fact, today we receive removal requests for more URLs every week than we did in the twelve years from 1998 to 2010 combined. At the same time, Google is processing the notices we receive for Search faster than ever before—currently, on average, in less than six hours.

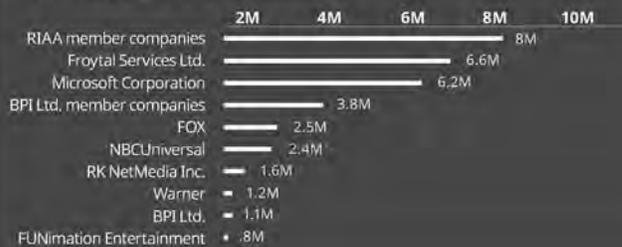
Google has a strong track record of developing solutions that scale efficiently. The trend line is striking—from more than three million pages for all of 2011 to more than 4 million pages per week today. As the numbers continue to swell, it becomes both more difficult and more important to detect and pick out the abusive and erroneous removal notices.

Google has never charged copyright owners for providing these services, and we will continue to invest substantial resources and engineering effort into improving our procedures for receiving and processing copyright removal notices.

Top 10 Reporting Organizations in 2012



Top 10 Copyright Owners in 2012



Transparency

When we remove material from search results, we believe users and the public should be able to see who made the removal request and why. Because copyright infringement allegations are the basis for more than 95% of the legal requests that we receive to remove items from search results, we have taken the following steps to ensure transparency:

- ✓ **Maintaining an ongoing Transparency Report.** In 2012, we added details regarding copyright removal notices to our Transparency Report site.¹⁴ Updated daily, the site shows the aggregate number of URLs that we have been asked to remove, as well as who submitted the notices, on behalf of which copyright owners, and for which websites.
- ✓ **Notifying webmasters of removals.** If a website operator uses Google's Webmaster Tools, notification will be provided to webmasters there when a web page in their domain has received a takedown notice.¹⁴
- ✓ **Informing users when results have been removed from their results.** When users perform a search where results have been removed due to a copyright complaint, Google displays the following notice:

In response to a complaint we received under the US Digital Millennium Copyright Act, we have removed 1 result(s) from this page. If you wish, you may [read the DMCA complaint that caused the removal\(s\)](#) at [ChillingEffects.org](#).

- ✓ **Providing copies of notices to Chilling Effects.** Since 2002, Google has provided a copy of each copyright removal notice that we receive for search results to the nonprofit organization Chilling Effects. By gathering together copyright removal notices from a number of sources, including Google and Twitter, Chilling Effects fosters research and examination of removal notices submitted by copyright owners.¹⁵

Detecting and Preventing Abuse

Google works hard to detect and prevent abuses of the copyright removal process. From time to time, we may receive inaccurate or unjustified copyright removal requests for search results that clearly do not link to infringing content.

¹⁴Google.

¹⁴ Google, "Transparency Report: Removal Requests," January 2013, <https://www.google.com/transparencyreport/removals/>.

¹⁵ Google, "What's New: 2012-2013," <http://www.google.com/transparencyreport/removals/>.

¹⁵ Chilling Effects, "A 10th Anniversary Issue: Chilling Effects," December 2010, <http://www.chillingeffects.org/10th/>.

EXAMPLES OF DMCA ABUSE

Here are a few examples of requests that have been submitted through our copyright removals process that were clearly invalid copyright removal requests. In each case, we did not remove the URL in question from search results.

- A major U.S. motion picture studio requested removal of the Internet Movie Database (IMDb) page for a movie released by its own studio, as well as the official trailer posted on a major authorized online media service.
- A U.S. reporting organization working on behalf of a major movie studio twice requested removal of a movie review on a major newspaper website.
- A driving school in the U.K. requested the removal of a competitor's homepage from Google Search, on the grounds that the competitor had copied an alphabetized list of cities and regions where instruction was offered.
- A content protection organization, acting on behalf of motion picture, record, and sports programming companies, requested the removal of search results. They linked only to copyright removal requests on Chilling Effects that had originally been submitted by one of its clients.
- An individual in the U.S. requested the removal of search results that link to court proceedings referencing her first and last name on the ground that her name was copyrightable.
- Multiple individuals in the U.S. requested the removal of search results linking to blog posts and web forums that associated their names with certain allegations, locations, dates, or negative comments.
- A company in the U.S. requested the removal of search results that link to an employee's blog posts about unjust and unfair treatment.

In 2012, we terminated two partners from the Trusted Copyright Removal Program for Web Search for repeatedly sending inaccurate notices through our high-volume submission mechanisms. Because the TCRP is reserved for partners with a track record of submitting accurate notices, access to the program can be revoked where a partner falls short of these high standards.

As the volume of removal notices continues to rise, detecting inaccurate or abusive notices continues to pose a challenge. Google invests continuously in engineering and machine learning solutions to address this risk. The Transparency Report has also proven useful in detecting abusive notices, as journalists, webmasters, and other interested members of the public have examined the data made available there.

Webmasters may also submit a counter-notice if they determine that a page on their site has been removed from Google Search results due to an erroneous copyright removal notice. Google affords webmasters two ways to be notified if any pages on their sites are targeted by removal notices. If the site operator uses Google's Webmaster Tools, notification will be provided to webmasters there. Alternatively, the search feature on the Transparency Report will show copyright removal notices received for a domain.

Using Copyright Removal Notices in Ranking

In addition to removing pages from search results when notified by copyright owners, Google also factors in the number of valid copyright removal notices we receive for any given site as one signal among the hundreds that we take into account when ranking search results. As a result, sites with high numbers of removal notices may appear lower in search results. We believe that this ranking change should help users find legitimate, quality sources of content more easily.

While we use the number of valid copyright removal notices as a signal for ranking purposes, we do not remove pages from results unless we receive a specific removal request for the page. As shown on the Transparency Report, we generally receive removal notices for a very small portion of the pages on a site. Even for the websites that have received the highest numbers of notices, the number of noticed pages is typically only a tiny fraction of the total number of pages on the site. It would be inappropriate to remove entire sites under these circumstances.



Sites with high numbers of removal notices may appear lower in search results.



SEARCH AND PIRACY: THE REALITY

In reflecting on the role search engines can play in addressing the problem of piracy, commentators often overlook some important realities:

1. Search is not a major driver of traffic to pirate sites.

Google Search is not how music, movie, and TV fans intent on pirating media find pirate sites. All traffic from major search engines (Yahoo, Bing, and Google combined) accounts for less than 16% of traffic to sites like The Pirate Bay.¹⁶ In fact, several notorious sites have said publicly that they don't need search engines, as their users find them through social networks, word of mouth, and other mechanisms.¹⁷ Research that Google co-sponsored with PRS for Music in the UK further confirmed that traffic from search engines is not what keeps these sites in business.¹⁸ These findings were confirmed in a recent research paper published by the Computer & Communications Industry Association.¹⁹

2. Search can't eradicate pirate sites.

Search engines do not control what content is on the Web. There are more than 60 trillion web addresses on the Internet, and there will always be new sites dedicated to making copyrighted works available, as long as there is money to be made doing so. According to recent research, replicating these sites is easy and inexpensive, and attempts to make them disappear should focus on eradicating the business model that supports them.²⁰

3. Volume of allegedly 'piracy-related' queries is dwarfed by broader queries.

When it comes to building anti-piracy measures, we prioritize efforts where they can make the most difference. Google Search receives more than three billion queries each day. We want to focus our efforts where the users are.

The good news is that the most popular queries relating to movies, music, books, video games, and other copyrighted works return results that do not include links to infringing materials. This is thanks to both our constant improvements to the algorithms that power Google Search, and the efforts of rightsholders to prioritize and target their copyright removal notices.

So when some critics focus on infringing materials appearing in search results for particular queries, it is important to consider how many users actually make those queries. During the first six months of 2013, Google users searched for “:

“carly rae jepsen call me maybe”
16 TIMES MORE OFTEN THAN
“carly rae jepsen call me maybe mp3”

“flo rida whistle”
30 TIMES MORE OFTEN THAN
“flo rida whistle download”

“game of thrones”
200 TIMES MORE OFTEN THAN
“game of thrones download”

“django unchained”
1,000 TIMES MORE OFTEN THAN
“django unchained free download”

“30 rock”
5,000 TIMES MORE OFTEN THAN
“30 rock free stream”

“katy perry”
200,000 TIMES MORE OFTEN THAN
“free katy perry mp3”

Removing Terms Associated with Piracy from Autocomplete and Related Search

Autocomplete is a convenience feature in Google Search that attempts to "complete" a query as it's typed based on similar queries that other users have typed. Related Search shows queries that other users have typed that may be similar to yours. Google has taken steps to prevent terms closely associated with piracy from appearing in Autocomplete and Related Search. This is similar to the approach we have taken for a narrow class of terms related to pornography, violence, and hate speech.

The Next Step: Making Legitimate Alternatives More Visible

In addition to removing infringing pages from search results and using valid removal notices as a ranking signal, Google has an ongoing dialogue with content owners about ways to increase the visibility of authorized services in search results.

For example, in 2011, we launched a new open standard for the markup of websites which enables authorized music sites to more prominently feature streaming "preview" music content in our search results ("rich snippets").²² With this standard, anyone searching for popular music can immediately stream authorized previews right in the search results. A number of music sites (including Amazon and Last.FM) have implemented the new standard, distinguishing their offerings from results from unauthorized sites.

Lady Gaga | Free Music, Tour Dates, Photos, Videos

www.myspace.com/ladygaga - Cached

Lady Gaga's official profile including the latest music, albums, songs, music videos and more updates.

| | | |
|-------------------|--------|---------------|
| Judas | 🔊 4:10 | Judas |
| The Edge Of Glory | 🔊 5:21 | Born This Way |
| Born This Way | 🔊 4:20 | Born This Way |
| You And I | 🔊 5:07 | Born This Way |

Sources:

16. Techdirt, "Data Shows: Removing 'Rogue Sites' From Search Won't Make Much of A Difference," November 2011 <<http://go.gl/4E50g>>
17. TorrentFreak, "Pirate Bay and iso-hunt Respond to Google Search Result Punishment," August 2012 <<http://go.gl/4UJ00E>>
18. BAE Systems Detrica, "The Six Business Models for Copyright Infringement," June 2012 <<http://go.gl/yZd>>
19. CCA, "The Search Fixation, Infringement, Search Results, and Online Content," 2012 <<http://go.gl/4M5LE>>
20. Northeastern University, "Clickonomics: Determining the Effect of Anti-Piracy Measures for One-Click Hosting," 2012 <<http://go.gl/y3wCT>>
21. These queries were raised by RIAA and MovieLabs in discussions with Google.
22. Google, "Webmaster Tools: Rich snippets - Music," May 2013 <<http://go.gl/7M8Eg>>

There is more that authorized music, TV, and movie sites can do to help their sites be more effectively indexed by search engines. The film and television industry has launched wheretowatch.org, and the music industry has launched whymusicmatters.com to help consumers find legitimate channels for buying films, TV shows, and songs. And NARM has recently offered advice to online music retailers on optimizing their sites for better performance in search engine results.²³ But these industries could do even more to build pages specific to albums, movies, and TV shows that could then appear in search engine results (for example, a specific page on “Where to Watch Modern Family online”).

Indexing subscription music and video services is also a challenge for search engines. It is difficult for a search engine to return results from licensed services like Spotify or Netflix if it doesn't know what songs and programs are available from those services. With more information, search engines could return better, more relevant legitimate results to users seeking the content. Google looks forward to continuing collaborative efforts with content owners and authorized services, intended to make the offerings of authorized services more visible in search results.

Sources
23. NARM, “INFOGRAPHIC: Search Engine Optimization for Music Websites,” May 2013 (<http://www.narm.com>).



Following the Money

The most effective way to combat rogue sites that specialize in online piracy is to cut off their money supply. These sites are almost exclusively for-profit enterprises, and so long as there is money to be made by their operators, other anti-piracy strategies will be far less effective. As a global leader in online advertising, Google is committed to rooting out and ejecting rogue sites from our advertising services. We are also working with other leaders in the industry to craft best practices aimed at raising standards across the entire online advertising industry.

Best Practices

In April 2011, Google was among the first companies to certify compliance in the Interactive Advertising Bureau's (IAB's) Quality Assurance Certification program, through which participating advertising companies will take steps to enhance buyer control over the placement and context of advertising and build brand safety.²⁴ This program will help ensure that advertisers and their agents are able to control where their ads appear across the web.

In July 2013, Google worked with the White House's Office of the U.S. Intellectual Property Enforcement Coordinator (IPEC) and other leading ad networks to participate in Best Practices and Guidelines for Ad Networks to Address Piracy and Counterfeiting.²⁵ Under these best practices, ad networks will maintain and post policies prohibiting websites that are principally dedicated to engaging in copyright piracy from participating in the ad network's advertising programs. By working across the industry, these best practices should help reduce the financial incentives for pirate sites by cutting off their revenue supply while maintaining a healthy Internet and promoting innovation.

²⁴Sources:

24. IAB, "Quality Assurance Guidelines," November 2011 <<http://goo.gl/BiDcyp>>

25. The White House, "Coming Together to Combat Online Piracy and Counterfeiting," July 2013 <<http://www.whitehouse.gov/the-press-office/2013/07/11/13-07-11-coming-together-to-combat-online-piracy-and-counterfeiting>>

AdSense

More than two million web publishers use AdSense to make money from their content on the web, making it the chief Google advertising product used by online publishers. The overwhelming majority of those publishers are not engaged in any kind of copyright infringement. AdSense has always prohibited publishers from using AdSense to place ads on pages that contain pirated content, and Google proactively monitors the AdSense network to root out bad publishers.

- ✓ In 2012, Google disabled ad serving to 46,000 sites for violating our policies prohibiting the placement of ads on sites with infringing content, the vast majority being violations Google detected before we were notified.
- ✓ Almost all AdSense ad formats include a link that permits a copyright owner to report sites that are violating Google's policies. Copyright owners may also notify us of violations through a web form. In 2012 we took action on several thousand URLs in response to these complaints.

Violating URL: *

Format: <http://www.SiteURL.com> or <http://www.SiteURL.com/page.html>

Please select the type of media on which you saw the violation *

- website
- mobile website
- video
- feed

Description of location on URL: *

- ✓ Each time we receive a valid copyright removal notice for Search, we also blacklist that page from receiving any AdSense advertising in the future.

Google does not want to be in business with rogue sites specializing in piracy. Thanks to our ongoing efforts, we are succeeding in detecting and ejecting these sites from AdSense. While a rogue site might occasionally slip through the cracks, the data suggests that these sites are a vanishingly small part of the AdSense network. For example, we find that AdSense ads appear on far fewer than 1% of the pages that copyright owners identify in copyright removal notices for Search.

DoubleClick

DoubleClick offers a suite of online advertising platform solutions for both advertisers and web publishers. The principal customers for DoubleClick services are large advertisers, ad agencies, large publishers, and ad networks. It is virtually unheard of for these sorts of "blue chip" commercial entities to be operating rogue sites specializing in copyright infringement.

DoubleClick also offers a free service to smaller web publishers on a self-service basis through the DoubleClick for Publishers (DFP) Small Business program. Although the program has policies in place to prohibit its use in connection with infringing activity, rogue publishers have tried to sneak in through this door. Publishers do not pay Google to use this platform, nor does Google pay them for using it. Nevertheless, Google has recently revised its policies and stepped up enforcement efforts for DoubleClick for Publishers Small Business in an effort to deny rogue sites access to the service as a platform for serving ads sourced from other networks.

AdWords

AdWords is Google's premier advertising product, responsible for the advertisements that appear next to Google search results, as well the text advertisements on sites across the web. Advertisers pay Google for these placements, generally on a cost-per-impression or cost-per-click basis.

Rogue sites specializing in online piracy generally do not use AdWords. Google receives very few complaints regarding AdWords being used by rogue pirate sites. Nevertheless, we maintain strict policies forbidding the use of AdWords to promote copyright infringement. We take a variety of proactive and reactive steps, through both manual and automated review, to enforce our policies.

BLOGGER

Blogger is Google's free blog publishing platform, which enables users to create and update blogs. We remain vigilant against use of the Blogger platform by pirates looking to set up a free website. Consistent with other Google products that host user-uploaded content, we will remove infringing blog posts when properly notified by a copyright owner, and will terminate the entire blog where multiple complaints establish it as a repeat infringer.

Blogger has also created an automated bulk submission tool for copyright owners who have a track record of reliable submissions and a regular need to submit large volumes of takedown notices. This tool allows qualified copyright owners to obtain rapid removals of infringing posts appearing on Blogger.

GOOGLE'S ANTI-PIRACY PRINCIPLES

Create More and Better Legitimate Alternatives. The best way to battle piracy is with better, more convenient, legitimate alternatives to piracy. By developing licensed products with beautiful user experiences, we help drive revenue for creative industries.

Follow the Money. Rogue sites that specialize in online piracy are commercial ventures, which means the most effective way to combat them is to cut off their money supply. Google is a leader in rooting out and ejecting rogue sites from our advertising and payment services, and are raising standards across the industry.

Be Efficient, Effective, and Scalable. Google strives to implement anti-piracy solutions that work. For example, beginning in 2010, Google has made substantial investments in streamlining the copyright removal process for search results. As a result, these improved procedures allow us to process copyright removal requests for search results at the rate of four million requests per week, with an average turnaround time of less than six hours.

Guard Against Abuse. Unfortunately, fabricated copyright infringement allegations can be used as a pretext for censorship and to hinder competition. Google is committed to ensuring that, even as we battle piracy online, we detect and reject bogus infringement allegations, such as removals for political or competitive reasons.

Provide Transparency. We disclose the number of requests we receive from copyright owners and governments to remove information from our services. We hope these steps toward greater transparency will inform ongoing discussions about content regulation online.



Mr. COLLINS. And would have also entered the Motion Picture of America's filing as well, but my distinguished colleague, Ms. Chu, beat me to it.

Mr. COBLE. Without objection.

Mr. COLLINS. As we look on this.

To the witnesses, I would like to thank, you know, all for being here. I have listened a great deal. I have been listening even out of here in a meeting for—and holding this hearing. I believe we have got to continue to examine the volunteering issue before the industry, because I believe they are a step forward. In considering any legislative remedies, we need to see what is already being done, because the last thing I would like to see is just come again. What I think we do too many times in all forms of government, from local to Federal, is we rush in with the, quote, "legislative fix," and then all of a sudden that fixes it for all of 6 months. And then somebody is not happy, let us fix it again. We have got to have some common sense here.

And also, I think, a little bit of marketplace issue as well. Government will not, cannot, and should not solve all of your problems. You need to get this right, and you need to get it together voluntarily, and then, as is spoken of just a few minutes ago, then government can step in where need be and help the process along.

In looking at this, I am encouraged by what I am hearing and have been encouraged by some meetings that I have had even this week. But I believe there is still a lot of work that needs to be done. In fact, even this morning, did a quick Google search for "Parks and Recreation" episodes online, and at the bottom of the search results on the first page, I read this: "In response to a complaint we have received from the U.S. Digital Millennium Copyright Act, we have removed one results from this page. If you wish, you may read the DMCA complaint that caused the removals or removal at chillingeffects.org."

Okay. There is a little bit of a political comment right there. That is fine. I get it. And, look, I would like to have Google here to discuss this.

Now, in full disclosure, I have talked to Google this week in one of their offices, and we have brought up some of this as we went along, because I think they have an already important role that search engines play in this and the possibility that they can really dramatically alter the online piracy landscape for the better.

However, I am concerned that maybe we are not addressing this or investing in this as much as we should. In fact, I want to go to you, Mr. Sherman, because out of your written testimony, you seem to indicate that they are not invested at all and, in fact, do not seem to be making any effort to promote legitimate options for streaming content. I just want to ask you, is that an accurate representation of your testimony?

Mr. SHERMAN. No, I don't think so. I think Google has done things. My problem is that they are measuring their actions by how much stuff they are doing rather than the impact that it is having. When they run their own business, I doubt that if they keep a lot of people busy, they would regard that as sufficient. They probably want to make sure that it results in a meaningful revenue impact. We need the same thing.

Mr. COLLINS. So you are saying quantity doesn't always recommend to quality.

Mr. SHERMAN. Right.

Mr. COLLINS. Okay. Would others like to address this? I will open it up to the rest of the panel, from Ms. Lesser all the way down. Anybody want to take a bite?

It is okay, guys. It is afternoon, you can laugh.

Mr. COBLE. It is afternoon provided they beat the red light.

Mr. COLLINS. Exactly. As we do that. They are saying, we are going to get in under his minutes as we can.

Here is the question. Look, I am going to actually give back a little bit of my time today, because this is something that our office has been heavily involved with and will continue to be involved with.

I want to go back to my statement just a few minutes ago. This applies not only in this environment here. There is definitely a need for this Committee, and we will be heavily in jurisdiction with the fine folks from both sides of the aisle here looking at this. I think there are going to be ways that we can work to protect the owners and protect the rights and then still provide content, because I believe by protecting those rights, you actually expand innovation, you expand productivity, and we are going to be a part of that.

But I think what we also got to come to the conclusion here is that this is an issue that needs to be addressed, it needs all parties to the table, and to do so in a long-lasting way. So, again, to come here is voluntary agreements are fine. Those are what needs to be happening. We need to continue this discussion. But I am also not convinced this is going to be where it ends. So it will continue this process as we go further.

With that, Mr. Chairman, I yield back.

Mr. COBLE. I thank the gentleman.

The distinguished gentleman from New York Mr. Jeffries is recognized for 5 minutes.

Mr. JEFFRIES. Thank you, Mr. Chairman.

And let me thank the witnesses for your testimony today.

It is clear to me that reasonable people should be able to agree that online piracy is a significant problem, deserves to be addressed. The people who create content, it seems to me, should have the opportunity to benefit from the fruits of their labor and encourages creativity moving forward. It is fair, and it is just as consistent with Article I, Section 8 of the Constitution designed to promote the progress of science and useful arts.

But it is also the case, I think, I believe, that the Internet has been a wonderful field of opportunity for entrepreneurship, for innovation, for growth beyond which many could have even contemplated 15 or 20 years ago. And so we don't want to do anything in the Congress certainly, or even in the business context, that limits the ability for that innovation and that growth and that entrepreneurship to continue to flourish on this field of opportunity called the Internet.

And you have got a lot of different players in the Internet ecosystem, I gather. You know, you have the search engines, the ISPs, content creators, payment processors, ad companies.

And so I guess I will start by asking Ms. Lesser, and then maybe Mr. Sherman and Mr. Rothenberg can weigh in, from your perspective, what is the best way to get all of the individuals in this ecosystem to work together in a manner that deals with the online piracy, that clearly should be a problem that we take seriously and confront, but also respects the Internet in a manner not designed to limit the opportunities that have been available through the innovation and the entrepreneurship and the growth in this medium?

Ms. LESSER. What I would say from the experience that we have had thus far in our small group involving ISPs and the content industry is that if you look at this in your silo, you are not going to find a solution. If we start from where you started with the Constitution, that there is a value in protecting creative content, something that if you ask people on the street they agree with, something that we are trying to teach to kids, I think if you start with that premise and you move down, what you find is that innovation and the development and the distribution of content cannot only co-exist, but can help each other. And I think what we are learning in our group, that there are benefits to both.

So our program is an educational program, is focused on the attitude toward creative content generally and then helping people find the legal ways that they can access content.

So I don't think that it should be as hard as it is. And it is based on, you know, 15 years of back-and-forth in the policy arena, in the business arena. But everything is really moving toward the same place, and I think once this group came to the table, it was very clear that their interests were aligned, which is why you see companies like the five leading ISPs investing their own resources in this agreement and bringing this agreement to fruition.

Mr. JEFFRIES. Thanks.

Mr. Sherman.

Mr. SHERMAN. I think there is no substitute for dialogue, and I mean nonthreatening dialogue where it isn't over liability, it isn't over responsibility; it is how you can work together.

When we engaged in conversations with the ISPs, we started in very different places, but we learned a lot from each other by just talking it through. And we brought in additional stakeholders who looked at consumer viewpoints, and privacy viewpoints, and so on. And the end of that stew was a process that everybody could buy into and support.

That is the kind of process I think we need to replicate with respect to multiple industry sectors to get lots of people involved in solving this. And as soon as you have two groups and three groups and four groups, more and more people will be willing to do it.

On the advertising side, because of the best practices that the ad networks and the IAB did, we have been contacted just in the last couple of weeks by a number of additional ad networks asking for our help and for information so that they could do a better job themselves. You get buy-in because you have had buy-in, and that is the process we need to get going.

Mr. ROTHENBERG. Again, thank you for the question, Mr. Jeffries. And, again, I can't really improve on what Mr. Sherman and Ms. Lesser have said, but I will try.

You can't get them all in a room. There are hundreds of millions of people around the world that are part of the Internet ecosystem. The beauty of the Internet supply chain is also the great vulnerability of the digital supply chain. It is basically open source. It allows for enormous innovation from the smallest players, but it also creates great vulnerabilities.

You can get the biggest and most significant players in the room to reach voluntary agreement. And as Mr. Sherman has said, that process, with encouragement from the Congress and from other bodies, can actually yield great results.

Importantly, one of the big changes over the past several years is that many of the biggest players in the digital technology industry have also become content creators. Google, Microsoft, AOL all are presenting slates of original digital video programming, and they are basing a very substantial part of their evolving business on being content creators. So they have stakes in this game on all sides.

I think working together among major stakeholder groups to create a coherent program in which all have skin in the game is the best way to go about it. Now, I would tell you that my ideal, and I am not necessarily speaking for all my members, but certainly what I would like to see happen is the development of some kind of Good Housekeeping Seal of Approval program for participation in the digital supply chain, so that buyers of digital advertising, for example, can look and see who is a legitimate player and who is not. I would like to see us push in that direction.

Mr. COBLE. The gentleman's time has expired.

Mr. Levitt, if you and Mr. Barchiesi wish to respond very briefly.

Mr. BARCHIESI. From our perspective, I hear a lot about content, but the International AntiCounterfeiting Coalition, we represent cross industries, there is health and safety issues, there is content issues. Ultimately again I will emphasize voluntary agreements work when there is willing partners. There is proof of concept. We have had this program for 2 years. And could I tell you 3 years ago, if I said I want to work with MasterCard, Visa, or American Express, PayPal, MoneyGram, Western Union, they wanted to run me out of town. Now we host events together. We work together on public service messaging. I think it is a model that could be used and established in other arenas to move forward.

Mr. COBLE. Very briefly, Mr. Levitt. We are running out of time.

Mr. LEVITT. Okay. Well, you know, Pharmacy Checker's area is not copyright content. It has to do with the purchase of medication online. And I just think it is important when we look at these voluntary agreements that different areas should be treated differently.

Former Intellectual Property Enforcement Coordinator Espinel, I quote, "challenged the private sector to voluntarily address the health and safety issues presented by rogue online pharmacies." And I just want to reiterate that this is the only way we should engage in this area for shutting down those sites that endangers a person's health.

Mr. COBLE. Gentleman's time has expired.

I am trying to keep this train rolling. You know, of course, your complete statements are in part of the record. So even though I

may have been accelerating my pace at one time, your information will be read by all.

I am now pleased to recognize the gentlelady from California Ms. Lofgren for 5 minutes.

Ms. LOFGREN. Thank you, Mr. Chairman.

And thanks to the panel for your testimony.

And I remember just a short time ago, when we were having a rather raucous discussion of SOPA, that the discussion was maybe we should follow the money, and it looks like actually some of that has occurred here, to good effect. So I want to congratulate those who have worked to try and find solutions. And I am sure there is lots more to do, but sometimes it is worthwhile to celebrate what has been achieved, not just complain about what yet remains to be done.

Just a couple of questions, and I don't want these to be taken as opposition to making progress, because they are not. But one of the things that these voluntary agreements raise is the issue of due process for people who are legitimate, but maybe aren't found to be legitimate. For example, and you said, Ms. Lesser, we start with the Constitution. Yes, we have a protection for intellectual property, copyright, and patent. But in the copyright arena we also have the First Amendment and the fair use doctrine. So how do we make sure that, I mean, people who are making fair use, that their rights are protected? How do you address that in your system?

Ms. LESSER. Well, that is one of the very important aspects of the system. As I said in my testimony, we developed a system that on the front end is very much focused on notifying consumers about copyright violations of whole works. So there is a methodology that has been put in place and streamlined so that we are very assiduously trying to avoid capturing works that are not covered by copyright or that would fall into this fair use category. So on the front end, there has been a lot of work put into making sure there are not false positives.

At the end of the process, however—and our process does not end with really a punitive consequence; it ends with a heightened measure we call mitigation—but just before a user would have that mitigation measure imposed, they are offered the right to an appeal. And I put “appeal” in quotes.

Ms. LOFGREN. If I can interrupt. It is not that I don't want to hear the whole thing, but we have limited time.

The user has interests, but the speaker also has interests, and the two are not always perfectly aligned. So if you are the speaker, and let us say you have a belief, maybe correctly or incorrectly, I don't know, that what you are doing is a parity, or it is a political speech, or that it is protected, how do you protect your rights without relying on the Internet user to establish your rights?

Ms. LESSER. I am not sure that the protection of that right actually falls within the program. The program itself assumes that an alert has been sent to an account holder, and that account holder has the ability to go during that appeal process and say, this file was a fair use.

Ms. LOFGREN. Right. Right. But what about the person who created the content that is being dinged? Are they being notified?

Ms. LESSER. They are not. But I actually think the best way to protect people engaging in fair use is on the front end, which is to enforce copyrights against—

Ms. LOFGREN. Right.

Ms. LESSER [continuing]. Protected files.

Ms. LOFGREN. In terms of payment processing, I remember during the SOPA discussion we had a substantial discussion about cutting off credit card payments for infringing sites. And I remember Visa, which is right outside my district, said that they would be happy to do that, but they were rarely ever asked to do so. And it sounds like that has changed considerably in the time that has processed. And I think that makes sense. But, again, for example, a notice and takedown, the person who has an opportunity to dispute that if they feel that it is incorrect.

You know, cutting off payments is a death sentence for a Web site. Do they have any opportunity to contest that if they think that there is an incorrect decision that has been made? What is the process for that?

Mr. ROTHENBERG. In our program, which is about cutting off or helping to choke off advertising revenues, it is basically an information system between the buyers and the sellers. They are the ones who are the trading partners; they are the ones in contract. We don't have a consumer-facing side to it. And I agree with you that there needs to be some form of due process in there.

But by the same token, I think what we ought to be most concerned about are the largest and most persistent violators. I am less worried, although I, as you do, I worry about smaller players falling through the cracks deeply. But I think if we keep our focus on the worst violators and the most persistent violators, those problems will not—the problem of the—the small fry being shut off will not be so—

Ms. LOFGREN. I just have one final question. I know from the study that was released this morning that about 30 percent—what was the number—37 percent of the searches for infringing content were searches for a domain name or a specific service, like Mega Upload or something like that. So at least, you know, a big chunk of the people that are looking for infringing content know what they are looking for, they are looking for infringing content, and not being confused.

So I guess that leads to the question, and MPAA isn't here. What further efforts are being made to have digital content more freely available for a fee? And I will just give you an example.

You know, there was a movie. It is out on DVD now. I wanted to watch it streaming. I Googled it. The only place it was available were infringing sites. I won't do that, but I imagine other people do. So the more that you could actually pay for stuff, the more that is out there, I think the less than honest people will infringe. So I am just wondering what further efforts are being made. And I think it is probably more for the movie industry than for the music industry.

Mr. SHERMAN. Certainly the music industry, we are almost two-thirds now of our revenues being digital. And all the music is out there, all the music is up there in every possible way. We think

that movies and TV are getting there quickly. I can't speak for that.

But that same survey that you mentioned also had a figure that 58 percent of the people were using search where they weren't entering anything indicating they were looking for an illegal copy, but they were led to an illegal copy anyway, because search engines can be used for discovery. How did they find out about Mega Upload the first time? Now they know to go—no longer, fortunately—but how do they know to go to the Pirate Bay or MP3 Skull? Search takes them there. That is why we would like to work with them to try and find ways to address that.

Ms. LOFGREN. My time is up, Mr. Chairman. I don't want to abuse the clock. Thank you.

Mr. COBLE. I thank the gentlelady from California.

The distinguished gentleman from North Carolina Mr. Watt is recognized.

Mr. WATT. Thank you, Mr. Chairman. And I want to thank the Chairman for having another hearing about this. I want to make sure that nothing I say gets misconstrued to imply that I don't believe in these agreements. I think they are great.

I am not sure I agree with Mr. Poe that all of this can be done without some government involvement. I suppose if private agreements worked to solve all criminal activity, it would be—we wouldn't need any enforcement in the non-Internet world. I think we still need some help in this area.

And the magnitude of the problem, I hope, is going down, but I assume there is nobody on this panel who believes that this can all be done by private agreements. If there is, I certainly want to hear from them and give you the opportunity to express that opinion, because we need it on the record.

But you were getting ready to press your button?

Mr. ROTHENBERG. I would just say, Mr. Watt, I think we would all, or at least most of us, agree that we should start with the voluntary agreements, and then where there are gaps that cannot be filled by the voluntary self-regulation, then and only then would we seek to fill them with legislation and regulation.

Mr. WATT. Okay. We started our SOPA discussions dealing with foreign sites. Has any of these private agreements dealt with that problem effectively? Can somebody address that for me?

Mr. BARCHIESI. The ICC's program does deal with foreign sites because it doesn't matter where in the world the site is hosted. These are contractual agreements between credit card companies and banks and merchants, and it has global terms to it, and they could terminate merchant accounts regardless of where they are, anyplace in the world.

Mr. WATT. And it is a voluntary agreement.

Mr. BARCHIESI. Yes.

Mr. SHERMAN. I think it is important to remember that the voluntary agreements are built on contractual relationships that already exist. So Visa has contractual relationships with the people it serves that they will not process payments for illegal activities. So if illegal activities are called to their attention, and then they do their own investigation and confirm that, they have a contrac-

tual right to terminate whether it is domestic or foreign, but it is under their own contractual relationship.

The voluntary agreement is simply providing a mechanism for routing all of these complaints through one portal to make it efficient, to not have duplication of efforts, to have a standardized system. That is the benefit of these agreements. It creates a mechanism for everybody to go forward in the same direction to address the issue in a similar way.

Mr. ROTHENBERG. And to your specific point about foreign infringement, again, we would be very much in favor of this Congress pushing in the direction of incorporating the frameworks that we are talking about into global trade agreements. Whether you call that public solutions, or private solutions, or a quasi public-private, there is definitely a role for the public sector there.

Mr. WATT. Another major problem that we were trying to solve with SOPA was the problem of repeat offenders. Sites that went up one day, got the DNCA notice, they got taken down, they were back up the next day, how the voluntary agreement is solving that problem.

Mr. SHERMAN. That is one of the core elements that we would like to see in all of these agreements, like with locker services or search engines who—for example, there are mobile apps. We asked Google to take it down because it is clearly infringing. Google takes it down. They go up again a week later using a slightly different name, but it is the same app.

Repeat infringement policies there would make a difference where developers could be banned from the app store if they are going to continue to infringe.

Mr. WATT. But I guess my question is can that be done through a voluntary agreement?

Mr. SHERMAN. I don't see why not.

Mr. WATT. Who would be the parties to that agreement?

Mr. SHERMAN. Well, the policy would be basically articulated by whoever the platform is. It could be Google, it could be Visa, it could be a locker service. Basically saying that if you are—

Mr. WATT. Encourage them to come to the table and enter into that agreement, I guess.

Mr. SHERMAN. Exactly. Just that we are going to adopt as a best practice a repeat infringement police. For one company, it might be two; for another company, it might be five. But they are going to have a policy so that they don't basically have the up, down, up, down, up, down process. But after a while they are saying—

Mr. WATT. So you would have a “three strikes and you are out” policy—

Mr. SHERMAN. Whatever number of strikes.

Mr. WATT [continuing]. Or “five strikes and you are out” policy that sometimes we apply criminal law.

Mr. SHERMAN. After all, we are talking about people who are in business, and they don't want to be in the business of basically harboring illegal content or dealing with the same problem over and over again, just like an ISP doesn't want to have to deal with somebody who keeps violating their terms of service. They have an absolute right to decide who they are going to serve if they continue to engage in illegal conduct.

Mr. WATT. Okay. Well, I do want to applaud everybody who has been parties to these agreements. I think it is great that the private sector and all of the parties are trying to solve a problem. I am not sure I believe you are going to be able to solve all of the problem that way, but I guess if we keep having hearing after hearing after hearing about whether something is necessary, maybe it at least keeps the focus on the issue.

At some point I think we are actually going to have to do something other than have a hearing about it. So that is kind of where I come down on this.

But I applaud it. I applaud your efforts. I heard Mr. Levitt's concerns about—and especially in the pharmaceutical area. But I encourage all parties to continue to try to work toward these voluntary agreements so that we don't have to keep having the hearing after hearing after hearing, and ultimately so that possibly we don't have to do anything that would involve the government being involved. Surely that would be the worst thing that could happen. We could disband the police if we had enough voluntary agreements.

So anyway, I yield back, Mr. Chairman.

Mr. COBLE. Gentleman's time is expired.

I want to thank the very fine panel of witnesses. I also want to thank those in the audience who have remained for this entire hearing. This indicates to me that you have more than a casual interest in this subject matter. And I thank all of you.

This concludes today's hearing. Thanks to all of you for attending.

Without objection, all Members will have 5 legislative days to submit additional written questions for the witnesses or additional materials for the record.

This hearing stands adjourned.

[Whereupon, at 3:41 p.m., the Subcommittee was adjourned.]

A P P E N D I X

MATERIAL SUBMITTED FOR THE HEARING RECORD



QUALITY ASSURANCE GUIDELINE (QAG)

VERSION 2.0

Released: July 25, 2013

This document has been developed by the IAB Quality Assurance Guideline Initiative Committee

The IAB Quality Assurance Guideline (QAG) was updated to version 2.0 by a working group of volunteers from 26 IAB member companies.

The Working Group was led by Chairs:

- **Tim Avila**, Vice President, Product Marketing, BrightRoll, Inc.
- **Jed Nahum**, Senior Director, Global Channels & Exchange, Microsoft
- **Aianna Gombert**, Strategic Partnerships Manager, Google

The following IAB member companies contributed to this document:

| | |
|----------------------------------|---------------------|
| Accuen (Omnicom) | Millennial Media |
| Adapt.TV | Mojiva |
| AppNexus | NBC Universal |
| BrightRoll | Ogilvy (WPP) |
| CBS Interactive | OpenX |
| Cadreon (IPG) | PubMatic |
| DataXu | Rocket Fuel |
| DGB Digital Broadcasting Group | SpotXchange |
| Google | TubeMogul |
| Im Services | Telemetry |
| Mediacom (WPP) | Tremor Video |
| M6D media6degrees | ValueClick |
| Microsoft | The Weather Company |

The lead on this initiative was Rob Rasko of The 614 Group on behalf of the IAB

Contact qag@iab.net to comment on this document. Please be sure to include the version number of this document (found on the bottom right corner on this page).

ABOUT THE IAB'S QUALITY ASSURANCE GUIDELINE INITIATIVE STEERING COMMITTEE

The QAG Initiative has been formed to oversee the guidelines and oversee any future iteration. The 614 Group has been engaged to manage the process of updating and the promotion of the guidelines in the marketplace. The IAB's Ad Technology group has been tasked with operational management of the Initiative. Before QAG was expanded beyond only Networks and Exchanges, the QAG initiative was overseen by the Networks and Exchanges Committee.

The mission of the QAG Initiative Steering Committee is to reduce friction and foster an environment of trust in the digital advertising marketplace by defining guidelines that promote transparency in digital advertising transactions. For more information about the QAG, please email qag@iab.net.

This document is on the IAB website at:

http://www.iab.net/QAGInitiative/overview/quality_assurance_guidelines

Table of Contents

| | |
|---|-----------|
| Executive Summary | 5 |
| Audience | 6 |
| 1 Overview: Digital Advertising Transactions | 6 |
| 1.1 The Parties to a QAG Transaction Agreement | 6 |
| 1.1.1 Sellers | 6 |
| 1.1.2 Buyers | 7 |
| 1.1.3 Non-Transactional Parties | 8 |
| 1.2 The QAG Transaction | 8 |
| 1.2.1 Inventory Acquisition | 9 |
| 1.2.2 Inventory Evaluation | 9 |
| 1.2.3 Transaction Execution | 9 |
| 1.3 Advertising Formats of a QAG Transaction | 10 |
| 1.3.1 Display and text | 10 |
| 1.3.2 In-Stream Video | 10 |
| 1.3.3 Mobile | 11 |
| 1.3.4 Programmatic Buying/Auction Mechanics | 11 |
| 2 QAG Certification Process | 11 |
| 2.1 Application | 12 |
| 2.1.1 Qualification | 12 |
| 2.1.2 Key contacts | 12 |
| 2.1.3 Certification Fee | 13 |
| 2.1.4 Training Availability | 13 |
| 2.2 Six-Month Gating Period | 13 |
| 2.3 Certification | 14 |
| 2.3.1 Self-Certification | 14 |
| 2.3.2 Independent Validation | 14 |
| 2.3.3 Publication of Certification Status | 15 |
| 2.4 Certification Renewal | 15 |
| 2.4.1 Self-Certification | 15 |
| 2.4.2 Independent Validation | 15 |
| 3 QAG Certification Program | 15 |
| 3.1 IAB QAG Initiative Steering Committee | 15 |
| 3.2 Disclosure | 16 |
| 3.2.1 Inventory Acquisition | 16 |
| 3.2.2 Inventory Evaluation | 16 |
| 3.2.3 Transaction Execution | 16 |
| 3.3 Compliance Officer | 17 |

IAB Quality Assurance Guidelines 2.0

| | | |
|----------|---|-----------|
| 3.3.1 | Qualifications | 17 |
| 3.3.2 | Responsibilities | 17 |
| 3.3.3 | The QAG Compliance Team | 17 |
| 3.4 | Quarterly Reviews | 18 |
| 3.5 | Description of Methodology (DOM) | 18 |
| 3.6 | Enforcement & Appeal | 18 |
| 3.6.1 | QAG Non-Compliance | 19 |
| 3.6.2 | Validating Complaints | 19 |
| 3.6.3 | Loss of Certification | 19 |
| 3.6.4 | Appeal and Recertification | 19 |
| 3.7 | Intellectual Property (IP) Infringement Complaints | 19 |
| 4 | Disclosure Details | 20 |
| 4.1 | Inventory Acquisition | 20 |
| 4.1.1 | Transaction Party Source Identification and Relationships | 20 |
| 4.1.2 | Source Level Transparency | 21 |
| 4.1.3 | Technical Context | 22 |
| 4.2 | Inventory Evaluation | 23 |
| 4.2.1 | Content Type | 23 |
| 4.2.2 | Content Classification | 23 |
| 4.2.2.1 | The QAG Taxonomy | 24 |
| 4.2.2.2 | Custom Taxonomies for QAG | 25 |
| 4.2.2.3 | Labeling Contextual Content | 25 |
| 4.2.2.4 | Adding categories to the QAG Taxonomy | 25 |
| 4.2.3 | Content Rating | 26 |
| 4.2.4 | Non-Standard Classification | 27 |
| 4.2.5 | Illegal Content Prohibited from Sale | 28 |
| 4.2.6 | Level of Confidence | 28 |
| 4.2.7 | Targeting Depth | 29 |
| 4.2.8 | Placement Details | 30 |
| 4.2.9 | Creative Specifications | 31 |
| 4.3 | Transaction Execution | 32 |
| 4.3.1 | Data | 32 |
| 4.3.2 | Programmatic Buying/Auction Mechanics | 32 |
| 5 | Glossary of terms | 34 |
| 6 | Appendix | 43 |
| | Exhibit A: Compliance Officer Attestation | 44 |
| | Exhibit B: Executive Attestation | 45 |
| | Exhibit C: Sample Independent Validation Attestation | 46 |

Executive Summary

With more than a million sites that carry advertising and the hundreds of technology vendors, the transaction of ads in the digital advertising ecosystem is complex. Without some framework for common ground, buyers aren't sure which sellers to trust and sellers have a difficult time trying to prove their integrity.

The IAB Quality Assurance Guidelines (QAG) promotes the flow of advertising budgets into digital advertising with industry regulation that offers a framework for brand safety.

The mission of the Quality Assurance Guidelines (QAG) Program is to reduce friction and foster an environment of trust in the marketplace by providing clear, common language that describes characteristics of advertising inventory and transactions across the advertising value chain.

The goals of the QAG program are to:

- Support the information needs of advertising buyers
- Define a common framework of disclosures that sellers can use across the industry
- Offer clear language in the QAG disclosure framework that enables buyers to make informed decisions
- Review compliance among QAG-certified companies and facilitate the resolution of disputes and complaints.

QAG offers value to both buyers and sellers:

Benefits for the Buyer

QAG provides transparency for buyers, enabling them to buy advertising inventory with confidence. QAG was created in joint efforts by buyers and sellers and represents the buyers' voice to sellers in defining terms for seller disclosure.

Benefits for the Seller

QAG creates a simple, common, and standard language to describe and classify advertising opportunities. Doing so makes buying inventory easier for the buyer, which increases overall demand for QAG-certified sellers. Increased inventory value for certified companies enables increased revenue because QAG certification classifies these companies as industry leaders, which clearly distinguishes them from any bad actors.

Version 2.0 of the IAB Quality Assurance Guideline (QAG) includes updates that improve the quality of the QAG Program.

- **All Sellers:** Initially limited to only network and exchange members of the IAB, QAG 2.0 is opened up to any advertising inventory seller in the digital supply chain—IAB member or not.
- **Additional Certification Option:** Companies can choose to self-certify as traditionally offered, or add a layer of certification that involves an independent party who validates the self-certification.
- **Certification Process Defined:** While defined in the previous version of QAG, version 2.0 offers a more streamlined process for application, certification, and renewal.
- **Video, Mobile, Programmatic Considerations:** Disclosures for technical context, content type, creative specifications, programmatic exchange, and improved placement detail options incorporate information needs for buys that include video, mobile, and programmatic buying campaigns.

- **Improved Readability:** A document overhaul offers structure and guidance that is more clearly defined for both buyer and seller audiences.

Though QAG 2.0 offers improvements that are sure to increase adoption across the industry, the IAB QAG Initiative is a living process that is improved only by industry participation and adoption.

Audience

Any party interested in the requirements or certification process for the QAG Certification Program can benefit from being familiar with the guidelines in this document. Specifically, any company interested in achieving QAG Certification status can use these guidelines as a resource for taking the steps necessary to achieve and maintain QAG Certification.

1 Overview: Digital Advertising Transactions

A transaction in digital advertising is an agreement between a buyer and a seller in which the seller provides inventory that the buyer values and purchases at agreed upon terms and conditions. This agreement is typically defined by a contract such as an Insertion Order (IO), Terms and Conditions (T&C), or equivalent. This contract becomes the key vessel for a buy or campaign.

The IAB Quality Assurance Guideline (QAG) Initiative aims to ensure quality in such transactions; more specifically QAG describes a framework within which sellers represent inventory to buyers, and in this representation aim to deliver safety, transparency, and trust in digital advertising transactions.

The following sections describe the parties to a QAG transaction in more detail, the structural breakdown of a QAG transaction, and the different advertising formats that may be included in a QAG transaction.

1.1 The Parties to a QAG Transaction Agreement

A QAG Transaction is between a buyer and a seller, but in digital advertising a buyer may merely represent the party who owns the advertisements and ultimately pays for the transaction. A buyer may also purchase inventory without any initial representation of the advertisement owner. The seller may likewise represent the original owner of inventory, or may resell inventory that it has purchased from the inventory owner.

In addition, while a QAG transaction only directly involves the buyer and the seller, any number of indirect parties, such as technology and service providers, may play a role in providing the resulting digital advertising experience.

1.1.1 Sellers

A seller in a QAG transaction offers ad placement inventory to advertisers. Direct sellers either own the inventory for sale or represent the inventory owner. Indirect sellers don't have a direct relationship with the inventory owner, but may be qualified to resell a direct seller's inventory.

Direct Sellers and APAs

The most direct seller is a publisher company that provides content to an audience. The seller's inventory is ad space that offers value to advertisers depending on the size and demographics of the audience. While a publisher may sell this inventory directly, larger publishers may appoint an agent to manage and sell this inventory.

In the QAG Program, this agent is an Authorized Publisher Agent (APA). An APA is also a direct seller. Publishers formerly appoint APAs and the relationship is established with a contractual, and often financial, agreement.

A publisher may choose to have one exclusive APA to provide more control over its inventory or may have more than one authorized agent per site (domain). In either case, only the inventory owner may designate a representative APA. An APA is prohibited from appointing another APA or transferring its designation as an APA to another non-APA agent.

Indirect Sellers

An indirect seller sells publisher inventory but does not have a direct, contractual relationship with the publisher. For example, an indirect seller, such as a network or exchange, may have an agreement with a publisher-appointed APA to resell remnant inventory but does not have a direct relationship with the publisher.

As an example to distinguish a direct seller from an indirect seller, a publisher may partner with a company that is acting as an APA to manage its non-reserved inventory. The APA offers the publisher's inventory to various networks on a site-specific basis. When those networks contract with the APA to purchase inventory from the publisher, then the APA is a direct seller to the networks. If one of those networks resells the inventory purchased from the APA, the network is an indirect seller of the publisher's inventory.

The value of QAG for Sellers

Sellers work hard to offer value to buyers. Publishers, in particular, focus on developing quality content for their audiences and driving quality traffic to their sites, creating value for advertisers. However, the value to advertisers can be difficult to define and match to an advertiser's needs without some way to qualify claims made in a digital advertising transaction.

With QAG certification, sellers have a way to distinguish themselves among those companies that offer quality, transparently defined transactions in the digital advertising market.

1.1.2 Buyers

A buyer in a QAG transaction buys a seller's inventory that it uses to advertise products or services to the seller's audience. Direct buyers either own the advertisements for placement on the seller's site or directly represent the advertisements owner. Indirect buyers don't have a direct relationship with the advertisement owner, but may be qualified to assign the direct buyer's advertisements to a seller's inventory.

Direct Buyers and Authorized Advertiser Agent (AAA)

The most direct buyer is a brand company represented in the advertisements it wants to place on seller inventory; however, most prominent brands hire an agency to manage their advertisement campaigns.

In QAG, a brand-appointed agency is an Authorized Advertiser Agent (AAA). An AAA represents an advertisement owner under a contractual, often financial agreement, between the advertisement owner and the AAA. An AAA is also a direct buyer.

The advertisement owner may appoint more than one AAA, but only the advertisement owner may designate a representative AAA. An AAA may not appoint another AAA or transfer its designation as an AAA to another agent.

Indirect Buyers

An indirect buyer purchases seller inventory without formerly representing an advertisements owner. For example a technology company may purchase inventory in anticipation of placing a direct buyer's advertisements in the purchased inventory.

Also, an indirect buyer may purchase remnant inventory without any initial representation of the advertisements it will place in the purchased inventory. In many cases, an indirect buyer may purchase inventory and then become an indirect seller of the inventory purchased.

The Value of QAG for Buyers

With all the technology, proprietary practices, service vendors, and other digital advertising products, details for a purchase can be difficult to decipher. Agency buyers have a responsibility to their clients to ensure client brands are associated with a quality experience.

Buyers that buy from QAG-certified companies can be assured that transactional claims are inline with practices that are self-regulated and reviewed quarterly.

1.1.3 Non-Transactional Parties

Though a digital advertising transaction is an agreement between the buyer and the seller, several organizations may be party to enabling the transaction or offering additional products and services based on transactional data. Some examples of non-transactional parties are the technology platforms such as ad servers, privacy vendors, and tag management.

Additionally, services such as media attribution, creative optimization, and other analytic offerings may use data from a transaction they're not party to in order to add value either to the transaction or to future transactions with other, possibly unrelated, buyer-seller agreements.

A graphical view of the digital advertising arena might help illustrate all the parties that might be involved in delivering a successful media experience. Please visit <http://www.iab.net/iabarena> for an illustrative view of the IAB Digital Advertising Arena.

The Value of QAG for Non-Transactional Parties

For parties that are neither a buyer nor a seller in a transaction, supporting QAG-certified transactions can help an organization encourage more quality transactions in the marketplace. Commitment to working with QAG-certified companies helps a supporting organization ensure that it operates within quality market transactions and therefore provides better quality products and services.

For information on becoming a QAG Supporting Member, please visit <http://www.iab.net/QAGapply> and apply as a Supporting Sponsor.

1.2 The QAG Transaction

The QAG Transaction is an agreement between a buyer and a seller in which the seller discloses the expected context where ads display and the buyer agrees to the terms and conditions in which the transaction is disclosed. In a QAG transaction, a seller is as transparent as possible about how the transaction will be executed.

The IAB acknowledges that sellers can't always disclose everything in a transaction; sellers may not know or have access to such details, depending on the nature of the transaction. In such situations, the seller must disclose its lack of knowledge where applicable. This transparency enables the buyer to assess value and risk associated with the transaction.

Transaction details and level of transparency are disclosed at the time of transaction before the buy is executed. In the case of a programmatic transaction, certain details may be disclosed programmatically during real-time transactions as they occur, but details on the expected execution of programmatic transactions are disclosed at the time the buyer-seller agreement is made.

Disclosures in a transaction are categorized under:

- Inventory Acquisition
- Inventory Evaluation
- Transaction Execution

Each of these transaction categories is described in sections 1.2.1-1.2.3 as follows.

1.2.1 Inventory Acquisition

Acquiring inventory involves disclosing details such as the buyer and seller relationships to advertisement and inventory ownership, respectively, the level of transparency over the source URLs to where ads are expected to display, and the expected technical context in which ads display.

Inventory acquisition disclosures are described in the sections listed as follows:

- 4.1.1 Transaction Party Source Relationships
- 4.1.2 Source Level Transparency
- 4.1.3 Technical Context

1.2.2 Inventory Evaluation

Evaluating inventory involves determining how “safe” the inventory is for the buyer’s ads. For example, for what audiences are contextual sites rated? What type of content is provided on inventoried sites? Is the inventory being offered at a site or page level, or a deeper level? What are the placement details and what creative specifications are accepted?

Inventory evaluation disclosures are described in the sections listed as follows:

- 4.2.1 Content Type
- 4.2.2 Content Classification
- 4.2.3 Content Rating
- 4.2.4 Non-Standard Classification
- 4.2.5 Illegal Content Prohibited from Sale
- 4.2.6 Level of Confidence
- 4.2.7 Targeting Depth
- 4.2.8 Placement Details
- 4.2.9 Creative Specifications

1.2.3 Transaction Execution

Two important details are disclosed regarding the execution of the transaction: how data is used and what is disclosed in real-time for programmatic transactions. While programmatic buying details are disclosed in real-time, the expectation for real-time disclosures is stated at the time of establishing the buyer-seller agreement.

Transaction execution disclosures are described in the sections listed as follows:

- 4.3.1 Data
- 4.3.2 Programmatic Buying/Auction Mechanics

1.3 Advertising Formats of a QAG Transaction

A QAG transaction may include various types of advertising formats that can range from general display and text to video or mobile options. In addition, programmatic buys that may exchange a combination of these formats in a transaction may be defined as part of a campaign or as the primary execution of the campaign.

QAG 2.0 supports disclosures for advertising formats described in the following sections from 1.3.1 to 1.3.4.

1.3.1 Display and text

In general, traditional display and text advertising are the most common forms of advertising. Display and text advertising can provide rich, interactive experiences to audiences for which they are displayed.

QAG-certified transactions offer transparency into the context where ads are being served. This transparency enables advertisements to be paired with the right inventory, increasing the value of the inventory by offering some level of brand protection depending on the level of transparency disclosed in the transaction.

QAG was designed with traditional display and text formats in mind, but disclosures regarding details such as the technical context, content type, and placement and creative details help distinguish traditional display from formats such as that for video and mobile.

1.3.2 In-Stream Video

In-stream video inventory is ad space offered in the context of streaming video. Ads may be a linear video that plays before, after, or during a break in the streaming video, or ads may be in the format of an image or interactive media that overlays the streaming content.

QAG supports disclosures specific to transactions that include in-stream video ads. Disclosure options described in the following list help define in-stream video inventory in a QAG transaction.

- 4.1.3 Technical Context:** a seller can disclose the technical context for its inventory, which includes digital in-stream video as an option.
- 4.2.1 Content Type:** a seller can disclose the content type of its inventory. Video is an option for this disclosure, but may define any type of video content, including both streaming and progressive download formats as well as connected tv.
- 4.2.8 Placement Details:** a seller can disclose accepted media formats for its inventory, including specific in-stream video ad formats that align with the IAB Video Ad Serving Template (VAST) 3.0.

1.3.3 Mobile

With the rapid adoption of mobile devices over the last few years and the increased sophistication of each new mobile device brought to market, advertisers can't help but look for inventory that is offered in a mobile context.

Mobile advertising is specific to applications installed on consumer devices (native apps), browser-based applications designed for mobile (Web apps), or mobile-optimized and responsive design websites. Browser-based advertising designed for desktop computers and merely viewed on a mobile device is excluded from the generally accepted definition of mobile advertising.

As with in-stream video, certain QAG disclosures help to define a transaction that includes mobile advertising:

- 4.1.3 Technical Context:** a seller can disclose the technical context for its inventory, which includes mobile as an option.
- 4.2.1 Content Type:** a seller can disclose the content type of its inventory. Games and applications are offered as an option and are generally associated with mobile devices, but these content types may also be designed for desktops or game systems. Paired with disclosures for technical context and placement details, other content type disclosure options such as music, video, and text can help better define a transaction that includes mobile advertising.
- 4.2.8 Placement Details:** a seller can disclose accepted media formats for its inventory, such as whether the inventory is specific to native apps, web apps, or mobile-optimized or responsive design webpages.

1.3.4 Programmatic Buying/Auction Mechanics

Programmatic transactions are handled by automated systems that exchange ads and inventory in real-time. These exchanges are often executed based on various real-time bidding (RTB) auction types defined by parameters set up in user interfaces.

For buyer-seller agreements that include programmatic buying components, QAG offers guidance on disclosures that can be made in real-time programmatic transactions. While the nature and expectations of the programmatic buy are disclosed upon establishing the buyer-seller agreement, specific details are disclosed upon execution of real-time exchanges.

In addition to the option for "full real-time" disclosure of the source URL (section 4.1.2), section 4.3.2 offers guidance on disclosing the auction type and other optional details for a real-time exchange.

2 QAG Certification Process

Certification can be obtained at two different tiers: self-certification and independent validation certification. A company has the option to choose one tier or the other. The selected method is recorded and displayed on the IAB website. Since the internal processes for both certification tiers are the same, a company that certifies under self-certification can add independent validation certification at any time to achieve the higher level of certification.

IAB Quality Assurance Guidelines 2.0

Self-certification is obtained with a self-attestation that the company is adhering to the IAB Quality Assurance Guidelines. Independent validation certification is obtained by inviting an independent vendor to validate that a company is adhering to these guidelines. The process is parallel for both except that in an independent validation, the validating company submits additional required attestation paperwork and reports.

Transition from QAG 1.5 to QAG 2.0

Companies previously certified under QAG 1.5 can renew certification under those guidelines in 2013. However, all companies certified under QAG 1.5 are afforded six months from the release of QAG 2.0 to certify under the new 2.0 guidelines. QAG 1.5 certification will expire and no longer be supported six months after the release of QAG 2.0 (the publication date of this document is the QAG 2.0 release date and is indicated on the title page).

All new applicants will be certified under QAG 2.0 as of the release of this document.

The QAG certification process involves: application, a six-month gating period, and finalization of certification. These steps are outlined in the following sections from 2.1 to 2.3. Further details of compliance expectations are described in section 3.

2.1 Application

QAG certification begins by applying online at IAB's website. Details about application are defined below. More information can be found at <http://www.iab.net/QAGapply>.

2.1.1 Qualification

Any company that sells inventory in the digital advertising supply chain can qualify for QAG certification. Previously, certification was only open to IAB member companies; however, in QAG 2.0, certification is open to non-member companies. Additional fees may be required for non-member company certification.

Certification may not make sense for some companies. For example a brand company doesn't explicitly exchange any data or ads directly, but may choose to only work with QAG certified companies to serve and manage their campaigns. Companies that don't qualify for QAG certification can choose to be a supporting member of the QAG Certification Program. For a fee a QAG supporting member company receives a Supporting Member seal and the option of participating in future discussions around guideline evolution.

To apply as a QAG Supporting Member, please visit <http://www.iab.net/QAGapply> and apply as a Supporting Member.

2.1.2 Key contacts

Key contacts described in the following list are needed on file and available for QAG certification related communication. A single person may be listed for multiple contacts, and specific titles or roles are not required for any of the contacts. The IAB simply needs these contacts on file and available for QAG certification related communication.

IAB Quality Assurance Guidelines 2.0

The following contacts help facilitate IAB communications with QAG-certified companies:

- **Compliance Officer:** The compliance officer is an appointed person at the applicant company who will attend training and lead the effort to ensure that the company is QAG-compliant.
- **Billing:** A contact must be identified for billing QAG Certification and renewal fees.
- **Marketing:** Upon certification, the marketing contact on file is given the QAG Certification seal and any other materials and information that the company can use to promote itself as a certified company.
- **Business Lead:** Someone with decision-making authority must be identified to ensure QAG Certification is supported at the executive level.
- **Rights and IP Contact:** After certification, the IAB needs to make a contact available for the market should any claims of infringements on intellectual property, copyrights, or other proprietary work or process be brought to light while in the QAG Certification Program.

2.1.3 Certification Fee

The fee for certification depends on IAB membership and application details. IAB members pay a reduced fee while non-IAB members are charged a higher fee. A small fee is required for companies who want to be QAG Certification Program Supporting Members. And Start-ups receive a special introductory low rate for certification. The certification fee covers training for up to two people and supports the IAB infrastructure for processing and publishing certification.

Detailed fee information can be found on IAB's website at <http://www.iab.net/QAGapply>.

2.1.4 Training Availability

The application process includes scheduling training. Training is required for the company's appointed QAG Compliance Officer, and is scheduled during the application process. The compliance officer completes training during the six-month gating period described in the next section.

2.2 Six-Month Gating Period

To accommodate for training needs to be QAG certified, companies who apply to be QAG certified enter a 6-month gating period. The gating period starts with the date that the IAB QAG training program is scheduled to start.

During this time:

- The appointed compliance officer completes training
- Quality assurance compliance team is assembled
- Quality Assurance Description of methodology (DOM) is developed
- Compliance team is trained on quality assurance methodologies documented in the company's DOM
- Conduct at least one internal audit (self-certification) or coordinate with validation vendor to conduct independent review (independent validation)

2.3 Certification

With training and consistent quality assurance methodologies in practice, the company is certified when required documentation is submitted and certification status is posted to IAB's website. Upon certification, the IAB sends materials to the marketing contact on file for promoting the company's QAG certification status.

Document requirements for certification are dependent on the certification option selected: self-certification or independent validation.

2.3.1 Self-Certification

A company wishing to self-certify must submit the following documents:

- Application fee
- Internal audit report
- Signed Attestation documents:
 - Compliance Officer Attestation (see Exhibit A in the Appendix)
 - Executive Attestation, signed by the CEO, CFO, or Business Head (see Exhibit B in the Appendix)

2.3.2 Independent Validation

To achieve certification by independent validation, a company can invite an independent vendor to validate that the company is QAG-Compliant. A validating company may be any accredited auditing company such as a licensed law firm or licensed CPA. In addition, any company that submits for and is approved by the IAB may conduct independent validations.

While independent validation was designed to provide limited assurance, ensuring that all QAG requirements are being met within the company's operations, technology and supporting documentation may take some time to review. Review time depends on several factors such as company operations maturity level, organization size and complexity, and technology. Additionally, the initial review will take longer than subsequent reviews as is common in most ongoing engagements. Companies should solicit multiple proposals from qualified vendors to ensure that they are getting the appropriate level of service at the most competitive price.

Independent validation will include review of, but is not limited to, the following:

- Job description of the compliance officer
- Training policy and procedures
- Internal audit policies and procedures
- Established policies & procedures related to internal control
- Policies and procedures for adding new advertisers
- Policies & procedures related to adding new Publishers, including how new Publishers are vetted (and "re-vetted")
- Policies & procedures related to complaint handling/resolution to ensure compliance with the IAB Guidelines

Established policies & procedures related to internal control that have been established by the organization. To achieve independent validation, the certifying company submits documentation listed in section 2.3.1, and the validating company submits the following:

- Independent Validation Attestation (see sample attestation, Exhibit C in the Appendix)

2.3.3 Publication of Certification Status

The IAB publishes QAG certification announcements for companies that have successfully implemented these guidelines at the end of the 6-month gating period. Publication includes identification of the certification method chosen: self-certification or independent validation. The list on the IAB QAG Certified Companies page is updated as needed to reflect all current QAG certified companies.

To see a list of currently certified companies, please visit <http://www.iab.net/QAG>.

2.4 Certification Renewal

QAG Certification is an ongoing process and must be renewed each year. The QAG Certification year begins on April 1st. The IAB sends renewal notifications to all QAG-Certified companies prior to this date. Renewal requirements depend on whether the company is self-certified or independently validated.

2.4.1 Self-Certification

A company renewing self-certification must submit the following documents:

- Renewal fee
- Internal audit report
- Signed Attestation documents
 - Compliance Officer Attestation (see Exhibit A in the Appendix)
 - Executive Attestation, signed by the CEO, CFO, or Business Head (see Exhibit B in the Appendix)

2.4.2 Independent Validation

To renew an independent validation certification, a company invites an independent vendor to validate that the company is QAG-Compliant. This independent vendor must also submit an attestation validating the QAG certification applicant's quality assurance claims in addition to the company-submitted documents listed in section 2.4.1.

- Independent Validation Attestation (see Exhibit C in the Appendix)

3 QAG Certification Program

The IAB Quality Assurance Guidelines (QAG) Certification Program is voluntary and represents the ongoing process of defining and maintaining guidelines for transparency in the buying and selling of media inventory online.

QAG-certified companies enter into an agreement with the IAB in which the company is responsible for making inquiries, obtaining relevant and necessary reports, and otherwise regularly reviewing its activities so that it can represent and confirm at all times that it is in compliance with the Program.

The components of the QAG Certification Program are described in the following sections 3.1 to 3.6. Inventory transaction disclosure requirements are described in section 4.

3.1 IAB QAG Initiative Steering Committee

The IAB QAG Initiative Steering Committee (the Committee) is the governing body for the QAG Program. In general, the committee is seated with QAG company representatives.

The QAG Steering Committee mandate is:

- Evaluate any QAG related complaints and determine the responsibly and penalty
- Provide guidance and vision for current and future QAG efforts
- Oversee and ensure progress of QAG efforts
- Evangelize the program in the marketplace
- Report progress or issues to IAB Executive Committee and Board of Directors upon invitation
- Ensure any policy issues within the QAG effort is properly shared with IAB Policy leadership

Details about the structure, duties, and other relevant information about the IAB QAG Initiative Steering Committee can be found on the IAB website at:

http://www.iab.net/QAGInitiative/overview/steering_committee.

3.2 Disclosure

The following list summarizes disclosures that are expected at each of the three phases of digital advertising transactions outlined in this document: inventory acquisition, inventory evaluation, and transaction execution.

Please review section 4 for specific details on disclosures.

3.2.1 Inventory Acquisition

Upon inventory acquisition, QAG certified companies should accurately label inventory in accordance with the established content framework defined in section 4.1. This framework includes inventory disclosures in the following four categories:

- Source Identification
- Source Relationship
- Source Level
- Technical Context

3.2.2 Inventory Evaluation

Once inventory is identified, QAG certified companies should accurately label surrounding content and other inventory details in accordance with established guidelines as explained in section 4.2. Inventory evaluation disclosures fall within the following four categories:

- Contextual Content
- Targeting Depth
- Placement Details
- Creative Details

3.2.3 Transaction Execution

Upon final transaction, QAG-certified companies must accurately identify intent for data collection and usage and follow programmatic buying disclosures, if applicable, in accordance with established guidelines as explained in section 4.3. Execution disclosures are outlined as follows:

- Data
- Programmatic Buying/Auction Mechanics

3.3 Compliance Officer

To ensure that QAG-certified companies continue to maintain compliance with these guidelines, the compliant company appoints a QAG Compliance Officer. If a company is self-certified, this compliance officer oversees a quarterly review to ensure QAG compliance. Upon certification and each year during certification renewal, the QAG Compliance Officer submits a report of the most recent internal audit. For companies that are independently validated, the QAG Compliance Officer facilitates an independent vendor review for initial certification and each year for renewal. The independent vendor submits a letter of attestation validating the company's compliance with QAG.

Whether self-certified or independently validated, all QAG-certified companies are required to have a trained QAG Compliance Officer on staff. No requirements are made for the job description or specific title or role requirement of the QAG compliance officer.

3.3.1 Qualifications

The QAG compliance officer should meet the following minimum qualifications:

- Have reporting relationships whereby compliance assessments are not influenced or biased by operations personnel being tested for compliance
- Have adequate technical training and proficiency in testing and assessing compliance
- Have adequate knowledge of the subject matter covered within these guidelines
- Have an independence in mental attitude with regard to compliance assessments:
 - Maintaining intellectual honesty and impartiality
 - Objectively considering facts using unbiased judgment
 - Exercise due professional care in performing self-certification tasks described as follows in section 3.3.2.

3.3.2 Responsibilities

The Compliance Officer is responsible for the following:

- Attending IAB compliance training (in person or online*)
- Educating internal teams on IAB Quality Assurance Guidelines and notifying them of any changes
- Providing internal review documentation for QAG Attestation
- Maintaining the company's Description of Methodology

*While attending online training is acceptable, online training may or may not be available. Check with your QAG representative for availability.

3.3.3 The QAG Compliance Team

Recognizing that companies both large and small apply for QAG certification, no requirements are made for the resources needed to support QAG compliance.

The QAG compliance team is responsible for the following:

- Reviewing the publisher intake process
- Reviewing content
- Applying the standard rating system to content
- Implementing quarterly reviews for quality control

3.4 Quarterly Reviews

IAB training for compliance focuses on outlining the principles for internal reviews and is developed with the guidance of the IAB QAG Initiative Steering Committee. Quarterly reviews create consistency across the industry.

The QAG Compliance Officer is responsible for overseeing quarterly reviews, which should insure that:

- Guidelines are consistently and completely followed
- Error situations are detected in a timely fashion
- Appropriate corrective measures are taken in a timely fashion

Internal reviews should also include a risk analysis of certain control functions to assess how much testing is needed to validate adherence. Also, actual testing of data (i.e. sites, pages, ads, logs, etc.), both statistically and judgmentally based, should be used to validate that the existing control structure is designed correctly and operating effectively.

3.5 Description of Methodology (DOM)

The QAG Description of Methodology, or DOM, describes the company's technical methods for how inventory details are disclosed to parties with whom the QAG-certified company does business and the processes for ensuring that stated practices are maintained.

The DOM is central to QAG Certification. Quarterly and independent reviews are based on the methodologies documented in the DOM. The better the DOM and the technology and practices that support it, the more efficient the process for quarterly and independent validation reviews. The level of detail plays a role in a good DOM. A DOM too detailed might be overly complex and difficult to maintain, but a DOM too simplified may be too vague to appropriately meet minimum certification guidelines.

The IAB does not define how this document should be structured or the content required, but at a minimum, a well-defined description of methodology might incorporate the following:

- Clearly stated guiding principles for the company and its QAG Certification Program
- Regular practices involved in disclosing inventory details
- Description of how company technology discloses inventory details
- Defined plan for ensuring all quality assurance technology and regular practices are maintained
- Method for detecting and correcting errors
- Process for making updates to the QAG Certification Program and the corresponding documentation in the DOM

While the DOM is not submitted for certification or renewal, the internal audit is based on the DOM and the most recent version of the DOM should always be available should it be requested for review.

3.6 Enforcement & Appeal

QAG compliance is peer-enforced. In order to ensure that the value of QAG certification is maintained, a formal process is in place for companies to make complaints about non-compliance.

3.6.1 QAG Non-Compliance

Complaints made against a QAG-certified company may be one of two complaint types:

- QAG non-compliance
- Intellectual Property (IP) infringement

Complaints regarding QAG non-compliance may affect certification while IP infringement complaints do not. Please see section 3.7 for details on IP infringement complaints.

A company that is party to a QAG-certified transaction may submit a complaint against the other party of the transaction regarding any non-compliance experienced. The complaint must include specific evidence of non-compliance and must be signed by someone of at least manager level at the company making the complaint.

To submit a complaint, please visit <http://www.iab.net/QAGComplaints>.

3.6.2 Validating Complaints

Upon receiving a complaint, the IAB QAG Steering Committee votes on whether the complaint is valid. If deemed valid, the accused QAG-certified company is notified of the complaint before the Committee makes a judgment regarding the complaint.

Before judgment on a complaint is made, the accused company may repudiate the allegation of non-compliance or remediate any alleged incidents of non-compliance.

If the Committee makes a judgment against the accused company, the company must work in a good faith effort to resolve the complaint as quickly as possible.

3.6.3 Loss of Certification

If three or more complaints against a single company are deemed valid within a six-month period and valid complaints are not resolved within that six-month period, certification for the company is removed. The company must cease to market itself as a certified company and the company name is removed from the published list of QAG-certified companies. Complaints are not made public.

3.6.4 Appeal and Recertification

Within 10 days of the Committee decision to remove certification, the company may appeal before the full Committee.

In order to become recertified, the company must provide documentation on how and when the complaint was addressed and the steps it has taken to ensure that similar problems will not occur in the future. Documentation of complaint resolution must be presented before the full Committee.

If the majority of the Committee is satisfied with the explanations and evidence of resolution, the company may pay a recertification fee to the IAB and resume marketing itself as QAG certified. The company is also republished to the list of QAG-certified companies.

3.7 Intellectual Property (IP) Infringement Complaints

To facilitate a rights holder complaint about copyright infringement, the IAB provides an inbox for such complaints that it forwards to the alleged infringing companies. To file a complaint, please send details about your complaint and the offending company to IPcomplaints@iab.net. The IAB will direct this complaint to the relevant contact at each QAG participating company.

4 Disclosure Details

Transparency is vital to establishing trust and enabling the flow of advertising budgets throughout the marketplace. QAG 2.0 requires transparency at each phase of a media transaction and provides a framework for labeling inventory so that buyers can accurately assign value and/or assess risk. All disclosures defined throughout section 4 should be disclosed in the buyer-seller agreement prior to running the buyers ads on the sellers' sites.

Inventory Framework

The QAG Inventory Framework is a series of defined disclosures that clearly labels the seller's inventory for the buyer. This framework simplifies transparency and adds value to reported impressions regardless of the level of transparency.

QAG-certified sellers must use the QAG Inventory Framework to label all inventory sold so that advertisers can accurately assign value and/or assess risk. Recognizing that some transactions can't be as transparent as others, the QAG inventory framework allows for non-transparent transactions as long as they are labeled as such.

For each buyer-seller agreement (i.e. insertion order (IO), campaign, or buy), the buyer can reasonably expect that every impression run under the agreement meet the criteria represented.

If any seller within a single agreement sells an array of inventory with multiple levels of transparency, the agreement must structure the inventory so that each level of transparency is represented in a different line item. If the inventory is not or cannot be separated into different line items, then all inventory must be assigned a level of transparency equal to the least transparent item sold in the agreement.

The QAG Inventory Framework is broken down into phases of inventory transaction as it happens either in real time or processed prior to running impressions. The three phases of transaction defined in the inventory framework are: inventory acquisition, inventory evaluation, and transaction execution.

Required disclosures for each phase are described in sections 4.1 to 4.3.

4.1 Inventory Acquisition

The details disclosed as part of acquiring the inventory include identifying the parties involved in the agreement, the level of transparency in disclosing source page URLs, and the technical context describing the environment in which ads are served.

4.1.1 Transaction Party Source Identification and Relationships

QAG-certified companies must disclose their relationship with the owner of the source of media. This relationship may be either direct or indirect on either the sell side or the buy side.

IAB Quality Assurance Guidelines 2.0

Transaction party source relationships are defined in the following table:

Table 4-1: Transaction Party Source Relationships

| | Direct | Indirect | Programmatic |
|--------|---|--|---|
| Seller | Owens inventory to be sold or formerly represents the owner in a contractual agreement. Publishers or Authorized Publisher Agents (APA) are direct sellers. | Sells inventory that it doesn't own or directly represent. A network or exchange with no direct relationship to inventory owner is an example of an indirect seller. | Mimics a seller, either direct or indirect, but is represented by an automated technology platform in real-time transactions. |
| Buyer | The party that owns or represents advertisements to be placed on the seller's available media inventory. Advertisers or Authorized Advertiser Agencies (AAA) are direct buyers. | Purchases inventory on behalf of a direct buyer but lacks an authorized direct relationship with the advertiser. | Mimics a buyer, either direct or indirect, but is represented by an automated technology platform in real-time transactions. |

See section 1.1 for more detailed descriptions of the parties to a QAG Transaction.

| | |
|-----------------------------|--|
| Publisher Protection | Buyer may not resell inventory on an exchange without having disclosed to the seller in advance that an exchange-based re-sale is among the monetization options the buyer may pursue. |
|-----------------------------|--|

4.1.2 Source Level Transparency

Both buyers and sellers need to know how much will be disclosed regarding the source URL for the inventory to be sold. Source level transparency may be disclosed in full in real time, as a complete list of sites to be used (full disclosure), as a list of potential sites to be used (partial disclosure), or as a general list of possible contextual sites or unknown sites (no disclosure) where ads may run.

Except for full real-time disclosure, source URL disclosure level is disclosed in an agreement prior to running impressions. The buyer-seller agreement should specify the terms by which the seller may update the inventory source URL list.

Source level transparency includes the following:

Full real-time disclosure

The seller passes the buyer the complete URL for the inventory where the ad displays in real time for each automated transaction and is passed at the moment of impression. Full real-time disclosure enables the buyer's ad-serving workflow to decide on a number of factors for serving the ad such as valuation and creative selection.

Full real-time disclosure requires that the complete URL of the original publisher page where the ad displays among publisher content is provided to the buyer's system. Disclosing only the iframe URL that is separate from the page that contains content is NOT considered full real-time disclosure.

For native mobile applications, a source URL is not available. In these cases, full real-time disclosure requires providing the complete URL for the app store page where the application is listed.

In all cases for full real-time disclosure, sellers must pass the content source URL or app store URL without modification.

Full disclosure

In full disclosure, the seller discloses to the buyer, prior to running impressions, a list of all the website domains and/or native mobile applications where ads may run. Ads may not run on *all* sites or applications listed, but ads will *not* run on any sites or applications other than those listed.

Partial disclosure

In partial disclosure, the seller discloses to the buyer, prior to running impressions, a list of representative sites and/or native mobile applications where ads will run. Ads may run on sites and applications other than those listed, but will not necessarily run on all sites and applications listed.

No disclosure (blind/no site list):

With no disclosure, the seller discloses to the buyer, prior to running impressions, that the seller is blind to the sites or native mobile applications on which ads will run, or that ads may run on certain contextual sites, such as “automotive” sites.

4.1.3 Technical Context

The technical context of the inventory includes whether the inventory is intended for display in a browser, digital in-stream video, mobile specific, or unknown.

Browser: inventory displays in a browser, typically for desktop viewing.

Digital in-stream video: inventory displays in the context of streaming video within a video player. Video companion ad inventory is considered contextual to digital in-stream video even though it is displayed in a browser near the digital video player.

Mobile: inventory is intended to play within content optimized for mobile viewing, either within a native mobile application, in a browser-based application intended for mobile viewing, or a mobile-optimized web page.

Connected TV: inventory displays in the context of a web-connected television device.

Unknown: inventory may display in any of the contextual technology platforms.

4.2 Inventory Evaluation

Evaluating the seller's inventory means establishing the context in which ads are displayed. Disclosing contextual details for content includes identifying the following:

- 5.2.1 Content Type
- 5.2.2 Content Classification
- 5.2.3 Content Rating
- 5.2.4 Non-Standard Classification
- 5.2.5 Illegal Content Prohibited From Sale
- 5.2.6 Level of Confidence
- 5.2.7 Targeting Depth
- 5.2.8 Placement Details
- 5.2.9 Creative Acceptance Details

4.2.1 Content Type

While sections 4.2.2 - 4.2.5 address classification of content, disclosing the content type helps QAG-certified companies determine the medium of the content.

The content type describes the type of content that is displayed either near the ad, or immediately before or after the ad is displayed. It provides the advertiser with information about the viewing context, or the activity that the user is engaged in when they are shown the ad.

Content type may be classified as one of the following:

- **Video:** a video file that is streaming or loading, including (Internet) television broadcasts
- **Game:** an interactive software game that is running
- **Music:** an audio file or stream that is playing, including (Internet) radio broadcasts
- **Application:** an interactive software application that is running
- **Text:** a document that is primarily textual in nature, including web page, ebook, or news article
- **Other:** the user is consuming content of known type but which does not fit into one of the categories above
- **Unknown:** content type is unknown

4.2.2 Content Classification

The content in which an ad is placed is important to both parties, but especially for the buyer who is concerned about brand safety. The contextual content can be disclosed in all media types, whether browser-based, video, or mobile. If the contextual content for where ads are displayed can't be identified, then the content classification can be disclosed as "unknown."

A contextual taxonomy helps classify content in a familiar way across the industry. QAG-certified companies must, if applicable to the buy, develop a contextual taxonomy relevant to the inventory they offer and consistent with the tiered structure outlined in this section. Contextual content information is not to be passed in real-time unless the source level transparency is “full real-time disclosure.”

4.2.2.1 The QAG Taxonomy

The QAG Certification Program offers a contextual taxonomy developed in consultation with taxonomy experts from academia, ad measurement companies, and members of the IAB Networks & Exchanges Committee. This taxonomy defines contextual content categories on at least three different tiers.

The first tier is a broad level category defined as a targeting depth of either: category/portal, site section, or page. Tier 2 categories and greater are additional categories nested under Tier 1 categories. Both tier 1 and tier 2 categories are formerly established for the QAG Certification Program so content classification can be consistent across the industry.

QAG-certified companies define their own content classification taxonomy based on the QAG Contextual Content Tier Structure. See section 4.2.2.2 for details on defining a custom taxonomy that is compliant with the QAG program.

The following table (table 4-1) describes the tiered taxonomy for contextual content classification. Table 4-2 provides a sample of QAG established categories.

Table 4-2: QAG Contextual Content Classification Tier Structure

| | Definition |
|----------------|---|
| Tier 1 | Primary content definition for the targeting levels of category, site, or section. This level defines the general category of the content. Categories at this level are formerly established for QAG. |
| Tier 2 | Secondary content level categories nested under Tier 1. Categories at this level are formerly established for QAG. |
| Tier 3+ | Sub-categories nested under Tier 2. Categories at this level and greater are defined and maintained by individual companies. |

IAB Quality Assurance Guidelines 2.0

The following table is a sample of two of the tier 1 categories in the formally-established QAG Taxonomy along with their tier 2 nested categories. Updates are maintained on IAB's website at <http://www.iab.net/QAGInitiative/overview/taxonomy>.

Table 4-3: Sample QAG Contextual Content Categories

| Tier 1 Category | Tier 2 Categories | | | | | | | | | | | | | | | | | | | | | | |
|---------------------------------|--|------------|--------|-------------|--------|---------------------|----------|-------------|-------------|---------------------|-------------------|-------------|--------|-------|----------------------|-----------|-------|--------|------------------------|------------------|--------------|-----------|-------|
| Arts & Entertainment | Books and Literature Celebrity Fan/Gossip Fine Art Humor Movies | | | | | | | | | | | | | | | | | | | | | | |
| Automotive | <table border="0"> <tr> <td>Auto Parts</td> <td>Hybrid</td> </tr> <tr> <td>Auto Repair</td> <td>Luxury</td> </tr> <tr> <td>Buying/Selling Cars</td> <td>Mini Van</td> </tr> <tr> <td>Car Culture</td> <td>Motorcycles</td> </tr> <tr> <td>Certified Pre-Owned</td> <td>Off-Road Vehicles</td> </tr> <tr> <td>Convertible</td> <td>Pickup</td> </tr> <tr> <td>Coupe</td> <td>Road-Side Assistance</td> </tr> <tr> <td>Crossover</td> <td>Sedan</td> </tr> <tr> <td>Diesel</td> <td>Trucks and Accessories</td> </tr> <tr> <td>Electric Vehicle</td> <td>Vintage Cars</td> </tr> <tr> <td>Hatchback</td> <td>Wagon</td> </tr> </table> | Auto Parts | Hybrid | Auto Repair | Luxury | Buying/Selling Cars | Mini Van | Car Culture | Motorcycles | Certified Pre-Owned | Off-Road Vehicles | Convertible | Pickup | Coupe | Road-Side Assistance | Crossover | Sedan | Diesel | Trucks and Accessories | Electric Vehicle | Vintage Cars | Hatchback | Wagon |
| Auto Parts | Hybrid | | | | | | | | | | | | | | | | | | | | | | |
| Auto Repair | Luxury | | | | | | | | | | | | | | | | | | | | | | |
| Buying/Selling Cars | Mini Van | | | | | | | | | | | | | | | | | | | | | | |
| Car Culture | Motorcycles | | | | | | | | | | | | | | | | | | | | | | |
| Certified Pre-Owned | Off-Road Vehicles | | | | | | | | | | | | | | | | | | | | | | |
| Convertible | Pickup | | | | | | | | | | | | | | | | | | | | | | |
| Coupe | Road-Side Assistance | | | | | | | | | | | | | | | | | | | | | | |
| Crossover | Sedan | | | | | | | | | | | | | | | | | | | | | | |
| Diesel | Trucks and Accessories | | | | | | | | | | | | | | | | | | | | | | |
| Electric Vehicle | Vintage Cars | | | | | | | | | | | | | | | | | | | | | | |
| Hatchback | Wagon | | | | | | | | | | | | | | | | | | | | | | |

4.2.2.2 Custom Taxonomies for QAG

QAG-certified companies are not required to use all categories developed for the taxonomy and should develop their own customized taxonomy; however, the custom taxonomy should clearly map back to the QAG Contextual Taxonomy. For example, if a company has a Recreation category, the company must be able to show how it maps back to the tier 1 Sports category in the QAG Taxonomy. A buyer should be able to understand a seller's custom taxonomy in sufficient detail. If a seller does not adhere to the QAG Taxonomy, the company's Description of Methodology should disclose this and include the appropriate mapping.

4.2.2.3 Labeling Contextual Content

Contextual content labeling may be done internally or by an independent organization. No requirement is made for designating who should label contextual content.

4.2.2.4 Adding categories to the QAG Taxonomy

The QAG Contextual Taxonomy is dynamic and developing categories is an ongoing process. This taxonomy is intended to capture the breadth of available online content and present a clear and consistent framework to buyers.

The IAB QAG Initiative Steering Committee oversees a sub-committee on taxonomy for matters pertaining to the established taxonomy structure. QAG-certified companies may petition the Committee to include new content categories into the existing QAG Taxonomy. The Committee reviews petition submissions quarterly, and publishes results to the IAB website for the QAG Taxonomy at <http://www.iab.net/QAGInitiative/overview/taxonomy>.

4.2.3 Content Rating

Content ratings are already standardized across all certified networks & exchanges with the site rating determined at the time the site first joins the network or exchange. However, for companies that are not a network or exchange, any sites that offers inventory in the QAG Program must be rated in compliance with QAG.

QAG-certified companies should rate site content according to the following rating system*:

All Audiences

Appropriate for all segments of the general public. For this rating, all of the following must apply:

- No profanity
- No sexual content
- No violence
- No depictions of alcohol, tobacco, weapons, gambling, or drug use

Everyone over 12

May contain material considered inappropriate for young children. Any of the following may be present:

- Implicit references to vulgar language
- Kissing
- Violence to animated characters
- Journalistic references to alcohol, tobacco, weapons, gambling, or drug use

Mature Audiences

May contain material suitable only for mature audiences. Any of the following may be present:

- Profanity
- Provocative images
- Nudity
- Violence to human beings or animals
- Depictions of alcohol, tobacco, weapons, gambling or drug use, etc.

Unknown

Content cannot be determined or is unknown.

*Rating site content according to the above rating system is compliant with QAG; however, a company can choose to use a different rating system as long as the rating system used is described in the company's DOM and ratings map back to the rating system described above.

4.2.4 Non-Standard Classification

Non-standard classification may be disclosed at a page, section or site level but should be labeled at the lowest common denominator for that page, section or site. The following characteristics must be disclosed for each transaction and must be accurate for the level of targeting:

| Non-Standard Classification | |
|--|---|
| Extreme Graphic/Explicit Violence | The depiction of especially vivid, brutal and realistic acts of violence. It may be real, simulated live action, or animated. Graphic and/or Explicit Violence goes beyond lesser forms of violence due to its clear and unabashed nature of the violence portrayed. |
| Pornography | Sexually explicit material whose primary purpose is designed to produce sexual arousal. Types of content can include, but is not limited to, representations of sexual acts and exposed body parts, sexual coercion, and illegal sexual acts. |
| Profane Content | Excessive or inappropriate use of profane language |
| Hate Content | Speech or hate graphic content |
| Under Construction | Sites that are under construction |
| Incentivized | Sponsor "incentivized clicks," or "pay-to-surf" programs |
| Unmoderated UGC | UGC sites that do not have a clear set of posted guidelines on what type of content is acceptable and do not take an active position in reviewing content for compliance with posted guidelines. For the purposes of these guidelines, User Generated Content (UGC) is defined as forums as well as the uploading by users of video, audio or photographic content that is either user-created or created by a third-party. |

4.2.5 Illegal Content Prohibited from Sale

QAG prohibits the sale of any inventory within the following categories of illegal content. The category descriptions below include non-exclusive examples of the types of sites that fit in those categories.

| Illegal Content Prohibited from Sale | |
|--------------------------------------|---|
| Illegal Content | Content related to engaging in, promoting or facilitating illegal or legally questionable activities such as drugs, bombs, theft, and online pirating, hacking, spamming, and infecting as governed by United States Federal law. |
| Warez | P2P, torrent sites, illegal music downloads, pirated software |
| Spyware/Malware | Distribute or promote spyware or malware |
| Copyright Infringement | Infringes on copyrights (for example by hosting and streaming infringing copyrighted content). |

4.2.6 Level of Confidence

The QAG review involves vetting the site against the list of non-standard content and characteristic descriptions provided in section 4.2.4. To ensure that site ratings stay current, a statistically valid sample size of publishers is reviewed as part of the quarterly review described in section 3.4.

By taking a statistically valid sample size, advertisers are assured with a reasonably high level of confidence that the rating and classification systems are being upheld. Certified companies may employ an independent rating service as long as the service vendor complies with the guidelines established in the most recent version of QAG. Ultimately, the QAG-certified company is responsible for maintaining and certifying compliance.

IAB Quality Assurance Guidelines 2.0

The table below shows the different sample sizes required at three different confidence levels with a margin of error of 5%.

| Sample size with a 5% margin of error | | | |
|--|--|------------|------------|
| # of Sites | Sample Sizes @ Confidence Level | | |
| | 90% | 95% | 99% |
| 100 | 74 | 80 | 87 |
| 250 | 131 | 152 | 182 |
| 500 | 176 | 217 | 286 |
| 1,000 | 214 | 278 | 400 |
| 2,500 | 245 | 333 | 526 |
| 5,000 | 257 | 357 | 588 |
| 10,000 | 264 | 370 | 624 |
| 25,000 | 268 | 378 | 648 |
| 50,000 | 270 | 381 | 657 |
| 100,000 | 270 | 383 | 661 |

An example of how to interpret the table is as follows: if you conduct a poll to determine the percentage of "unsafe sites" with a pool of 250 sites, and you want to be 95% confident in the results, then you must check 152 sites. If after checking this sample, you didn't find any unsafe sites, then you may claim that you are 95% confident that the actual percentage of unsafe sites in your network is null – with a margin of error of 5%.

Note: The above table was developed using statistical probabilities of a normal distribution. For further information, please see http://en.wikipedia.org/wiki/Normal_distribution.

The required confidence level for QAG is at least 90%. In the case that the 90% confidence level is not achieved, the process below must be followed:

- Review and re-categorization of publishers in accordance with established guidelines
- Complete re-test of inventory at or above pre-determined confidence level
- Record each test result as proof of the internal review

4.2.7 Targeting Depth

Five levels of targeting are defined for disclosure in the QAG program. Depth of targeting starts at the broadest tier in which a group of sites may be included in a buy and funnels down through the site, site section, specific page, and individual unit such as a specific video.

IAB Quality Assurance Guidelines 2.0

In addition to content category, the content level being targeted must be defined. The following table explains the targeting hierarchy, ranging from the multi-site level to the individual units on the page. These guidelines do not require certified QAG-certified companies to offer all targeting levels.

| Targeting Depth | |
|---|---|
| Category/Portal Level | Target a grouping of sites within a specific buy |
| Site Level | Targeting to endemic sites where the majority of the content is on a specific topic that can be targeted at site level |
| Site Section Level | Subsections of sites are classified into subordinate categories |
| Page Level | Pages within a web site (determined using a semantic or contextual engine) |
| Unit Level (widget, video, image, text, other) | This type of targeting classifies every element on a "page" into one of the defined categories. Text content identified by semantic or contextual search engine; Video and image content identified by metadata tags. |
| None | Not targeting content but targeting users. |

4.2.8 Placement Details

The seller discloses placement details in the buyer-seller agreement regarding where on the page or in an application the ad will be placed and what media characteristics are accepted for the inventory being sold. Placement details are not to be passed in real-time unless the source level transparency is "full real-time disclosure."

Display Ads

Sellers should indicate what type of ads they accept for given inventory and the features they support for accepted ads:

- Expandable creative (yes, known, unknown)
- Supported rich media properties (list of RM properties or unknown)
- Supported creative behavior (list of behaviors or unknown)
- In-banner video* (yes, no, unknown)
- In-text video (yes, no, unknown)
- Positioning (above-the-fold, below-the-fold, or unknown)

* in-banner video must include audio controls and default to audio off

Digital In-Stream Video Ads

Digital in-stream video ads are ads that display in the context of streaming video content played in a video player and not to be confused with in-banner ads that may also play in a video player but within the context of a banner and NOT within the context of streaming video content. Sellers should disclose what digital in-stream video ad formats they accept.

Sellers should disclose each of the following parameters (if known) for digital video ads:

- Ad Type (linear, nonlinear, unknown)
- Linear ad type position (pre-roll, mid-roll, post-roll, unknown)
- Ad Duration (in seconds)
- Default width and height (in pixels)
- Auto Play (yes, known, unknown)
- Ad Pod length and position
- Skippable (yes, no, unknown)
- Audible (yes, no, unknown)
- Incentivized: (yes, no, unknown)

Mobile Ads

Mobile inventory includes inventory that displays in native mobile applications (App), browser-based Web applications (wApp), or mobile-optimized websites. Sellers should disclose the following details about mobile inventory:

- App (yes, no, unknown)
- Web App (yes, no, unknown)
- Mobile Web* (yes, no, unknown)
- Responsive Design** (yes, no, unknown)
- Positioning (header, footer, side bar, full screen, or unknown)
- Targeted Platform (iOS, Android, Blackberry, Windows Phone, webOS, Symbian, or other)

*Mobile-optimized websites are distinguished by some variation in the site URL such as mobile.example.com, or example.com/mobile.

**Responsive design websites are programmed to scale in response to the size of the browser so that content can be viewed as intended whether on a large-screen device or a small-screen device.

In general, browser-based display inventory designed for viewing on a desktop-sized computer or laptop screen is NOT considered mobile despite visitors' ability to view the content in a mobile device.

4.2.9 Creative Specifications

Publishers have a fundamental interest in promoting an experience for their visitors that sustains or increases their loyalty, session time, and engagement. Ads can enhance that experience if the ads are appropriately matched to the space, content, and audience.

Publishers have varying degrees of tolerance for the aggressiveness of advertisement implementation, content and features. Creative specifications are to be disclosed in the buyer-seller agreement prior to running impressions unless the source level transparency is "full real-time disclosure," in which case creative specifications can be disclosed in real-time.

The seller should disclose any applicable creative specifications for accepting creative using attributes from the following list:

- Creative width and height (in pixels)
- Creative file weight
- Auto sound
- Auto play animation
- Video
- Video duration
- Video controls required
- Expanding
- Expansion direction
- Expanded size
- Specific IAB formats

4.3 Transaction Execution

Once inventory has been identified for acquisition and evaluated for contextual content classification and placement, how data is to be collected and used should be disclosed in the buyer-seller agreement. In addition, programmatic exchange details should be disclosed, but these details (described in section 4.3.2) may be disclosed in real-time at the time of transaction.

4.3.1 Data

While IAB membership is not required for certification, any company interested in becoming QAG certified should also agree to abide by the IAB Member Code of Conduct. Details about the IAB Member Code of Conduct can be found on IAB's website at http://www.iab.net/public_policy/codeofconduct.

| | |
|---------------------|---|
| General Note | A working group in the QAG initiative plans to define data transparency in more detail in an update following the release of QAG 2.0. |
|---------------------|---|

4.3.2 Programmatic Buying/Auction Mechanics

Disclosures under programmatic buying are yet to be finalized but may include items such as the auction type, inventory type, and whether the CPM floor is soft or dynamic.

Types of Auction

First Price Auction: A first-price auction is a form of auction where platform partners submit bids and the highest bid sets the market price, winning the auction. Platform partners pay the amount of the bid to the ad exchange with no price reduction.

Second Price Auction: A second-price auction is a form of auction where platform partners submit bids and the second highest bid sets the market price, but the highest bid wins the auction. Platform partners pay the amount of the second highest bid to the ad exchange. In some cases it is one cent over the second highest bid depending on the marketplace.

Modified Second Price Auction: A modified second-price auction is a form of auction where platform partners submit bids and the market price is set between the bid submitted and the second highest bid. Platform partner pays the market price to the ad exchange. The ad exchange determines the market price.

Optional Disclosures

Data: How data from a bid request will be used.

Floor: The presence of either a manual or dynamic mechanism within a platform for an inventory holder or marketplace steward to set their own clearance price. The disclosure may be one of: dynamic, manual, soft, or hard.

Inventory Categorization: The characteristics of the inventory being offered. The disclosure may be one of: toolbar, desktop, rotating creative, or other categorization that is described in the DOM or buyer-seller agreement.

5 Glossary of terms

A list of technical, administrative, and procedural terms used in this document

To demystify and prevent confusion, the following definitions provide a standard list of commonly used terms. Consistent standards ensure that all industry players are on the same page and working towards the same goals. Universal industry definitions are also a vital ingredient to moving online marketing forward and increasing its allocation in the marketing mix.

The behavioral definitions were developed in conjunction with the Behavioral Targeting Standards Consortium Advisory Board (www.BTStandards.org). The data definitions were developed in conjunction with the IAB's Data Usage and Control Taskforce.

Ad Click: The user activity of pressing a navigation button or hitting the enter key on the keyboard on an advertisement unit on a Web site (banner, button or text link). (See Click-through)

Ad Creative Pixel (See Pixel)

Ad Duration (Video): the maximum allowable duration of the video ad creative. Ad duration does not include user interaction with the ad. Any user interaction with the ad may increase its effective duration. Ad duration should be expressed as an integer value in seconds ar, if undefined, as "undefined."

Ad Exchange: Ad exchanges provide a sales channel to publishers and ad networks, as well as aggregated inventory to advertisers. They bring a technology platform that facilitates automated auction based pricing and buying in real-time. Ad exchanges' business models and practices may include features that are similar to those offered by ad networks. For the purposes of the IAB Networks & Exchanges Quality Assurance Guidelines, the definition of an ad exchange excludes technology platforms that only provide tools to enable direct media buying and selling between exchange participants.

Ad Network: Ad networks provide an outsourced sales capability for publishers and a means to aggregate inventory and audiences from numerous sources in a single buying opportunity for media buyers. Ad networks may provide specific technologies to enhance value to both publishers and advertisers, including unique targeting capabilities, creative generation, and optimization. Ad networks' business models and practices may include features that are similar to those offered by ad exchanges.

Ad Pod: a sequential grouping of one or more linear ads in digital in-stream video shown back-to-back.

Ad Pod Length: the number of distinct video ads (of any ad duration) that are shown back-to-back in an ad pod.

Ad Pod Position: the specific sequential designation of an ad within the pod (i.e. 1, 2, 3, etc.)

Ad Server: A computer application that enables the delivery, tracking and management of advertising content on publisher inventory.

Add to Cart: The user activity of storing merchandise in a virtual shopping cart that the user intends to later purchase from an online e-commerce website. This enables users to continue browsing and "check-out" later or alternately delete these items from the cart.

Advertiser Ad Tag: Software code that an advertiser provides to a publisher or ad network that calls the advertiser's ad server for the purposes of displaying an advertisement.

Advertising Banner (also called Ad Banner or Banner): A static graphical image (GIF or JPEG files) or interactive content (Flash files) used to display an advertising unit on a web site. Most banners enable users to click on ad to be redirected to another website.

Adware: Computer software provided to the user free of charge or at a discounted price that downloads and displays advertising to support its continued development and maintenance. This software often tracks what Internet sites the user visits.

Affiliate Conversion Data: Data that is collected by an affiliate marketing system when a user completes a transaction or manifests certain behaviors on a web page. The system typically collects this data by means of a conversion pixel that is placed on the merchant's site.

Affiliate Marketing: Affiliate Marketing is a method of generating leads or sales, whereby an online publisher is paid for referring users to an online e-commerce merchant. Referrals are measured by clicks, registrations or sales.

Aggregate Campaign Data: Data combined from several advertising campaigns to create a segment where campaign level data is not identifiable.

Agency: An organization that, on behalf of clients, plans marketing and advertising campaigns, drafts and produces advertisements, places advertisements in the media. In interactive advertising, agencies often use third party technology (ad servers) and may place advertisements with publishers, ad networks and other industry participants.

Attribute: A single piece of information known about a user and stored in a behavioral profile which may be used to match ad content to users. Attributes consist of demographic information (e.g., age, gender, geographical location), segment or cluster information (e.g., auto enthusiast), and retargeting information (e.g., visited Site X two days ago). Segment or cluster information is derived from the user's prior online activities (e.g., pages visited, content viewed, searches made and clicking and purchasing behaviors). Generally, this is anonymous data (non-PII).

Auction: An opportunity for an ad exchange to compete for and win an ad impression.

Audience Measurement: The counting of unique users (i.e. audience) and their interaction with online content. At a campaign level, this service is conducted by a third party to validate that a publisher delivered what an advertiser had requested. At the industry level, this service enables media buyers to understand which brokers of online content to negotiate with to reach a specific audience.

Audible Sound: Describes whether the video ad impression default volume is audible when the ad is being played. The minimum volume level for audible sound is 26%.

Authorized Advertiser Agent (AAA): Party that holds a direct legal relationship with a marketer or agency with the intent of buying inventory on their behalf or providing them a platform with which to do so. AAAs are considered indirect parties in the context of transaction types.

Authorized Publisher Agent (APA): Party that holds a direct legal relationship with a publisher or party who owns inventory with the intent of selling inventory on their behalf or providing them a platform with which to do so.

Auto Play: A video ad or animation that initiates "play" without explicit user interaction or without a user actively starting the video. If a user has a reasonable expectation that a video will play when clicking a link (for example, a small video icon appears next to the link), clicking the link is considered explicit user interaction and is not considered auto-play.

Bid: The maximum value a platform partner wishes to pay for an auction.

Bid request: A call to a platform partner's bid URL for an opportunity to compete in an auction.

Bid URL: The mechanism by which an ad exchange initiates bid requests to platform partners.

Beacon (See Pixel)

Behavioral Event: A user-initiated action which may include, but not limited to: searches, content views, clicks, purchases, form-based information and other interactions. Behavioral events are anonymous and do not include personally identifiable information (PII).

Business Visitor: A user that accesses online content in furtherance of their employment.

Buyer: the party that owns or represents advertisement to be placed on the seller's available media inventory

Click-through: The measurement of a user clicking on a link that re-directs the user's web-enabled device to another Web destination.

Clickstream Data: A Clickstream is the recording of what a computer user clicks on while web browsing. As the user clicks anywhere in the webpage or application, the action is logged on a client or inside the web server, as well as possibly the web browser and ad servers. Clickstream data analysis can be used to create a user profile that aids in understanding the types of people that visit a company's website, or predict whether a customer is likely to purchase from an e-commerce website.

Client-side call: An HTTP request made directly from a browser. A platform partner can read and set cookies for a client side call.

Content (Site/Page): Site content is the textual, visual or aural content is encountered as part of the user experience on a website. It may include, among other things: text, images, sounds, animations and videos. Web content is dominated by the "page" concept, with multiple pages of related content typically forming a site.

Content Delivery Network (alternately Content Distribution Network) (CDN): A service that hosts online assets and provides content management via servers located around the globe to reduce the latency of downloads to users.

Communication: The activity of conveying information by or to people or groups. Examples of online communication include email, instant messaging, text-messaging, group-messaging.

Connection Type (Mobile): The type of connection a mobile device is using to access the World Wide Web. Mobile connection types may include: 3G, 4G, wi-fi, or unconnected. Connection type

distinctions are important because some ads may require the highest connectivity rate (wi-fi) for large creative files or the ability to download files such as games or other apps. Knowing the connection type enables buyers to restrict ad delivery dependent on the connection type.

Conversion Pixel (See Pixel)

Conversion rate: The percentage of users who complete a desired action (e.g., purchase or registration) compared to all users who were exposed to an online ad.

Cookie: A small text file sent by a website's server to be stored on the user's web-enabled device that is returned unchanged by the user's device to the server on subsequent interactions. The cookie enables the website domain to associate data with that device and distinguish requests from different devices. Cookies often store behavioral information.

Cookie Matching: A method of enabling data appending by linking one company's user identifier to another company's user identifier.

Creative Retargeting: A method that enables advertisers to display information (typically an ad) specifically to visitors that previously were exposed to or interacted with the advertisers' creative.

Cross-site Publisher Analytics: Services that provide normative metrics about and estimates of multiple publishers' inventory.

Cross-site Advertiser Analytics: Software or services that allow an advertiser to optimize and audit the delivery of creative content on pre-bought publisher inventory. Data can range from numbers of pages visited, to content visited, to purchases made by a particular user. Such data is used to surmise future habits of user or best placement for a particular advertiser based on success.

Data: Any information collected.

Data Aggregator: An organization that collects and compiles data from individual sites to sell to others.

Data Append: User data from one source is linked to a user's profile from another source.

Data Segment: (See Segment)

Default Width & Height (Video Ads): The default height and width (expressed in pixels) of the video ad impression being rendered. The width and height measurement disclosures are subject to the following guidelines:

Width and height measurements may include persistent player controls (i.e. play/pause, mute and full screen buttons as well as countdown timers) and privacy compliance controls (i.e. Ad Choices icon). Persistent controls should make up no more than 10% of the ad viewing space.

Default width and height should be reported as the width and height the ad will be rendered prior to any user interactions. In general, with the exceptions noted above, the video ad viewing space should be free from viewability obstructions.

Demand Side Platform (also called DSP, buy side optimizers, and buy side platforms): Demand Side Platforms provide centralized (aggregated) media buying from multiple sources including ad exchanges, ad networks and sell side platforms, often leveraging real time bidding capabilities of said sources. While there is some similarity between a DSP and an ad network, DSP's are differentiated

from ad networks in that they do not provide standard campaign management services, publisher services nor direct publisher relationships.

Desktop Application: Software that is installed on a computer.

Deep Packet Inspection: A form of computer network packet filtering that examines the data and/or header part of a packet as it passes an inspection point. In the context of online advertising, it is used to collect data, typically through an Internet Service Provider, which can be used to display targeted advertising to users based on previous web activity.

Dynamic bidding: Platform partner assigns a unique bid to each auction opportunity and populates that bid in every bid response.

First price auction: A form of Auction where Platform Partners submit bids and the highest bid sets the Market Price, winning the Auction. Platform Partner pays the amount of his bid to the Ad Exchange with no price reduction.

Floors: In programmatic ad buying and selling, either a manual or dynamic mechanism within a bidding platform for an inventory holder or marketplace steward to set their own clearance price.

Frequency Capping: The limit of how many times a given ad will be shown to a unique cookie during a session or within a specified time period.

Hit: The record of a single online transaction event stored in a log file. One page view may contain multiple hits, one for each image on a web page.

Home Visitor: A user that access online content from their residence.

Impression (also called a View): A single display of online content to a user's web-enabled device. Many websites sell advertising space by the number of impressions displayed to users. An online advertisement impression is a single appearance of an advertisement on a web page. Each time an advertisement loads onto a user's screen, the ad server may count that loading as one impression. However, the ad server may be programmed to exclude from the count certain non-qualifying activity such as a reload, internal user actions, and other events that the advertiser and ad serving company agreed to not count.

In-application (in-app) advertising: Advertisement served within a native application environment on a mobile device, either Smartphone or tablet. Typically, these apps are downloaded from an app store such as iTunes, Google Play, Amazon Market, Windows Apps Store, Blackberry's App World, Facebook apps store, and other distribution points. (Examples: Angry Birds iPhone app; Pandora Android app).

Incentivized View: An ad impression that offers the user some incentive other than content in exchange for watching the ad. Examples of incentives may include, loyalty points, coupons, sweepstakes entries, e-currency and gaming status.

Intended Transaction: a transaction between buyer and seller for an ad placement or impression in accordance with agreed upon specifications and representations. Any transaction that happens outside of the agreed upon specifications and representations are transactions that are unintended. For example, if a Buyer specifies that it only wishes to purchase inventory from a QAG-compliant Seller, and the Seller represents that its inventory is QAG-compliant, any transactions between them that involve inventory that is noncompliant with QAG is an unintended transaction.

Internet Service Provider (ISP) (also called Online Service Provider): A company that enables its customers to access the Internet.

Inventory: The aggregate number of opportunities near publisher content to display advertisement to visitors.

Linear In-Stream Video Ads: video ads shown before, during, or after streaming content. Linear in-stream ads take over the user experience for a period of time and are played within the context of video content. Linear ads can include both VAST and VPAID creative types. The following descriptors should be used for linear in-stream ad types:

- **Pre-roll** – plays appears before the video content plays.
- **Mid-roll** – plays during a break somewhere in the middle of the video content.
- **Post-roll** – plays after the video content completes.

Link (short for Hyperlink): A text of graphical portion of a webpage that, when selected, redirects the user's web-enabled device to another webpage.

Market Price: The value of the placement after the auction.

Metadata: Data that provides information about other data. This includes descriptions of the characteristics of information, such as quality, origin, context, content and structure.

Mobile web: Advertisement served within a site optimized for the mobile experience, either from an internet-enabled smartphone or tablet. Mobile sites are frequently referred to as "m-dot" sites, mobile-specific URLs that users typically access from a mobile browser. (Examples: <http://mobile.example.com>, <http://m.example.com>, <http://example.com/mobile>.) Mobile web advertising also includes advertising on a browser-based site that is adaptive or responsively designed when viewed on mobile devices. Mobile web advertising also includes advertising served within a desktop web site that is visited via a mobile browser. This is a use-case that is generally undesirable from advertising perspective, detail on this below.

Modified second price auction: A form of Auction where Platform Partners submit bids and the Market Price is set between the bid submitted and the second highest bid. Platform Partner pays the Market Price to the Ad Exchange. The Ad Exchange determines the Market Price.

Multi-site company: A single entity that owns and operates multiple web sites, each under a separate domain.

Nonlinear In-Stream Ads: an image ad that displays concurrently with video content, most commonly as an "overlay," overlaying the video content, but may also play within the video player but in a manner that does not obstruct the video content (non-overlay). Sellers should disclose, if known, whether accepted nonlinear ads allow for rich media expanding and interaction.

Non-Session data (also called out-of-session data): information that cannot be gleaned from the current, single event of a visitor.

Online Publisher: A creator and/or aggregator of online content, which often monetizes user visits by displaying advertisements.

Out-of-session data: (See Non-Session data)

Pass Back: an impression offered to a media buyer with the right of first refusal, such that when this right is exercised the impression is offered to another media buyer.

Personalization: Aggregating previous online activity to match non-ad related information to users.

Personalization Service: Software or service that enables websites to match non-ad related information to user.

Personally Identifiable Information (PII): User data that could be used to uniquely identify the consumer. Examples include name, social security number, postal address, and email address.

Piggyback Pixel (See Pixel)

Pixel (also called Beacon or Web Beacon): An HTML object or code that transmits information to a third-party server, where the user is the first party and the site they are interacting with is the second party. Pixels are used to track online user activity, such as viewing a particular web page or completing a conversion process. See Ad Creative Pixel, Conversion Pixel, Publisher Pixel.

Ad Creative Pixel: A pixel request embedded in an ad tag which calls a web server for the purpose of tracking that a user has viewed a particular ad.

Conversion Pixel: An image tag or code that transmits to a third-party server that a user has successfully completed a process (such as purchase or registration).

Piggyback Pixel: An image tag or code that redirects a user browser to another pixel not directly placed on the publisher page.

Platform Partner: A technology stack capable of integrating with an ad exchange using an API real-time bidder (RTB).

Profile: Profile is the collection of attributes describing segments, clusters or aggregated data, including prior online activity of a user.

Profile Aggregator: A profile aggregator collects data from various third-party sources to generate behavioral profiles.

Profile Database: Profile Database a server-side store of behavioral profiles.

Publisher Pixel: An object embedded in a web page (typically a 1x1 image pixel) that calls a web server for purposes of tracking some kind of user activity.

Publisher Ad Tag: Code that is placed on a publisher's web page that calls an ad server for the purposes of displaying an advertisement.

Purchase: The user activity of completing an e-commerce transaction.

QPS: Queries per second. Number of times ad exchange or platform partner will be initiating requests to the other. Knowing the QPS is important for infrastructure planning.

Query String: Meta data appended to an HTTP "GET" request url.

Referring URL: The address of the webpage that a user previously visited prior to following a link.

Registration: The user activity of subscribing to a website or requesting additional information by filling in personally-identifying contact details.

Retargeting (or re-targeting): The use of a pixel tag or other code to enable a third-party to recognize particular users outside of the domain from which the activity was collected. See Creative Retargeting, Site Retargeting.

Really Simple Syndication (RSS): Metadata about content that enables a website to distribute new content with identical metadata to a subscriber of this feed.

RSS Reader: Software or website that aggregates syndicated content (e.g., news headlines, blogs, and podcasts) into a single location for easy viewing.

Run of Exchange (ROE): No targeting overlays. All traffic on the exchange is exposed.

Screen Scraping: A way of collecting information from a web page, whereby a remote computer program copies information from a website that is designed to display information to a user.

Search: The act of entering a query at a search engine by entering in a series of keywords describing their desired content.

Search Click: A click originating from a list of links returned by a query to a search engine.

Search Engine: A website that provides a searchable index of online content, whereby users enter keywords describing what they are seeking and the website returns links related to this search query.

Second price auction: A form of Auction where Platform Partners submit bids and the second highest bid sets the Market Price, but the highest Bid wins the Auction. Platform Partner pays the amount of the second highest bid to the Ad Exchange. In some cases it is one cent over the second bid depending on the marketplace.

Segment: Also called "data segment" or "audience," a segment is a set of users who share one or more similar attributes.

Seller: the party that makes media available to another party for purchase.

Sell Side Platform (also called sell side optimizers, inventory aggregators, and yield optimizers) – Sell Side Platforms provide outsourced media selling and ad network management services for publishers. Sell-side platform and ad networks business models and practices are similar. Sell-side platforms are typically differentiated from ad networks in not providing services for advertisers. Demand Side Platforms and Ad Networks often buy from Sell Side Platforms.

Server Side Call: An HTTP request made from a server. A platform partner cannot read or set cookies in a server-side call.

Single-site Publisher Ad Server: Single-site Publisher Ad Servers focus on maximizing the yield to the publisher.

Single-site Publisher Analytics: Software or services that analyze information about users, including metrics such as unique visitors and site usage. The collected data is used only on behalf of the site from which the data is collected.

Site/Page/Position Transparency: Ability for the buyer of media (typically an advertisement) to understand the location and context within which the media will be displayed. Transparency can be at the level of web property (site), page content (page) or position (specific location within page). Site transparency, in the context of a network or an exchange, refers to the ability of a buyer of inventory to know the exact identity of the website domain or page on which they have shown advertisements.

Skippable: Skippable creatives are linear in-stream creatives that users can choose to skip, typically after a prescribed number of seconds have passed.

Spyware: Computer software that is installed surreptitiously to intercept or take partial control over the user's interaction with a computer, without the user's informed consent. Spyware programs can collect various types of information, such as Internet surfing habits, but can also interfere with user control of the computer in other ways, such as installing additional software, and redirecting web browser activity. The software usually does not contain generally accepted standards of notice describing what the purpose and/or behavior of the software is nor does it usually contain visible or functioning choice mechanisms for complete uninstall. The programs are typically characterized by behaviors that can be considered deceptive if not harmful to the user and/or his computer.

Static bidding (Flat CPM): Platform partner pre-negotiates bids via offline process for segments of inventory. Buyer bids for inventory at a flat CPM rate.

Targeted Advertisement: an advertisement that is shown only to users exhibiting specific attributes or in a specific context or at a particular time of day.

Transaction: Transaction is defined as the execution of any form of trade (cash, barter, etc.) between a buyer and seller that results in the exposure of advertising on media

User Syncing: The process of exchanging cookie data between an ad exchange and platform partner so that platform partner's cookie data is available for decision-making during the RTB process.

Video context: Context of video content with which the video ad will be shown or "unknown" if not known. The contextual taxonomy defined by the network and exchanges quality assurance guidelines shall be used for this parameter.

Viewability Obstructions: Any item within the video ad viewing space other than persistent player controls (e.g. play/pause, mute, skip ad) or privacy compliance notifications (e.g. AdChoices icon) which masks or obstructs the video viewing experience. For example, a 30x50 pixel publisher logo box overlay that obstructs the content viewing space of an ad during playback is a Viewability Obstruction.

Web App Advertising: Advertising served into an application that is browser-based but may be wrapped within native mobile device code. Web apps are typically accessed using an online or mobile site and then reside as a 'widget' on phone or tablet-top.

Mobile Video Advertising: Video advertising in which ads are served within an application, or mobile web environment. Despite the platform, mobile video has unique characteristics including "skippability," overlays that are clickable or not, force view {}.

6 Appendix

The following exhibits offer sample letters of attestation to be delivered to the IAB for QAG 2.0 certification and renewal.

Exhibit A: Compliance Officer Attestation

Exhibit B: Executive Attestation

Exhibit C: Independent Validation Attestation

Exhibit A: Compliance Officer Attestation IAB Quality Assurance Guideline 2.0

I, _____ (name of Compliance Officer), attest that:

1. I have conducted quarterly internal audits for _____ (name of Company) for _____ quarter(s) and year _____;
2. The executive named in the Executive Attestation and I are responsible for following the procedures outlined in the IAB Quality Assurance Guidelines 2.0:
 - a. Acquiring Inventory: accurately label inventory in accordance with established content framework along 3 criteria:
 - i. Transaction Party Source Identification and Relationships (section 4.1.1)
 - ii. Source Level Transparency (section 4.1.2)
 - iii. Technical Context (section 4.1.3)
 - b. Contextual Taxonomy (section 4.2.2) & Targeting (section 4.2.7): accurately categorize content in accordance with Tiers 1 & 2 of IAB Contextual Taxonomy, and specify the depth (e.g. site level vs. page level) of categorization
 - i. If we have chosen to use a different taxonomy, we can clearly map our taxonomy back to the IAB taxonomy and explain to a buyer with sufficient detail
 - c. Inventory Vetting: accurately label content in accordance with established guidelines in accordance with sections 4.2.3, 4.2.4, 4.2.5, and 4.2.6; and
 - d. Data Disclosure: accurately disclosed to publisher partners who are contributing data and to advertisers when using third party data (section 4.31)
3. Based on my knowledge and best efforts, _____ (name of Company) is in compliance with the IAB Quality Assurance Guidelines 2.0; and
1. I agree to allow the IAB to publically disclose _____ (name of Company) compliance with the IAB Quality Assurance Guidelines 2.0 at the following certification status, providing all required materials are submitted in accordance with section 2.3 (or 2.4 for renewal):
 - QAG 2.0 Self-Certification
 - QAG 2.0 Independent Validation
 And in the case of loss of certification, I agree to allow the IAB to remove _____ (name of Company) certification status from published list of certified companies.

Signature:

Date:

Name:

Title:

Exhibit B: Executive Attestation IAB Quality Assurance Guideline 2.0

I, _____ (name of CEO, CFO, or business unit head), attest that:

2. I have reviewed quarterly internal audits _____ (name of Company) for _____ quarter(s) and year _____;
3. The Compliance Officer and I are responsible for following the procedures outlined in the IAB Quality Assurance Guidelines 2.0:
 - a. Acquiring Inventory: accurately label inventory in accordance with established content framework along 3 criteria:
 - i. Transaction Party Source Identification and Relationships (section 4.1.1)
 - ii. Source Level Transparency (section 4.1.2)
 - iii. Technical Context (section 4.1.3)
 - b. Contextual Taxonomy (section 4.2.2) & Targeting (section 4.2.7): accurately categorize content in accordance with Tiers 1 & 2 of IAB Contextual Taxonomy, and specify the depth (e.g. site level vs. page level) of categorization
 - i. If we have chosen to use a different taxonomy, we can clearly map our taxonomy back to the IAB taxonomy and explain to a buyer with sufficient detail
 - c. Inventory Vetting: accurately label content in accordance with established guidelines in accordance with sections 4.2.3, 4.2.4, 4.2.5, and 4.2.6; and
 - d. Data Disclosure: accurately disclosed to publisher partners who are contributing data and to advertisers when using third party data (section 4.31)
4. Based on my knowledge and best efforts, _____ (name of Company) is in compliance with the IAB Quality Assurance Guidelines 2.0; and
5. I agree to allow the IAB to publically disclose _____ (name of Company) compliance with the IAB Quality Assurance Guidelines 2.0 at the following certification status, providing all required materials are submitted in accordance with section 2.3 (or 2.4 for renewal):
 - QAG 2.0 Self-Certification
 - QAG 2.0 Independent Validation

And in the case of loss of certification, I agree to allow the IAB to remove _____ (name of Company) certification status from published list of certified companies.

Signature:

Date:

Name:

Title:

Exhibit C: Sample Independent Validation Attestation IAB Quality Assurance Guideline 2.0

I, _____ (name of representative from independent validation company),
 _____ (representative title) at _____ (name of independent
 validation company) attest that:

1. I have reviewed quarterly internal audits _____ (name of Company) for
 _____ quarter(s) and year _____;
2. The named Compliance Officer and Executive named in the Compliance Officer
 Attestation and Executive attestation, respectively, have facilitated my efforts to
 validate that the following the procedures outlined in the IAB Quality Assurance
 Guidelines 2.0:
 - a. Acquiring Inventory: accurately label inventory in accordance with
 established content framework along 3 criteria:
 - i. Transaction Party Source Identification and Relationships (section
 4.1.1)
 - ii. Source Level Transparency (section 4.1.2)
 - iii. Technical Context (section 4.1.3)
 - b. Contextual Taxonomy (section 4.2.2) & Targeting (section 4.2.7):
 accurately categorize content in accordance with Tiers 1 & 2 of IAB
 Contextual Taxonomy, and specify the depth (e.g. site level vs. page
 level) of categorization
 - i. If we have chosen to use a different taxonomy, we can clearly
 map our taxonomy back to the IAB taxonomy and explain to a
 buyer with sufficient detail
 - c. Inventory Vetting: accurately label content in accordance with established
 guidelines in accordance with sections 4.2.3, 4.2.4, 4.2.5, and 4.2.6; and
 - d. Data Disclosure: accurately disclosed to publisher partners who are
 contributing data and to advertisers when using third party data (section
 4.31)
3. Based on my knowledge and best efforts, _____ (name of
 Company) is in compliance with the IAB Quality Assurance Guidelines 2.0 and
 qualifies for QAG 2.0 Independent Validation, providing all required materials are
 submitted in accordance with section 2.3 (or 2.4 for renewal).

Date:

Signature:

Name:

Company:

Title:





Leading the Marketing Community



**STATEMENT OF BEST PRACTICES
TO ADDRESS ONLINE PIRACY AND COUNTERFEITING**

The Association of National Advertisers (ANA) and the American Association of Advertising Agencies (4A's) strongly believe that U.S. advertisers must have confidence that their ads are not unintentionally providing financial support to, or otherwise legitimizing, "rogue" Internet sites whose primary and apparent purpose is to steal or facilitate theft of the intellectual property of America's innovators and creators. U.S. advertisers must also have confidence that their corporate brands and images are not being harmed by association with such unlawful activity. In order to help address this complex problem, our Associations believe that our members should each commit to take affirmative steps to avoid placement of their ads on such sites.

At the outset, we emphasize that this commitment is not intended to foreclose advertising on legitimate social media or user-generated content sites, even if infringing content occasionally appears on such sites. Rather, this commitment addresses "rogue" sites that are dedicated to infringement of the intellectual property rights of others, in that they have no significant, or only limited, use or purpose other than engaging in, enabling or facilitating such infringement. It is understood that in most instances such sites will initially – but not conclusively -- be identified by intellectual property owners. With respect to such sites, marketers and their agencies should seek to include conditions along the following lines in media placement contracts and insertion orders with ad networks and other intermediaries involved in their U.S.-originated digital advertising campaigns on both domestic and foreign Internet sites:

- (i) All such intermediaries shall use commercially reasonable measures to prevent ads from being placed on such sites;
- (ii) All such intermediaries shall have and implement commercially reasonable processes for removing or excluding such sites from their services, and for expeditiously terminating non-compliant ad placements, in response to reasonable and sufficiently detailed complaints or notices from rights holders and advertisers;
- (iii) All such intermediaries shall refund or credit the advertiser for the fees, costs and/or value associated with non-compliant ad placements, or provide alternative remediation.

The above language is provided for illustrative purposes, and individual members may adopt policies, guidelines and provisions that result in similar obligations, including the relevant provisions of the IAB Standard Terms and Conditions for Internet Advertising.

We acknowledge that our members are asked to make this commitment in the context of a highly dynamic and complex digital advertising ecosystem, and that inadvertent non-compliant ad placements will occasionally occur. While we encourage our members to take appropriate steps to safeguard their brands, this commitment is not intended to impose a duty on marketers or the advertising intermediaries with which they transact to monitor their advertising to identify

"rogue" sites. Similarly, it is understood that knowledge gained in the course of implementing this voluntary commitment should not be used as the basis for any legal liability or loss of any applicable "safe harbor" from such liability.

At bottom, the critical point for ANA, the 4A's and our members is this: we should not knowingly allow our businesses and brands to supply financial life-blood or lend a veneer of legitimacy to fundamentally illicit business models that threaten the jobs of millions of Americans in the creative industries and, ultimately, our national economic welfare.



Internet Business Voluntary Best Practices and Agreements 2013

Marketplace solutions are an important aspect in protecting the country's vital IP industries³ that drive innovation. The development and adoption of voluntary best practices and agreements by legitimate Internet businesses to assure they are not benefitting from or facilitating illegal conduct by others online is a critical component of developing a robust and flexible response to the problem of content theft. The past few years have witnessed the development of a number of cooperative initiatives, including with the following intermediaries: Internet ad networks, advertisers and ad agencies; ISPs; payment processors; User Generated Content (UGC) services; and domain name registrars. Each of these groups has participated in a process to avoid profiting from illegal conduct. Similar best practices negotiated by search engines storage services, and those in the mobile space, with the IP community, are necessary. Below is a summary of the best practices developed so far:

UGC Principles (2007)

- These practices were established among multiple stakeholders to make the DMCA more effective for UGC sites in practice, to promote the promises and benefits of UGC services, and to protect the rights of copyright owners.

IAB Network and Exchanges Quality Assurance Guideline (2010, 2013)

- The Interactive Advertising Bureau (IAB) released recommended ad network and exchange guidelines (Quality Assurance Guidelines – QAG) in 2010 that provide policies to address the funding of theft on the Internet. These were updated in July, 2013. Among other things, the guidelines prohibit the sale of ad inventory on sites that engage in copyright infringement.

ISP Copyright Alert Program (2011)

- The five major ISPs (AT&T, Comcast, TimeWarner Cable, Verizon, and Cablevision,) the major movie studios and record labels, and their trade associations, reached agreement on a system for multi-step copyright alerts to be sent to ISP users in response to notices of p2p infringement by rights holders. The practices include:
 - Copyright education to consumers through a new consumer information center;
 - Technical validation; and
 - An independent review process for users to challenge alerts administered by the American Arbitration Association (AAA) utilizing a leading copyright lawyer as a technical expert.
- Does not require termination of Internet access, nor that an ISP impose a mitigation measure that would impair a user's essential services (VOIP, etc.)
- Provides for multiple notices and grace periods to give the user information and time to change behavior.
- Protects users' privacy.
- Administered by the Center for Copyright Information (CCI).
- Went live in Q1-2013.

³ According to a 2012 Administration report, "IP-intensive" industries directly account for 27 million American jobs, or 15% of total US employees. Those industries account for \$5 trillion in value added to the US economy, which is 35% of total GDP.

Payment Processors (2011)

- Visa, MasterCard, Amex, Discover and PayPal announced a series of best practices negotiated under the auspices of the Intellectual Property Enforcement Coordinator (IPEC).
- Participants agree to terminate their relationship with a website if the site persists in intentionally selling infringing/counterfeit products.
- Payment Processors have worked with IACC to develop mechanized secure and valid requests for ending affiliation with rogue sites.

Center for Copyright Information (2012)

- Part of the ISP Copyright Alert Program, above.
- Established to educate the public, advise on implementation, and analyze the impact of the program.
- Advisory board members include experts from the consumer advocate, copyright, ISP, and Internet education communities.

Online Advertisers (May 2012)

- The Association of National Advertisers (ANA) and the Associations of Advertising Agencies of America (4As) released best practices supported by the Interactive Advertising Bureau (IAB).
- Advises marketers to include language in their media placement contracts and insertion orders with ad networks to prevent their ads from appearing on 'rogue sites' dedicated to infringement of intellectual property rights of others, in that they have no significant, or only limited, use or purpose other than engaging in, enabling or facilitating such infringement.

Ad Network Best Practices (2013)

- The Office of the Intellectual Property Enforcement Coordinator (IPEC) facilitated recently announced Ad Network best practices to address sites that are principally dedicated to selling counterfeit goods or engaging in copyright piracy and have no substantial non-infringing uses.

Registrars/Registries/ICANN (2013)

- After input from stakeholders, ICANN passed a resolution that makes clear that registries and registrars should take action to prohibit new gTLD website operators from engaging in piracy, trademark or copyright infringement, or other fraudulent or deceptive practices, and to provide for consequences for such activity, including suspension of the domain name.
- Need to see what best practices may develop from this obligation.

What's Missing?

- Search Engines
- Storage Services
- Mobile Services

Let's get to work.

Principles for User Generated Content Services

Foster Innovation. Encourage Creativity. Thwart Infringement.

Related Releases

- [Yahoo! Joins Broad Coalition in Support of UGC Principles](#)
- [Several Artists Protest Content Patents and User Generated Video](#)
- [Sony Pictures Entertainment and Crackle Join Promoting User-Generated Content Coalition](#)
- [Internet and Media Industry Leaders Urge UGC Principles to Foster Online Innovation While Protecting Copyrights](#)

Translated Principles

- [Chinese](#)

The following companies support these principles:



CRACKLE

Dailymotion



Microsoft



seventload



SONY PICTURES

Leading commercial copyright owners ("Copyright Owners") and services providing user-uploaded and user-generated audio and video content ("UGC Services") have collaborated to establish these Principles to foster an online environment that promotes the promises and benefits of UGC Services and protects the rights of Copyright Owners. In this context, UGC Services are services such as Soapbox on MSN Video, MySpace, Dailymotion and Veoh.com, and not other technologies such as browsers, applets, email, or search services. While we may differ in our interpretation of relevant laws, we do not mean to resolve those differences in these Principles, which are not intended to be and should not be construed as a concession or waiver with respect to any legal or policy position or as creating any legally binding rights or obligations. We recognize that no system for deterring infringement is or will be perfect. But, given the development of new content identification and filtering technologies, we are united in the belief that the Principles set out below, taken as a whole, strike a balance that, on a going-forward basis, will result in a more robust, content-rich online experience for all.

In coming together around these Principles, Copyright Owners and UGC Services recognize that they share several important objectives: (1) the elimination of infringing content on UGC Services, (2) the encouragement of uploads of wholly original and authorized user-generated audio and video content, (3) the accommodation of fair use of copyrighted content on UGC Services, and (4) the protection of legitimate interests of user privacy. We believe that adhering to these Principles will help UGC Services and Copyright Owners achieve those objectives.

1. UGC Services should include in relevant and conspicuous places on their services information that promotes respect for intellectual property rights and discourages users from uploading infringing content.
2. During the upload process, UGC Services should prominently inform users that they may not upload infringing content and that, by uploading content, they affirm that such uploading complies with the UGC Service's terms of use. The terms of use for UGC Services should prohibit infringing uploads.
3. UGC Services should use effective content identification technology ("Identification Technology") with the goal of eliminating from their services all infringing user-uploaded audio and video content for which Copyright Owners have provided Reference Material (as described below). To that end and to the extent they have not already done so, by the end of 2007, UGC Services should fully implement commercially reasonable Identification Technology that is highly effective, in relation to other technologies commercially available at the time of implementation, in achieving the goal of eliminating infringing content. UGC Services should enhance or update the Identification Technology as commercially reasonable technology that makes a meaningful difference in achieving the goal becomes available.
4. If a Copyright Owner has provided: (1) the reference data for content required to establish a match with user-uploaded content, (2) instructions regarding how matches should be treated, and (3) representations made in good faith that it possesses the appropriate rights regarding the content (collectively, "Reference Material"), then the UGC Service should apply the Identification Technology to



that content to implement the Filtering Process described below. UGC Services should ensure that reasonable specifications, as well as any tools and/or technical support, for the delivery of Reference Material are made available to Copyright Owners. If a Copyright Owner does not include in the Reference Material instructions regarding how matches should be treated, the UGC Service should block content that matches the reference data.

- b. The Identification Technology should use Reference Material to identify user-uploaded content and should permit Copyright Owners to indicate how matches should be treated.
- c. If the Copyright Owner indicates in the applicable Reference Material that it wishes to block user-uploaded content that matches the reference data, the UGC Service should use the Identification Technology to block such matching content before that content would otherwise be made available on its service ("filtering"). UGC Services should permit Copyright Owners to indicate in the Reference Material that it wishes to exercise an alternative to blocking (such as allowing the content to be uploaded, licensing use of the content on other options), in which case, the UGC Service may follow those instructions or block the content, in its discretion.
- d. Copyright Owners and UGC Services should cooperate to ensure that the Identification Technology is implemented in a manner that effectively balances legitimate interests in (1) blocking infringing user-uploaded content, (2) allowing wholly original and authorized uploads, and (3) accommodating fair use.
- e. UGC Services should use the Identification Technology to block user-uploaded content that matches Reference Material regardless of whether the UGC Service has any licensing or other business relationship with the Copyright Owners who have provided such Reference Material (except that UGC Services may require that Copyright Owners enter into agreements with respect to the commercial use of their Reference Material, and that facilitate the provision of Reference Material by Copyright Owners and promote the goal of the elimination of infringing content). If a Copyright Owner authorizes specific users to upload content that would otherwise match Reference Material submitted by the Copyright Owner, the Copyright Owner should provide to the UGC Service a list of such users (a so-called "white list").
- f. UGC Services may, at their option, utilize manual (human) review of all user-uploaded audio and video content in lieu of, or in addition to, use of Identification Technology, if feasible and if such review is as effective as Identification Technology in achieving the goal of eliminating infringing content. If a UGC Service utilizes such manual review, it should do so without regard to whether it has any licensing or other business relationship with the Copyright Owners. Copyright Owners and UGC Services should cooperate to ensure that such manual review is implemented in a manner that effectively balances legitimate interests in (1) blocking infringing user-uploaded content, (2) allowing wholly original and authorized uploads, and (3) accommodating fair use.
- g. Copyright Owners should provide Reference Material only with respect to content for which they believe in good faith that they have the appropriate rights to do so, and should update rights information as reasonable to keep it accurate. The inclusion of reference data for content by, or at the direction of, a Copyright Owner should not constitute an implied representation of good faith that such Copyright Owner has the appropriate rights regarding such content. Copyright Owners should reasonably cooperate with UGC Services to avoid unduly stressing the Services' Identification Technology during limited periods when Copyright Owners, collectively, may be providing an overwhelmingly high volume of Reference Material. UGC Services should reasonably

11. UGC Services should use reasonable efforts to track infringing uploads of copyrighted content by the same user and should use such information in the reasonable implementation of a repeat infringer termination policy. UGC Services should use reasonable efforts to prevent a terminated user from uploading audio and/or video content following termination, such as blocking re-use of verified email addresses.
12. In engaging in the activities set forth in these Principles outside the United States, UGC Services and Copyright Owners should follow these Principles to the extent that doing so would not contravene the law of the applicable foreign jurisdiction.
13. Copyright Owners should not assert that adherence to these Principles, including efforts by UGC Services to locate or remove infringing content as provided by these Principles, or to replace content following receipt of an effective counter notification as provided in the Copyright Act, support disqualification from any limitation on direct or indirect liability relating to material online under the Copyright Act or substantively similar statutes of any applicable jurisdiction outside the United States.
14. If a UGC Service adheres to all of these Principles in good faith, the Copyright Owner should not assert a claim of copyright infringement against such UGC Service with respect to infringing user-uploaded content that might remain on the UGC Service despite such adherence to these Principles.
15. Copyright Owners and UGC Services should continue to cooperate with each other's reasonable efforts to create content-rich, infringement-free services. To that end, Copyright Owners and UGC Services should cooperate in the testing of new content identification technologies and should update these Principles as commercially reasonable, informed by advances in technology, the incorporation of new features, variations in patterns of infringing conduct, changes in users' online activities and other appropriate circumstances.

↑ **Top**

U.S. companies that offer "Ad Networks" in the U.S., as further defined below, are committed to maintaining high quality standards for advertisers and publishers and at the same time respecting intellectual property rights.

Ad Networks do not control the content on third-party websites and are not able to remove websites from the Internet. Nor can Ad Networks engage in extensive or definitive fact finding to determine a particular party's intellectual property rights. Nevertheless, we believe it is useful for Ad Networks to maintain policies intended to discourage or prevent, to the extent possible, websites that are principally dedicated to selling counterfeit goods or engaging in copyright piracy and have no substantial non-infringing uses from participating in the Ad Network. The signatories to this Statement have individually decided to adopt these voluntary best practices in furtherance of that goal.

Each signatory will independently maintain internal procedures designed to implement these practices. This is an important step toward maintaining a healthy Internet and promoting innovation and protecting intellectual property. These efforts should be undertaken in a manner that is consistent with all applicable laws and the balance of copyright interests, including fair use, and that respects privacy, free speech, and fair process.

The sale of counterfeit goods and copyright piracy are issues Ad Networks take seriously, and Ad Networks have policies and practices in place to address this problem. Rights holders are in the best position to identify and evaluate infringement of their intellectual property. Therefore, the Ad Networks agree that without specific, reliable notices from rights holders, Ad Networks lack the knowledge and capability to identify and address infringement. Accordingly, intellectual property holders are expected to be accurate in demonstrating infringement of their copyrights and trademark rights and to target only infringing conduct. We believe that policies for Ad Networks should reflect best practices that encourage and supplement, not replace, responsible and direct independent actions taken by intellectual property owners to enforce their intellectual property rights.

To reflect these important principles, Ad Networks will voluntarily seek to observe the following best practices:

General Commitment:

(a) Maintain policies prohibiting websites that are principally dedicated to selling counterfeit goods or engaging in copyright piracy and have no substantial non-infringing uses from participating in the Ad Network's advertising programs and post such policies on the Ad Network's website;

- (b) Maintain and post these best practices guidelines on the Ad Network's website;
- (c) Ad Network policies will include language indicating that websites should not engage in violations of law;
- (d) Participate in an ongoing dialogue with content creators, rights holders, consumer organizations, and free speech advocates.

Identification and Verification Process:

- (e) Agree to (i) be certified against the Interactive Advertising Bureau (IAB) Networks and Exchanges Quality Assurance Guidelines, or (ii) maintain an independent quality assurance vetting and auditing process; and work to support such measures across industry;

Complaint Process:

- (f) Accept and process valid, reasonable, and sufficiently detailed notices from rights holders or their designated agents regarding websites participating in the Ad Network alleged to be principally dedicated to selling counterfeit goods or engaging in copyright piracy and to have no substantial non-infringing uses. To enable Ad Networks to respond most effectively, such notices should provide information outlined in Exhibit A attached;
- (g) Publicly post on the Ad Network's website the contact information for its designated agent for receiving such notices from rights holders or their designated agents;
- (h) Upon receipt of a valid notice, perform an appropriate investigation into the complaint, including a determination of whether the website has a direct contractual relationship with the Ad Network. An Ad Network may take steps including but not limited to requesting that the website no longer sell counterfeit goods or engage in copyright piracy, ceasing to place advertisements on that website (or pages within that website) until it is verified that the website (or pages within the website) is no longer selling counterfeit goods or engaging in copyright piracy, or removing the website from the Ad Network; and
- (i) Upon receipt of a valid notice, Ad Networks may consider any credible evidence provided by the accused website that it is not principally dedicated to selling counterfeit goods or engaging in copyright piracy or has substantial non-infringing uses. Such credible evidence may take the form of a counter-notice containing the elements set forth in 17 U.S.C. § 512(g)(3). In addition, Ad Networks may also consider any response by the rights holder to credible evidence provided by the accused website in defense of its conduct.

The policies and procedures of any individual Ad Network will be independently designed to achieve reasonable mechanisms to help prevent the participation of websites that are principally dedicated to selling counterfeit goods or engaging in copyright piracy and have no substantial non-infringing uses in each Ad Network's advertising programs based on the unique aspects and experience of each Ad Network. This Statement is not intended to impose a duty on any Ad Network to monitor its network to identify such websites. Similarly, it is understood that the voluntary best practices reflected in this Statement should not, and cannot, be used in any way as the basis for any legal liability or the loss of any applicable immunity or "safe harbor" from such liability.

The term "Ad Networks" encompasses only services whose primary business is to broker for compensation the placement of website display advertisements and does not include services which are ad-serving platforms or ad exchanges.

Exhibit A – Notice

The exact form and structure of Notice may vary somewhat by Ad Network; however, generally, a notice must include, at minimum, the information listed below, and should be sent to the Ad Network's Designated Agent for such notices.

(a) A description of the alleged sale of counterfeit goods and/or copyright piracy (the "Illegitimate Activity") that includes (i) the specific URLs where the alleged Illegitimate Activity occurs; (ii) the identity, location and contact information for the participating website allegedly engaged in Illegitimate Activity. If only certain items or materials on a website are alleged to be illegitimate, the Notice must clearly identify those specific products or materials and their location on the website.

(b) Evidence (i) of the Illegitimate Activity, by providing, for example, a recent time-and-date-stamped screenshot of the page containing both the Illegitimate Activity and advertising from the Ad Network and (ii) that the advertising appearing on the participating website containing the Illegitimate Activity is provided by the Ad Network. This can be done by providing, for example, a Tamper Data trace and relevant screenshots showing that the participating website is making ad calls to the Ad Network for the advertising reflected in the screenshots.

(c) A copy of the rights holder's notice provided to the website under 17 U.S.C. §

512 or the cease & desist letter related to the Illegitimate Activity provided to the website, along with responsive communications or a description of action undertaken by the website;

(d) A statement under penalty of perjury that the person submitting the notice has a good faith belief that the Illegitimate Activity is not authorized by the rights holder, its agent, or the law; that the information and materials provided to the Ad Network are accurate; that the person submitting the notice owns the copyright or trademark for the products or materials that are the subject of the notice (in the case of trademark, including evidence of a federal trademark registration from the United States Patent and Trademark Office for the product or materials that are the subject of the notice) and, if not the owner, that the person is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed;

(e) Information reasonably sufficient to permit the Ad Network to contact the rights holder, such as an address, telephone number, and an e-mail address.

(f) Physical or electronic signature of a person authorized to act on behalf of the rights holder.

FIRST AMENDMENT TO MEMORANDUM OF UNDERSTANDING

THIS FIRST AMENDMENT TO MEMORANDUM OF UNDERSTANDING (this "*Amendment*"), dated as of August 25, 2011, is entered into by and among the parties listed as signatories hereto (the "*Parties*").

WHEREAS, the Parties wish to amend that certain Memorandum of Understanding dated July 6, 2011, by and among the Parties hereto (the "*MOU*"), to (i) extend the deadline for establishing the Center for Copyright Information ("*CCI*") from sixty (60) days after the effective date of the MOU to September 23, 2011 and (ii) delete the first sentence of Attachment D to the MOU;

WHEREAS, Section 10(C) of the MOU provides that the Parties may amend the MOU by a written agreement signed by all parties thereto; and

WHEREAS, in accordance with such Section 10(C) of the MOU, the Parties have executed and delivered this Amendment;

NOW, THEREFORE, in consideration of the premises and the mutual promises hereinafter set forth, the Parties agree as follows:

1. The beginning of the first sentence of Section 2(A) of the MOU is hereby amended to delete the phrase, "Not later than sixty (60) days after the Effective Date (as defined in Section 8(A) below)," and insert the phrase, "Not later than September 23, 2011," in place thereof.

2. The first sentence of Attachment D to the MOU (*i.e.*, "The MPAA member companies' affiliates are entities under the control of an MPAA member company.") is hereby deleted in its entirety.

3. This Amendment, when signed and delivered by each of the Parties, shall be effective as to all of the Parties as of the date first above written. This Amendment may be amended only in accordance with the provisions of the MOU, as amended by this Amendment and as further amended from time to time.

4. As amended by this Amendment, the MOU shall continue in full force and effect in accordance with its terms.

5. This Amendment may be executed in any number of counterparts, each of which shall be deemed an original, but all of which taken together shall constitute one and the same instrument. Any of the Parties hereto may execute this Amendment by signing any such counterpart.

6. This Amendment shall be governed by, and construed and enforced in accordance with, the substantive laws of the State of New York, without regard to its principles of conflicts of laws.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK.]

IN WITNESS WHEREOF, this First Amendment to Memorandum of Understanding has been executed and delivered as of the date first above written.

SIGNATORIES:

The Motion Picture Association of America, Inc.

By: _____
Name: _____
Title: _____

The Recording Industry Association of America, Inc.

By: Steven M. Ware
Name: Steven M. Ware
Title: EVP & General Counsel

Walt Disney Studios Motion Pictures

By: _____
Name: _____
Title: _____

Paramount Pictures Corporation

By: _____
Name: _____
Title: _____

Sony Pictures Entertainment Inc.

By: _____
Name: _____
Title: _____

Twentieth Century Fox Film Corporation

By: _____
Name: _____
Title: _____

Universal City Studios LLC

By: _____
Name: _____
Title: _____

IN WITNESS WHEREOF, this First Amendment to Memorandum of Understanding has been executed and delivered as of the date first above written.

SIGNATORIES:

The Motion Picture Association of America, Inc.

By: _____
Name: _____
Title: _____

The Recording Industry Association of America, Inc.

By: _____
Name: _____
Title: _____

Walt Disney Studios Motion Pictures

By: 
Name: ALAN BRAVERMAN
Title: EXEC V-P & GENERAL COUNSEL

Paramount Pictures Corporation

By: _____
Name: _____
Title: _____

Sony Pictures Entertainment Inc.

By: _____
Name: _____
Title: _____

Twentieth Century Fox Film Corporation

By: _____
Name: _____
Title: _____

Universal City Studios LLC

By: _____
Name: _____
Title: _____

IN WITNESS WHEREOF, this First Amendment to Memorandum of Understanding has been executed and delivered as of the date first above written.

SIGNATORIES:

The Motion Picture Association of America, Inc.

By: _____
Name: _____
Title: _____

The Recording Industry Association of America, Inc.

By: _____
Name: _____
Title: _____

Walt Disney Studios Motion Pictures

By: _____
Name: _____
Title: _____

Paramount Pictures Corporation

By: *[Signature]* _____
Name: _____
Title: _____

Sony Pictures Entertainment Inc.

By: _____
Name: _____
Title: _____

Twentieth Century Fox Film Corporation

By: _____
Name: _____
Title: _____

Universal City Studios LLC

By: _____
Name: _____
Title: _____

IN WITNESS WHEREOF, this First Amendment to Memorandum of Understanding has been executed and delivered as of the date first above written.

SIGNATORIES:

The Motion Picture Association of America, Inc.

By: _____
Name: _____
Title: _____

The Recording Industry Association of America, Inc.

By: _____
Name: _____
Title: _____

Walt Disney Studios Motion Pictures

By: _____
Name: _____
Title: _____

Paramount Pictures Corporation

By: _____
Name: _____
Title: _____

Sony Pictures Entertainment Inc.

By:  _____
Name: _____
Title: _____

Twentieth Century Fox Film Corporation

By: _____
Name: _____
Title: _____

Universal City Studios LLC

By: _____
Name: _____
Title: _____



IN WITNESS WHEREOF, this First Amendment to Memorandum of Understanding has been executed and delivered as of the date first above written.

SIGNATORIES:

The Motion Picture Association of America, Inc.

By: _____
Name: _____
Title: _____

The Recording Industry Association of America, Inc.

By: _____
Name: _____
Title: _____

Walt Disney Studios Motion Pictures

By: _____
Name: _____
Title: _____

Paramount Pictures Corporation

By: _____
Name: _____
Title: _____

Sony Pictures Entertainment Inc.

By: _____
Name: _____
Title: _____

Twentieth Century Fox Film Corporation

By: *Ronald C. Wheeler*
Name: *Ronald C. Wheeler*
Title: *Assistant Secretary*

Universal City Studios LLC

By: _____
Name: _____
Title: _____

IN WITNESS WHEREOF, this First Amendment to Memorandum of Understanding has been executed and delivered as of the date first above written.

SIGNATORIES:

The Motion Picture Association of America, Inc.

By: _____
Name: _____
Title: _____

The Recording Industry Association of America, Inc.

By: _____
Name: _____
Title: _____

Walt Disney Studios Motion Pictures

By: _____
Name: _____
Title: _____

Paramount Pictures Corporation

By: _____
Name: _____
Title: _____

Sony Pictures Entertainment Inc.

By: _____
Name: _____
Title: _____

Twentieth Century Fox Film Corporation

By: _____
Name: _____
Title: _____

Universal City Studios LLC

By: *[Signature]*
Name: *Richard Cotton*
Title: *CVP and General Counsel*

Warner Bros. Entertainment Inc.

By: 
Name: John Rogovin
Title: VP & General Counsel

UMG Recordings, Inc.

By: _____
Name: _____
Title: _____

Warner Music Group

By: _____
Name: _____
Title: _____

Sony Music Entertainment

By: _____
Name: _____
Title: _____

EMI Music North America

By: _____
Name: _____
Title: _____

SBC Internet Services, Inc., BellSouth Telecommunications, Inc., Southwestern Bell Telephone Company, Pacific Bell Telephone Company, Illinois Bell Telephone Company, Indiana Bell Telephone Company, Incorporated, Michigan Bell Telephone Company, Nevada Bell Telephone Company, The Ohio Bell Telephone Company, Wisconsin Bell, Inc., The Southern New England Telephone Company, and BellSouth Telecommunications, Inc. (the AT&T Inc. companies)

By: _____
Name: _____
Title: _____

Warner Bros. Entertainment Inc.

By: _____
Name: _____
Title: _____

UMG Recordings, Inc.

By: 
Name: **Jeffrey S. Harleston**
Title: **General Counsel, Executive Vice President N. America**

Warner Music Group

By: _____
Name: _____
Title: _____

Sony Music Entertainment

By: _____
Name: _____
Title: _____

EMI Music North America

By: _____
Name: _____
Title: _____

SBC Internet Services, Inc., BellSouth Telecommunications, Inc., Southwestern Bell Telephone Company, Pacific Bell Telephone Company, Illinois Bell Telephone Company, Indiana Bell Telephone Company, Incorporated, Michigan Bell Telephone Company, Nevada Bell Telephone Company, The Ohio Bell Telephone Company, Wisconsin Bell, Inc., The Southern New England Telephone Company, and BellSouth Telecommunications, Inc. (the AT&T Inc. companies)

By: _____
Name: _____
Title: _____

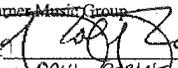
Warner Bros. Entertainment Inc.

By: _____
Name: _____
Title: _____

UMG Recordings, Inc.

By: _____
Name: _____
Title: _____

Warner Music Group

By:  _____
Name: PAUL ROBINSON
Title: EVP-GENERAL COUNSEL

Sony Music Entertainment

By: _____
Name: _____
Title: _____

EMI Music North America

By: _____
Name: _____
Title: _____

SBC Internet Services, Inc., BellSouth Telecommunications, Inc., Southwestern Bell Telephone Company, Pacific Bell Telephone Company, Illinois Bell Telephone Company, Indiana Bell Telephone Company, Incorporated, Michigan Bell Telephone Company, Nevada Bell Telephone Company, The Ohio Bell Telephone Company, Wisconsin Bell, Inc., The Southern New England Telephone Company, and BellSouth Telecommunications, Inc. (the AT&T Inc. companies)

By: _____
Name: _____
Title: _____

Warner Bros. Entertainment Inc.

By: _____
Name: _____
Title: _____

UMG Recordings, Inc.

By: _____
Name: _____
Title: _____

Warner Music Group

By: _____
Name: _____
Title: _____

Sony Music Entertainment

By: *[Signature]*
Name: *Julie Swickler*
Title: *VP Business Affairs and
General Counsel*

EMI Music North America

By: _____
Name: _____
Title: _____

SBC Internet Services, Inc., BellSouth Telecommunications, Inc., Southwestern Bell Telephone Company, Pacific Bell Telephone Company, Illinois Bell Telephone Company, Indiana Bell Telephone Company, Incorporated, Michigan Bell Telephone Company, Nevada Bell Telephone Company, The Ohio Bell Telephone Company, Wisconsin Bell, Inc., The Southern New England Telephone Company, and BellSouth Telecommunications, Inc. (the AT&T Inc. companies)

By: _____
Name: _____
Title: _____

Warner Bros. Entertainment Inc.

By: _____
Name: _____
Title: _____

UMG Recordings, Inc.

By: _____
Name: _____
Title: _____

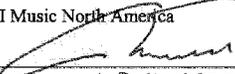
Warner Music Group

By: _____
Name: _____
Title: _____

Sony Music Entertainment

By: _____
Name: _____
Title: _____

EMI Music North America

By: 
Name: COLIN FINKELSTEIN
Title: COO

SBC Internet Services, Inc., BellSouth Telecommunications, Inc., Southwestern Bell Telephone Company, Pacific Bell Telephone Company, Illinois Bell Telephone Company, Indiana Bell Telephone Company, Incorporated, Michigan Bell Telephone Company, Nevada Bell Telephone Company, The Ohio Bell Telephone Company, Wisconsin Bell, Inc., The Southern New England Telephone Company, and BellSouth Telecommunications, Inc. (the AT&T Inc. companies)

By: _____
Name: _____
Title: _____

Warner Bros. Entertainment Inc.

By: _____
Name: _____
Title: _____

UMG Recordings, Inc.

By: _____
Name: _____
Title: _____

Warner Music Group

By: _____
Name: _____
Title: _____

Sony Music Entertainment

By: _____
Name: _____
Title: _____

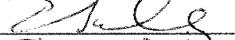
EMI Music North America

By: _____
Name: _____
Title: _____

SBC Internet Services, Inc., BellSouth Telecommunications, Inc., Southwestern Bell Telephone Company, Pacific Bell Telephone Company, Illinois Bell Telephone Company, Indiana Bell Telephone Company, Incorporated, Michigan Bell Telephone Company, Nevada Bell Telephone Company, The Ohio Bell Telephone Company, Wisconsin Bell, Inc., The Southern New England Telephone Company, and BellSouth Telecommunications, Inc. (the AT&T Inc. companies)

By: 
Name: Keith J. Epstein
Title: Assoc. General Counsel

Verizon Online LLC, Verizon Online LLC – Maryland, and Verizon Online Pennsylvania Partnership (the Verizon companies)

By: 
Name: Thomas M. D'Alto
Title: V.P. Dept. General Counsel

Comcast Cable Communications Management, LLC

By: _____
Name: _____
Title: _____

CSC Holdings, LLC

By: _____
Name: _____
Title: _____

Time Warner Cable Inc.

By: _____
Name: _____
Title: _____

Verizon Online LLC, Verizon Online LLC – Maryland, and Verizon Online Pennsylvania Partnership (the Verizon companies)

By: _____
Name: _____
Title: _____

Comcast Cable Communications Management, LLC

By: *Catherine Anselos*
Name: CATHERINE ANSELOS
Title: *SVP, PKM, Communications and Data Service*

CSC Holdings, LLC

By: _____
Name: _____
Title: _____

Time Warner Cable Inc.

By: _____
Name: _____
Title: _____

Verizon Online LLC, Verizon Online LLC – Maryland, and Verizon Online Pennsylvania Partnership (the Verizon companies)

By: _____
Name: _____
Title: _____

Comcast Cable Communications Management, LLC

By: _____
Name: _____
Title: _____

CSC Holdings, LLC

By: _____
Name: _____
Title: _____

Time Warner Cable Inc.

By: Jeff Zymanski
Name: JEFF ZYMANSKI
Title: SVP



SECOND AMENDMENT TO MEMORANDUM OF UNDERSTANDING

THIS SECOND AMENDMENT TO MEMORANDUM OF UNDERSTANDING (this "*Amendment*"), dated as of October 29, 2012, is entered into by and among the parties listed as signatories hereto (the "*Parties*").

WHEREAS, the Parties wish to amend that certain Memorandum of Understanding dated July 6, 2011, as amended, by and among the Parties hereto (the "*MOU*"), to (i) extend the deadline for establishing the Center for Copyright Information ("*CCP*") from sixty (60) days after the effective date of the MOU to September 16, 2011 and (ii) delete the first sentence of Attachment D to the MOU;

WHEREAS, Section 10(C) of the MOU provides that the Parties may amend the MOU by a written agreement signed by all parties thereto; and

WHEREAS, in accordance with such Section 10(C) of the MOU, the Parties have executed and delivered this Amendment;

NOW, THEREFORE, in consideration of the premises and the mutual promises hereinafter set forth, the Parties agree as follows:

1. Attachment C is hereby deleted in its entirety and replaced with the Attachment C set forth as Exhibit A to this Amendment.

2. This Amendment, when signed and delivered by each of the Parties, shall be effective as to all of the Parties as of the date first above written. This Amendment may be amended only in accordance with the provisions of the MOU, as amended by this Amendment and as further amended from time to time. As amended by this Amendment, the MOU shall continue in full force and effect in accordance with its terms. This Amendment may be executed in any number of counterparts, each of which shall be deemed an original, but all of which taken together shall constitute one and the same instrument. Any of the Parties hereto may execute this Amendment by signing any such counterpart. This Amendment shall be governed by, and construed and enforced in accordance with, the substantive laws of the State of New York, without regard to its principles of conflicts of laws.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK.]

IN WITNESS WHEREOF, this Second Amendment to Memorandum of Understanding has been executed and delivered as of the date first above written.

SIGNATORIES:

The Motion Picture Association of America, Inc.

By: _____

Name: _____

Title: _____

The Recording Industry Association of America, Inc.

By: _____

Name: _____

Title: _____

Walt Disney Studios Motion Pictures

By: _____

Name: _____

Title: _____

Paramount Pictures Corporation

By: _____

Name: _____

Title: _____

Sony Pictures Entertainment Inc.

By: _____

Name: _____

Title: _____

Twentieth Century Fox Film Corporation

By: _____

Name: _____

Title: _____

Universal City Studios LLC

By: _____

Name: _____

Title: _____

Warner Bros. Entertainment Inc.

By: _____

Name: _____

Title: _____

UMG Recordings, Inc.

By: _____

Name: _____

Title: _____

Warner Music Group

By: _____

Name: _____

Title: _____

Sony Music Entertainment

By: _____

Name: _____

Title: _____

EMI Music North America

By: _____

Name: _____

Title: _____

SBC Internet Services, Inc., BellSouth Telecommunications, Inc., Southwestern Bell Telephone Company, Pacific Bell Telephone Company, Illinois Bell Telephone Company, Indiana Bell Telephone Company, Incorporated, Michigan Bell Telephone Company, Nevada Bell Telephone Company, The Ohio Bell Telephone Company, Wisconsin Bell, Inc., The Southern New England Telephone Company, and BellSouth Telecommunications, Inc. (the AT&T Inc. companies)

By: _____

Name: _____

Title: _____

Verizon Online LLC, Verizon Online LLC – Maryland, and Verizon Online Pennsylvania Partnership (the Verizon companies)

By: _____

Name: _____

Title: _____

Comcast Cable Communications Management, LLC

By: _____

Name: _____

Title: _____

CSC Holdings, LLC

By: _____

Name: _____

Title: _____

Time Warner

By: _____

Name: _____

Title: _____

Exhibit A**Attachment C – Independent Review Program**

The Independent Review Program described below is intended to provide an alternative, fast, efficient and low-cost means for Subscribers and Copyright Owners to obtain independent resolution of genuine disputes that may occur in connection with the Copyright Alert program outlined in the Agreement. Its purpose is to provide a Subscriber with a non-exclusive procedure to seek review of Copyright Alerts associated with the Subscriber's account in the event a Mitigation Measure is about to be applied on the Subscriber's account. All days referred to herein are calendar days.

The Independent Review process shall be just one avenue of appeal for Subscribers challenging such measure. This Independent Review process does not prevent Subscribers or Copyright Owners from addressing disputes through the courts, and that is the proper forum for addressing issues that are beyond the scope of this Independent Review process.

1. Overview

1.1 Grounds for Independent Review. Once a Subscriber has received a Copyright Alert stating that a Mitigation Measure is about to be applied, the Subscriber may request an Independent Review of the Copyright Alerts associated with the Subscriber's account (as described in paragraph 4.1.4) on the following grounds:

- (i) Misidentification of Account – that the ISP account has been incorrectly identified as one through which acts of alleged copyright infringement have occurred.
- (ii) Unauthorized Use of Account – that the alleged activity was the result of the unauthorized use of the Subscriber's account of which the Subscriber was unaware and that the Subscriber could not reasonably have prevented.
- (iii) Authorization – that the use of the work made by the Subscriber was authorized by its Copyright Owner.
- (iv) Fair Use – that the Subscriber's reproducing the copyrighted work(s) and distributing it/them over a P2P network is defensible as a fair use.
- (vi) Misidentification of File – that the file in question does not consist primarily of the alleged copyrighted work at issue.
- (vii) Work Published Before 1923 – that the alleged copyrighted work was published prior to 1923.

1.2 Process and Determination. As further described below, if the Subscriber invokes Independent Review of the First Mitigation Measure Copyright Alert, the Subscriber shall have the opportunity to challenge some or all of the previously issued Copyright Alerts. In order to have the First Mitigation Measure avoided, the Reviewer must find in favor of the Subscriber for at least half of the previously issued Copyright Alerts (i.e. 2 of 4 or 3 of 5). If the Subscriber invokes Independent Review of the Second Mitigation Measure Copyright Alert, the Subscriber shall have the opportunity to challenge only the Second Mitigation Measure Copyright Alert. In order to have the Second Mitigation Measure avoided, the Reviewer must find in favor of the Subscriber for the Second Mitigation Measure Copyright Alert. All determinations shall be made by an independent "Reviewer" as described below, and the determinations shall have the effect set forth herein.

2. Standard of Review.

2.1. Misidentification of Account. A Subscriber shall prevail on this defense if the Participating ISP's and/or Copyright Owner's records indicate, upon Independent Review, that a factual error was made in (1) identifying the IP address at which the alleged copyright infringement occurred and/or (2) correlating the identified IP address to the Subscriber's account. In reviewing the Participating ISP's or Copyright Owner's records, automated systems for capturing IP addresses or other information in accordance with Methodologies have a rebuttable presumption that they work in accordance with their specifications, unless the Independent Expert's review of any such Content Owner Representative Methodology resulted in a Finding of Inadequacy in which event such rebuttable presumption shall not apply to such Content Owner Representative Methodology.

2.2. Unauthorized Use of Account. A Subscriber shall prevail on this defense if the Subscriber adequately and credibly demonstrates that the alleged activity was the result of unauthorized use of the Subscriber's account by someone who is not a member or invitee of the household (e.g., via an unsecured wireless router or a hacked Internet connection) of which the Subscriber was unaware and that the Subscriber could not reasonably have prevented. The foregoing sentence notwithstanding, the Reviewer may in his or her discretion conclude that a Subscriber is entitled to prevail under this defense despite the Subscriber's failure to secure a wireless router if the Reviewer otherwise concludes that the Subscriber adequately and credibly demonstrates that the alleged activity was the result of unauthorized use of the Subscriber's account by someone who is not a member or invitee of the household of which the Subscriber was unaware. In determining whether this standard has been satisfied, the Reviewer shall consider the evidence in light of the educational messages previously provided by the Participating ISP. Except as set forth herein, this defense may be asserted by a Subscriber only one (1) time to give the Subscriber the opportunity to take steps to prevent future unauthorized use of the Subscriber's account. Any subsequent assertion of this defense by a Subscriber shall be denied as barred, unless the Subscriber can show by clear and convincing evidence that the unauthorized use occurred despite reasonable steps to secure

the Internet account and that the breach of such security could not reasonably have been avoided.

2.3. Authorization. A Subscriber shall prevail on this defense if the Subscriber adequately and credibly demonstrates with written or other documented evidence that the Subscriber's alleged activity was actually specifically authorized by the Copyright Owner or its authorized representative. Such written or other documented evidence typically must include a true and unaltered copy of the agreement or communication asserted to grant the claimed authorization. Such evidence shall not be deemed adequate and credible if, among other things, (i) the evidence on its face does not support a claim of authorization, (ii) the evidence does not appear authentic, or (iii) a reasonable person in the Subscriber's position would not have concluded that the communication was in fact authorizing the specific use made of the work and that such authorization came from the actual Copyright Owner or by someone authorized to act on his/her behalf. The defense shall fail if the Copyright Owner has demonstrated: (x) that the specific use of the work made by the Subscriber was not in fact authorized by the Copyright Owner; (y) if the alleged authorization did not come directly from the Copyright Owner, that the person purporting to grant authorization was not authorized to act on behalf of the Copyright Owner for purposes of authorizing the specific use made of the work by the Subscriber; or (z) that the documentary evidence submitted by the Subscriber likely is not authentic or has been altered in a material manner.

2.4. Fair Use. A Subscriber shall prevail on this defense if the Subscriber adequately and credibly demonstrates fair use of the copyrighted work under prevailing principles of copyright law (which shall be identified as described in section 6).

2.5. Misidentification of File. A Subscriber shall prevail on this defense if the Subscriber adequately and credibly demonstrates that a factual error was made in identifying the file at issue as consisting primarily of the alleged copyrighted work. In making this determination, the Content Owner Representative Methodology used to identify the file shall have a rebuttable presumption that it works in accordance with its specifications, unless the Independent Expert's review of any such Content Owner Representative Methodology resulted in a Finding of Inadequacy in which event such rebuttable presumption shall not apply to such Content Owner Representative Methodology.

2.6. Work Published Before 1923. A Subscriber shall prevail on this defense if the Subscriber adequately and credibly demonstrates that the alleged copyrighted work in question was actually published prior to 1923.

3. Effect of Decision. If the Reviewer's decision is in favor of the Subscriber for at least half of the Copyright Alerts associated with the Subscriber's account, the filing fee described in paragraph 4.1.6 shall be promptly refunded to the Subscriber, the Participating ISP shall remove all of the previously issued Copyright Alerts from the Subscriber's account records and, except as set forth in paragraph 4.1.7 below, the Participating ISP shall refrain from applying any Mitigation Measure based on the

previously issued Copyright Alert(s). If the Reviewer's decision is not in favor of the Subscriber for a at least half of the Copyright Alerts associated with the Subscriber's account, the Mitigation Measure shall be applied promptly. The Reviewer's decision will be binding solely for the purposes of the Copyright Alert program. By participating in the Independent Review, the Subscriber, the Participating ISP, and the Copyright Owner agree to waive all rights to challenge the Reviewer's decision for purposes of the Copyright Alert program. The Reviewer's decision shall have no effect outside of the Copyright Alert program, shall not act as res judicata or collateral estoppel or any similar bar, and shall not have any precedential impact for other Independent Reviews with respect to other Subscribers within the Copyright Alert program. In any judicial proceeding between a Subscriber and a Copyright Owner concerning subject matter that is or has been the subject of Independent Review, neither the Subscriber nor the Copyright Owner shall seek to enter into evidence, or otherwise refer to or cite, either the fact of the Independent Review or any outcome of the Independent Review.

4. Independent Review Procedure.

4.1. How to Initiate an Independent Review.

4.1.1. *ACIR Form.* When the Participating ISP sends a Copyright Alert stating that the Subscriber's account is subject to a Mitigation Measure, the Participating ISP will also make available to the Subscriber access to an online Application to Commence Independent Review form/s ("ACIR form") and related materials. The ACIR form and related materials will permit the Subscriber to review all of the Copyright Alerts applicable to the Subscriber's account that have not previously been subject to review, as further described in paragraph 4.1.4. The ACIR form will identify all of the information necessary for the Subscriber to invoke an Independent Review, including each defense asserted as to the work identified in a Copyright Alert under review, and also include space for provision of the Subscriber's contact information.

4.1.2. *Authorization.* The ACIR form will contain an authorization by the Subscriber to disclose relevant personal information to the Administering Organization and the Reviewer only to the extent necessary. Except as explained in the next sentence or as required by judicial order or other legal process, all Subscriber personal information will be held in confidence and not disclosed to the Copyright Owner. If the Subscriber's defense is based on authorization, then the Reviewer may, in his or her discretion, disclose to the Copyright Owner only such personal information concerning the Subscriber as is reasonably necessary to permit the Copyright Owner to rebut a claim of authorization if that information is required for such purposes. The ACIR form will contain an authorization by the Subscriber to disclose relevant personal information to the Copyright Owner in the circumstances described in the immediately preceding sentence.

4.1.3. *Information Required.* The Subscriber must (1) identify the defense(s) asserted as to the work identified in each Copyright Alert at issue by

checking the proper boxes on the ACIR form, (2) explain the specific basis for each defense, and (3) provide the corresponding back-up material to support such grounds. In the case of a defense of authorization, the ACIR form must be accompanied by the applicable written or other documented evidence that the Subscriber's alleged activity was specifically authorized by the Copyright Owner or its authorized representative, as described in paragraph 2.3. In the case of a defense of fair use, the ACIR form must (1) be accompanied by a true and unaltered copy of each content file that the Subscriber asserts to be a fair use under prevailing principles of copyright law; and (2) an explanation of each use the Subscriber made of the file, including any distribution or downloading identified in the Copyright Alert(s), and the basis for claiming each such use as a fair use.

4.1.4. *Copyright Alerts Subject to Review.* The Subscriber shall have the right to invoke Independent Review for the last Copyright Alert sent as well as prior Copyright Alerts, provided that the right to have a particular Copyright Alert reviewed shall be waived if that right is not invoked the first time the Copyright Alert becomes eligible to be reviewed. Accordingly, when a Subscriber first receives a Mitigation Measure Copyright Alert, the Subscriber may invoke the Independent Review process as to any prior Copyright Alert and must, as noted above in section 1.2, prevail on at least half of the alerts previously received, but if any of those Copyright Alerts is not reviewed at that time it will thereafter be unreviewable.

4.1.5. *Multiple Works Identified in a Copyright Alert.* In cases in which a single Copyright Alert alleges or refers to allegations of infringing activity with respect to multiple works, the Subscriber need only offer a defense to the work that triggered the Copyright Alert, and the Independent Review process shall only apply with respect to that work for that particular Copyright Alert. For clarity, works in ISP Notices sent during the Grace Period would not trigger the Copyright Alert and thus not require a defense.

4.1.6. *Filing Fee.* The Subscriber shall be required to pay a filing fee of thirty-five dollars (\$35) in order to invoke the Independent Review, unless the Subscriber qualifies for a waiver or reduction in the filing fee in accordance with the procedures of the Administering Organization (as defined in paragraph 5.1 below). This fee will be refunded to the Subscriber in the event that the Reviewer decides in favor of the Subscriber as to any Copyright Alert eligible for review.

4.1.7. *Deadline.* The ACIR form, related materials and filing fee ("ACIR Package") must be submitted by the Subscriber electronically within fourteen (14) days after issuance (i.e., the date the alert is sent to the Subscriber) of the relevant Mitigation Measure Copyright Alert. Except as contemplated in paragraph 5.6 below, failure to properly submit an ACIR form by the due date shall be deemed a waiver of the right to seek Independent Review regarding the applicable Mitigation Measure.

4.1.8. *Submission of ACIR Package.* The Subscriber must submit the ACIR Package to the Administering Organization. The Administering Organization shall immediately send to the applicable Participating ISP notice that the ACIR Package has been filed, along with the anonymous account identifier associated with that ACIR.

4.1.9. *Effect of Filing for Independent Review.* A Subscriber's filing of the ACIR form with the Independent Reviewer will serve as a stay of the implementation of any Mitigation Measure if the ACIR form is submitted within fourteen (14) days of issuance of the relevant Mitigation Measure Copyright Alert. A Subscriber's failure to file an ACIR or otherwise challenge an allegation of copyright infringement shall not be construed as an admission or waiver in any other forum or context.

4.2 Process for Independent Review.

4.2.1. *Selection of Reviewer.* All Independent Reviews shall be resolved by one (1) individual serving as an independent Reviewer. The Reviewer will be selected by the Administering Organization from a panel of neutrals, as further described in paragraph 5.2.

4.2.2. *Initial Review of ACIR Package.* A Reviewer will review the ACIR package within seven (7) days of receipt to determine whether it is substantially complete. To be considered substantially complete, (1) the ACIR Package must include a substantially completed ACIR form; (2) the ACIR form must assert a defense as the work identified in the relevant Copyright Alert subject to Independent Review; (3) for each defense asserted as to each work, the ACIR Package must include sufficient information as described in paragraph 4.1.3 to permit the Independent Review to proceed meaningfully and to potentially result in a decision in favor of the Subscriber; and (4) the ACIR Package must include the required payment as provided in paragraph 4.1.6. If the ACIR Package is not substantially complete, the case will be denied. The first time an ACIR Package is denied, such a denial shall be without prejudice to afford the Subscriber one additional opportunity to correct any mistakes or omissions in the ACIR Package. In such a case, the Reviewer shall notify the Subscriber of the relevant defects and afford the Subscriber seven (7) days to remedy the defects by submitting a substantially complete ACIR Package. Otherwise (except as provided in paragraph 5.6 below), such a denial shall be with prejudice. Either a denial without prejudice that is not remedied within seven (7) days or a denial with prejudice shall have the same effects as a denial on the merits (see section 3).

4.2.3. *Verification that Defense of Unauthorized Use of Account is not Barred.* In the case of any defense of unauthorized use of account, the Reviewer's initial review will also consider whether that defense is barred because the Administering Organization's records indicate that the Subscriber

previously asserted that defense in another Independent Review. If so, the defense shall be denied, unless the Subscriber can show by clear and convincing evidence that the unauthorized use occurred despite reasonable steps to secure the Internet account and that the breach of such security could not reasonably have been avoided. If for any reason the Administering Organization's records are inconclusive as to this question, the Reviewer will request clarification from the Participating ISP pursuant to paragraph 4.2.4.

4.2.4. Collection of Standard Information from Participating ISP and Copyright Owner. If the ACIR Package is substantially complete, the Reviewer will, if needed, request standard relevant information from the Participating ISP and/or Copyright Owner to assess the grounds for review. Details of the standard information to be provided by the Participating ISP and/or Copyright Owner for different types of defenses shall be determined by mutual agreement of representatives of the Administering Organization, Participating ISPs and Copyright Owners as implementation proceeds, with the goal of having provision of this standard information be a straightforward and largely automated process. In the case of a defense of misidentification of account, information to be provided by the Participating ISP is anticipated to consist of information in the Participating ISP's possession, custody, or control relating to (1) those ISP Notices received by the Participating ISP that triggered Copyright Alerts and matched to the Subscriber's account, (2) Copyright Alerts sent to the Subscriber by the Participating ISP, and (3) the Participating ISP's matching of IP addresses on ISP Notices received by the Participating ISP to the Subscriber's account. Information to be provided by the Copyright Owner is anticipated to consist of all or part of the evidence package(s) (*i.e.*, information relating to the alleged access to copyrighted material) for one (1) or more Copyright Alerts that are the subject of the Independent Review. The Participating ISP and Copyright Owner, as applicable, will provide the relevant information to the Reviewer within fourteen (14) days after receipt of the request.

4.2.5. First Substantive Review. Within seven (7) days from receipt of the relevant standard information from the Participating ISP and/or the Copyright Owner, the Reviewer will review the case record substantively to determine if additional information from the Participating ISP and/or Copyright Owner is required, or whether it is apparent without soliciting further information that the Subscriber will not prevail as to at least half of the Copyright Alerts received by the Subscriber.

4.2.6. Supplemental Information. The Reviewer shall have the discretion to request supplemental information from the Participating ISP, Copyright Owner or Subscriber within the seven (7) day period referred to in paragraph 4.2.5, if such information would likely be material to a just resolution of the Independent Review and is consistent with the standards established in section 4.2.4. If the Reviewer makes such a request, the applicable party(ies) shall have fourteen (14) days to respond. If the Subscriber asserts a defense of authorization or fair use

and the Reviewer determines that the defense may have merit, then the Copyright Owner shall receive all relevant information about the defense from the Reviewer and be afforded an opportunity to provide evidence to rebut the defense within fourteen (14) days from receipt of such information. Such information shall include (1) in the case of a defense of authorization, all substantiating evidence and explanation submitted by the Subscriber as to each relevant work and the Subscriber's identifying information, unless the Reviewer concludes that the Copyright Owner does not need to know the identity of the Subscriber to evaluate the Subscriber's claim that his or her activity was authorized; and (2) in the case of a defense of fair use, the content file submitted by the Subscriber as to each relevant work and an explanation of why the Subscriber believes each use of that content file to be a fair use.

4.2.7. *Final Assessment and Issuance of Decision.* Within fourteen (14) days of receipt of all requested information, including any supplemental information provided pursuant to paragraph 4.2.6, or passage of the relevant time to provide supplemental information in the event no supplemental information is received, the Reviewer shall assess the complete case record and enter a final decision. In doing so, the Reviewer shall determine the relevance, materiality and weight of all evidence based on the available record. The proceedings will take place exclusively on the written record, and there shall be no live hearings. Upon reaching a final decision, the Reviewer will notify the Subscriber, Participating ISP and Copyright Owner of the outcome, and if the decision is a denial of the Subscriber's defense, the Reviewer will also include a short description of the rationale for the decision.

4.2.8. *Election not to Defend a Notice by Copyright Owner.* A Copyright Owner may elect not to defend a Copyright Alert at any time during the 7 day period following its receipt of notice that a case has been filed concerning that Copyright Alert, which shall have the same effect as a finding for the Subscriber with respect to such work (see section 3).

4.2.9. *Communications Among Parties.* Except as specifically described in these rules (e.g., in the case of requests for information as described in paragraphs 4.2.4 and 4.2.6), there will be no communication between the Reviewer and the Participating ISP, Copyright Owner or Subscriber concerning the Independent Review. There is to be absolutely no discovery between the parties to the dispute, and no party shall have any obligation to respond to any request for information or to provide any particular information, except as described herein.

5. Administration of Independent Review Process.

5.1. In General. The Independent Review process shall be coordinated by the administering organization selected by the CCI Executive Committee ("Administering

Organization”). The Independent Review process shall be governed exclusively by these rules.

5.2. Selection of Reviewers. The Administering Organization shall have mechanisms for establishing a panel of neutrals and for ensuring their continuing neutrality, their compliance with these rules, and their adherence to the governing principles of copyright law as provided in section 6. Reviewers must be lawyers, but need not necessarily have the legal or case management expertise that would qualify them to act as arbitrators of more complex disputes in a broader-ranging alternative dispute resolution process. The Administering Organization shall provide Reviewers training in this Independent Review process and governing principles of copyright law determined as described in section 6. Reviewers may be staff employees of the Administering Organization if the volume of disputes subject to the Independent Review process so warrants.

5.3. Automation. The Administering Organization shall implement automated processes for managing the workflow of cases proceeding through the Independent Review process, including means for seeking and obtaining information from Participating ISPs and Copyright Owners in a manner that minimizes the associated workload on Participating ISPs and Copyright Owners and is automated to the maximum extent practicable.

5.4. Records of Subscriber History of Invoking Independent Review. The Administering Organization will maintain a secure database of Subscribers’ history of invoking the Independent Review process, which will be available to Reviewers when evaluating future disputes involving the relevant Subscribers. Thus, it should be possible for a Reviewer to determine from this database whether a Subscriber has previously asserted a defense of unauthorized use of account, and a Reviewer may consider a Subscriber’s Independent Review history in evaluating the credibility of claims under review.

5.5. Recordkeeping and Review. The CCI Executive Committee and Administering Organization will establish processes for (1) maintaining records concerning proceedings, (2) periodically reviewing anonymous, aggregated information about issues and outcomes so that trends can be identified and addressed if warranted, and (3) confidentially auditing decisions for purposes of evaluating the performance of Reviewers and the Administering Organization. Except to the extent necessary to maintain records of outcomes of proceedings for purposes of operation and review of the Independent Review process or as otherwise expressly set forth herein, Reviewers shall not prepare written decisions in the cases they decide, and all decisions shall be treated in accordance with Section 4(H) of the MOU. The Parties to the Agreement agree to negotiate in good faith as to adjustments in the Independent Review process if such adjustments are warranted by actual experience in operating the Independent Review process.

5.6. Provision of Information. Fair and efficient administration of the Independent Review process depends upon timely provision of information requested by the Reviewer at various steps of the process, as described in paragraph 4.2. Whenever these rules set forth a timeframe for provision of information requested by the Reviewer, the Reviewer may grant reasonable extensions of such period (not to exceed fourteen (14) days) for substantial good cause shown. In the absence of the requested information at the deadline for providing the same, the following provisions will apply:

5.6.1. *Delays in Providing Standard Information.* If the Reviewer properly requests a standard package of information from a Participating ISP or Copyright Owner, as described in paragraph 4.2.4, and the Participating ISP or Copyright Owner does not provide the requested information as to some or all claims or works on a timely basis, (1) the Reviewer shall promptly notify the Participating ISP or Copyright Owner and the Participating ISP or Copyright Owner shall have a further seven (7) days to provide the requested information; and (2) the Administering Organization shall reflect such deficiency in reports to be provided periodically to the CCI Executive Committee. Recurring failure of a Participating ISP or Copyright Owner to provide requested standard information during the initial period identified in paragraph 4.2.4, in other than isolated instances, will be considered a breach of its obligations under the Agreement. If a Participating ISP or Copyright Owner does not provide available requested information within a further seven (7) days, (a) the dispute will proceed to the next step of decision making based on the available record without such information, giving the Subscriber the benefit of any doubt concerning the missing requested information; (b) the Administering Organization shall reflect such deficiency in reports to be provided periodically to the CCI Executive Committee; and (c) the Participating ISP or Copyright Owner will be considered in breach of its obligations under the Agreement.

5.6.2. *Delays in Providing Supplemental Information.* If the Reviewer properly requests supplemental information from a Participating ISP, Copyright Owner or Subscriber pursuant to paragraph 4.2.6, and the Participating ISP, Copyright Owner or Subscriber does not provide the requested information as to some or all claims or works on a timely basis, the dispute will proceed to the next step of decision making based on the available record without such information. If the Reviewer believes that the position of a party to the proceeding other than the one that has failed to provide the requested information is otherwise meritorious, the Reviewer shall give such party the benefit of any doubt concerning the missing requested information.

6. Legal Principles to Be Applied in Independent Review. The Independent Review process will, to the extent relevant, apply prevailing legal principles as determined by United States federal courts. The Administering Organization will commission an accepted, independent expert on copyright law, who is approved by the CCI Executive Committee, to outline prevailing legal principles of fair use for purposes of deciding defenses of fair use, and any other legal principles necessary for resolution of issues

within the scope of this Independent Review process. Such outline will be updated from time to time as necessary. If additional material questions of law arise as the Independent Review process is implemented, they may be referred to an accepted, independent expert approved by the CCI Executive Committee as needed. The Administering Organization will advise the Parties to the Agreement of issues referred to, and principles determined by, such an expert, and provide a process for the Parties to the Agreement to provide input concerning the issues, so as to ensure that the expert's determinations are fully-informed and reflect prevailing law as determined by United States federal courts.



MEMORANDUM OF UNDERSTANDING

Whereas:

- Copyright infringement (under Title 17 of the United States Code) on the Internet (“Online Infringement”) – including the illegal distribution of copyrighted works such as music, movies, computer software, gaming software, e-books and the like via Peer-to-Peer (“P2P”) file exchanges and other illegal distribution via Internet file hosting, streaming or other technologies – imposes substantial costs on copyright holders and the economy each year. Online Infringement also may contribute to network congestion, negatively affecting users’ Internet experiences. The availability of copyrighted content, including live and recorded programming, from pirated sources harms legitimate content creation and distribution. Content creators are taking steps to make lawful content more available online. The lawful online distribution businesses are vibrant and growing and they are harmed by infringement. In addition, law enforcement is pursuing opportunities to enhance its ability to investigate, prosecute, and ultimately punish and deter those who violate copyright law.
- While the government maintains a critical role in enforcing copyright law, it should be readily apparent that, in an age of viral, digital online distribution, prosecution of individual acts of infringement may serve a purpose, but standing alone this may not be the only or best solution to addressing Online Infringement. If Online Infringement is to be effectively combated, law enforcement must work with all interested parties, including copyright holders, their licensees, artists (and the guilds, unions and other organizations that represent them), recording companies, movie studios, software developers, electronic publishers, Internet Service Providers (“ISPs”), public interest groups, other intermediaries and consumers on reasonable methods to prevent, detect and deter Online Infringement. Such efforts must respect the legitimate interests of Internet users and subscribers in protecting their privacy and freedom of speech, in accessing legitimate content, and in being able to challenge the accuracy of allegations of Online Infringement. This work should include an educational component because evidence suggests that most informed consumers will choose lawful services and not engage in Online Infringement. This work also should include the development of solutions that are reasonably necessary to effectuate the rights that are granted by copyright without unduly hampering the legitimate distribution of copyrighted works online or impairing the legitimate rights and interests of consumers and ISPs. Such efforts serve not only the shared interests of creators and distributors of creative works, but also the interests of Internet users who benefit from constructive measures aimed at education and deterrence in lieu of litigation with its attendant costs and legal risk.
- A reasonable, alert-based approach may help to protect legal rights granted by copyright and stem the unlawful distribution of copyrighted works, while

CONFIDENTIAL

FINAL
7/6/2011

providing education, privacy protection, fair warning and an opportunity for review that protects the lawful interests of consumers. The efficiencies gained from such a cooperative model may benefit all interested parties, including consumers.

- Enforcement and consumer education programs alone may not be able to fully address the issue of Online Infringement. In addition, it is important for content and copyright owners to continue to make available an array of lawful alternatives for consuming movies, music, and other content online, including new distribution models that make it easy and attractive for consumers to lawfully obtain online the content they want. ISPs can assist in these efforts by encouraging subscribers to seek legal alternatives for obtaining content. The widespread availability of lawful content will benefit consumers, content owners and ISPs.

Whereas, the Content Owner Representatives, the Participating ISPs, and the members of the Participating Content Owners Group (all, as defined in Section 1 below) and independent record labels and film production companies (Independent Content Owners, as defined in Section 5C below) represented by the American Association of Independent Music ("A2IM") and the Independent Film and Television Alliance ("IFTA"), respectively, seek to establish a consumer-focused process for identifying and notifying residential wired Internet access service customers of the Participating ISPs ("Subscribers") (other than dial-up Subscribers) who receive multiple notifications of allegations of Online Infringement made via P2P networks and applications ("P2P Online Infringement"), in an effort to educate consumers, deter Online Infringement, and direct consumers to lawful online legitimate sources of content.

Whereas, having considered the desirability of implementing such a process as a means to encourage lawful and legitimate use of copyrighted content, the Parties (as defined in Section 1 below) hereby voluntarily enter into this Memorandum of Understanding (the "Agreement").

IT IS HEREBY UNDERSTOOD AND AGREED AMONG THE PARTIES THAT:

1. Parties to the Agreement

The parties to this Agreement (the "Parties") are The Recording Industry Association of America, Inc. ("RIAA"), The Motion Picture Association of America, Inc. ("MPAA" and together with RIAA, the "Content Owner Representatives"); the entities set forth in Attachment A (as may be amended from time to time) (collectively, the "Participating ISPs"); and solely for the purposes of Sections 2(E), 4(C), 4(D), 4(H), 4(I), 5(A), 5(C), 6, 7, 8, 9(E), 9(F), and 10 of this Agreement, MPAA members Walt Disney Studios Motion Pictures, Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corporation, Universal City Studios LLC, and Warner Bros. Entertainment Inc. (such MPAA members, together with MPAA, the "MPAA Group"), RIAA members UMG Recordings, Inc., Warner Music Group, Sony Music

Entertainment, and EMI Music North America (such RIAA members, together with RIAA, the “RIAA Group” and together with the MPAA Group, and any other entities set forth in Attachment B (as may be amended from time to time), the “Participating Content Owners Group”).

2. Establishment of CCI

A. Not later than sixty (60) days after the Effective Date (as defined in Section 8(A) below), the Content Owner Representatives and the Participating ISPs will establish the Center for Copyright Information (“CCI”) to assist in the effort to combat Online Infringement by, among other things, (i) taking an active role in educating the public about the laws governing the online distribution of works protected by copyright, including educating the public regarding civil and criminal penalties for Online Infringement; (ii) interfacing with third party stakeholders on issues and questions of common interest to the Content Owner Representatives and the Participating ISPs pertaining to Online Infringement and related matters; (iii) assisting in the design and implementation of a process that provides for consumer and Subscriber education through the forwarding of Copyright Alerts to, and application of Mitigation Measures (as defined in Section 4(G)(iii) below) on, Subscribers engaged in persistent P2P Online Infringement, including reviewing the accuracy and efficacy of Content Owner Representative processes for identifying instances of P2P Online Infringement and ISP processes for identifying the Subscriber accounts associated with such P2P Online Infringement; (iv) periodically reviewing the effectiveness and impact of such processes as further described in Section 9 below; (v) collecting and disseminating to interested parties and the public data regarding Online Infringement and the lawful means available to obtain non-infringing copyrighted works; and (vi) facilitating the involvement of non-participating ISPs in the work of CCI and in the Copyright Alert program (as defined in Section 4(G) below).

B. CCI will be governed by a six (6) member executive committee (the “Executive Committee”) that will be selected as follows: three (3) members to be designated collectively by the Content Owner Representatives, and three (3) members to be designated collectively by the Participating ISPs. Each member shall serve without compensation for a term of two (2) years, which may be renewed.

C. The members of the Executive Committee shall be selected within forty-five (45) days of the Effective Date (as defined in Section 8(A) below). The Executive Committee shall hold an initial meeting and designate an individual to serve as its Executive Director. The Executive Director shall not be one (1) of the six (6) members of the Executive Committee.

D. The Executive Committee shall also establish a three (3) member advisory board to the Executive Committee (the “Advisory Board”). The Content Owner Representatives shall select one (1) member of the Advisory Board, the Participating ISPs shall select one (1) member of the Advisory Board, and the two (2) selected Advisory Board members shall select the third member. Each of the members of the

Advisory Board shall be drawn from relevant subject matter expert and consumer interest communities and, unless otherwise agreed in writing, shall not be employees or agents of the Content Owner Representatives nor of the Participating ISPs. The Advisory Board shall be consulted on any significant issues the Executive Committee is considering relating to the design and implementation of the Notice Process and the Copyright Alert program (as defined in Section 4(C) and Section 4(G), respectively), and shall provide recommendations to the Executive Committee as appropriate. The Advisory Board may also provide recommendations regarding the CCI educational program described in Section 3 below, upon the Executive Committee's request.

E. Funding for CCI will be provided fifty percent (50%) by the Participating Content Owners Group and fifty percent (50%) by the Participating ISPs. The initial CCI budget shall be presented to and approved by the Executive Committee within ninety (90) days of the Effective Date (as defined in Section 8(A) below) and shall be funded by the Participating Content Owners Group and the Participating ISPs promptly thereafter according to the apportionment set forth in this Section 2(E). The Executive Committee shall also oversee and approve by majority all matters regarding the corporate formation of CCI and the further development of its internal structure. CCI shall be governed by its articles of incorporation and bylaws to be filed in connection with its corporate formation in the State of Delaware. The bylaws shall, inter alia, include a mechanism for adding parties to this Agreement.

3. CCI Educational Program

In conformance with its budget, CCI shall develop an educational program to inform the public about laws prohibiting Online Infringement and lawful means available to obtain digital works online and through other legitimate means. CCI will also establish, host and maintain an online information center where educational material will be available to the general public. The Content Owner Representatives and the Participating ISPs shall contribute to CCI any applicable educational materials already developed by the respective Content Owner Representatives and Participating ISPs, and CCI shall facilitate the dissemination of such educational materials through online or other media. Such educational materials shall include, among other things, information about the technical means Subscribers can use to secure their computers and networks to avoid unwittingly assisting others in Online Infringement. Any Content Owner Representative or Participating ISP may add additional educational materials to the online information center subject to the prior permission of the Executive Committee.

4. System for Reducing Instances of P2P Online Infringement

A. The Content Owner Representatives will develop and maintain written methodologies, which shall be adopted by the applicable Content Owner Representative, for identifying instances of P2P Online Infringement that are designed to detect and provide evidence that the identified content was uploaded or downloaded or copied and offered on a P2P network to be downloaded through a bit torrent or other P2P technology. Each Participating ISP will develop and maintain methodologies, which

shall be adopted by the applicable Participating ISP, to match Internet Protocol (“IP”) addresses identified by the Content Owner Representatives to the Participating ISP Subscribers’ accounts, to keep a record of repeat alleged infringers, and to apply Mitigation Measures (as defined in [Section 4\(G\)\(iii\)](#) below). Such Content Owner Representative and Participating ISP methodologies are collectively referred to herein as the “[Methodologies](#)”. The goal of these Methodologies shall be to ensure that allegations of P2P Online Infringement, related records, and the application of any Mitigation Measures are based on reliable, accurate, and verifiable processes and information.

B. In conformance with its budget, CCI shall retain an independent and impartial technical expert or experts (the “[Independent Expert](#)”) to review on a periodic and ongoing basis the Methodologies and any modifications thereto, and recommend enhancements as appropriate, with the goal of ensuring and maintaining confidence on the part of the Content Owner Representatives, the Participating ISPs, and the public in the accuracy and security of the Methodologies. If a Content Owner Representative Methodology is found by the Independent Expert to be fundamentally unreliable, the Independent Expert shall issue a confidential finding of inadequacy (“[Finding of Inadequacy](#)”) to the affected Content Owner Representative to permit the affected Content Owner Representative to modify or change the Methodology for review. The selection of the Independent Expert shall require approval by a majority of the members of the Executive Committee. The Content Owner Representatives and the Participating ISPs agree to provide reasonable cooperation to the Independent Expert and provide to the Independent Expert a copy of their respective Methodologies, and any technical or other information reasonably related to their respective Methodologies needed to undertake this review process. As a condition of retention, the Independent Expert shall agree in writing to keep confidential any proprietary or other confidential information provided by the Content Owner Representatives and the Participating ISPs as part of the Independent Expert’s review. The Content Owner Representatives and each Participating ISP shall exchange general descriptions of their respective Methodologies upon request. At the direction of CCI, the Independent Expert may consult with each Content Owner Representative or Participating ISP concerning the implementation and ongoing operation of that Representative’s or ISP’s Methodology. In addition, the Independent Expert will (i) review the Methodologies with recognized privacy experts agreed to by a majority of the Executive Committee and (ii) recommend enhancements to the Methodologies as appropriate to address privacy issues, if any, identified by the privacy experts. Failure to adopt a recommendation of the Independent Expert shall not amount to a breach under this Agreement. The Independent Expert’s recommendations must be shared with each of the Content Owner Representatives and the affected Participating ISP, but may not be disclosed to other parties, including Participating ISPs other than the affected Participating ISP, without the express written permission of each Content Owner Representative and the affected Participating ISP and any disclosure to such other third parties shall not include any proprietary or otherwise confidential information of the Content Owner Representative(s) or Participating ISP affected.

C. The Content Owner Representatives may send notices pursuant to this Agreement and the implementation agreements described in [Section 5\(A\)](#) of this

Agreement (the "Implementation Agreements") to the Participating ISPs of instances of alleged P2P Online Infringement (each an "ISP Notice"), and the Participating ISPs shall accept and process such notices involving the Participating ISPs' Subscribers (such Content Owner Representative and Participating ISP actions being, together, a "Notice Process"). The Content Owner Representatives agree to generate ISP Notices only for instances of P2P Online Infringement identified through the use of the Content Owner Representative Methodologies that have been reviewed and evaluated by the Independent Expert, and that have not been issued a Finding of Inadequacy. For purposes of generating ISP Notices, the Content Owner Representatives further agree to focus on instances of P2P Online Infringement involving files or data consisting primarily of infringing material or containing unauthorized copyrighted works in complete or substantially complete form and to avoid instances of P2P activity in which *de minimis* amounts of allegedly infringing material are incorporated into files or data consisting primarily of non-infringing material. The Content Owner Representatives will also endeavor to generally send the ISP Notices within twenty-four (24) hours of confirmed identification of the alleged activity described in the ISP Notice. ISP Notices shall be generated and sent solely by the Content Owner Representatives or their service providers (including on behalf of the Participating Content Owners Group, the Independent Content Owners (as defined in Section 5(C) below), the RIAA Group's members' distributed labels and those entities set forth in Attachment D hereto). The individual members of the Participating Content Owners Group; IFTA and A2IM; the Independent Content Owners (as defined in Section 5(C) below); the RIAA Group's members' distributed labels; and those entities set forth in Attachment D hereto shall not generate or send ISP Notices.

D. The Content Owner Representatives agree that each ISP Notice provided to a Participating ISP as part of the Notice Process shall clearly identify: (i) the copyrighted work that allegedly has been infringed and the owner of such work; (ii) a description of the basis upon which the notifying Content Owner Representative or its agent asserts the right to enforce the particular affected copyright on behalf of the person or entity who owns or controls the copyright and/or exclusive distribution rights in the copyright (a "Copyright Owner"); (iii) a statement that the notifying Content Owner Representative or its agent has a good faith belief that use of the material is not authorized by the Copyright Owner, its agent, or the law; (iv) a statement that the information in the ISP Notice is accurate and that, under penalty of perjury, the Content Owner Representative is authorized to act on behalf of the Copyright Owner whose rights were allegedly infringed; and (v) technical information necessary for the Participating ISP to identify the Subscriber (*e.g.*, IP address, date, time and time zone of the alleged P2P Online Infringement, and such additional information as may be necessary as the Participating ISPs transition to IPv6). The Content Owner Representatives and the Participating Content Owners Group agree that all notices of P2P Online Infringement generated by them or on their behalf and delivered to the Participating ISPs shall meet the requirements for ISP Notices hereunder, shall comply with the terms hereof and shall be governed exclusively by this Agreement and the Implementation Agreements.

E. Reserved.

F. Each Participating ISP agrees to communicate the following principles in its Acceptable Use Policies (“AUP”) or Terms of Service (“TOS”): (i) copyright infringement is conduct that violates the Participating ISP’s AUP or TOS and for which a Subscriber may be legally liable; (ii) continuing and subsequent receipt of Copyright Alerts (as defined in Section 4(G) below) may result in the Participating ISP taking action by the application of Mitigation Measures (as defined in Section 4(G)(iii) below); and (iii) in addition to these Mitigation Measures, the Participating ISP may also adopt, in appropriate circumstances, those measures specifically authorized by section 512 of the Digital Millennium Copyright Act (“DMCA”) and/or actions specifically provided for in the Participating ISP’s AUP and/or TOS including temporary suspension or termination, except that nothing in this Agreement alters, expands, or otherwise affects any Participating ISP’s rights or obligations under the DMCA.

G. Each Participating ISP will develop, implement and independently enforce a Copyright Alert program as described in this Section 4(G) (each such program a “Copyright Alert Program”), provided that each Participating ISP shall not be required to exceed the notice volumes pertaining to its Copyright Alert Program as established in Section 5 of this Agreement. Each Participating ISP’s Copyright Alert Program will be triggered by the Participating ISP’s receipt of an ISP Notice that can be associated with a Subscriber’s account and will result in the Participating ISP sending one (1) or more alert notices to the applicable Subscriber concerning the ISP Notice, as further described below (each such alert notice a “Copyright Alert”).

Each Participating ISP’s Copyright Alert Program shall be comprised of six (6) Copyright Alerts, except that a Participating ISP may elect to send a single Educational Step Copyright Alert (as defined in Section 4(G)(i) below). However, to give an affected Subscriber time to review each Copyright Alert pertaining to such Subscriber’s account and to take appropriate steps to avoid receipt of further Copyright Alerts, a Participating ISP and its Subscriber will be afforded a grace period of seven (7) calendar days after the transmission of any Copyright Alert before any additional Copyright Alerts will be directed to the account holder (the “Grace Period”). The same Grace Period shall apply following the sending of a Mitigation Measure Copyright Alert (as described in Section 4(G)(iii) and (iv) below) and during the pendency of any review requested by a Subscriber following the receipt of either such Copyright Alert. During such Grace Period, any further ISP Notices received by the Participating ISP that the Participating ISP determines to be associated with the applicable Subscriber’s account will be handled as described in sub-paragraphs (i), (ii), (iii), and (iv) below.

Each Participating ISP shall use commercially reasonable efforts to develop a Copyright Alert Program in accordance with this Section 4(G), and shall work in good faith to complete all technical development work necessary for implementation of its Copyright Alert Program by a target launch date set forth in the applicable Implementation Agreement (each Participating ISP’s target launch date referred to herein as its “Copyright Alert Program Launch Date”).

Each Participating ISP's Copyright Alert Program shall be substantially similar to the following four (4) step sequential framework, which shall include an educational step (the "Initial Educational Step"), an acknowledgement step (the "Acknowledgement Step"), a mitigation measures step (the "Mitigation Measures Step"), and a post mitigation measures step (the "Post Mitigation Measures Step") as further described below. Under this framework, each Participating ISP will send Copyright Alerts with escalating warning language to Subscribers who are the subject of continuing ISP Notices. Specifically, each Participating ISP (1) shall send the Subscriber up to two (2) Copyright Alerts during the Initial Educational Step; (2) shall send two (2) more Copyright Alerts during the Acknowledgement Step; (3) shall send one (1) Mitigation Measure Copyright Alert (as defined in Section 4(G)(iii) below) during the Mitigation Measures Step and shall apply the specified Mitigation Measure (as defined in Section 4(G)(iii) below), subject to the Subscriber's right to challenge (or the Participating ISP's discretion to waive) the Copyright Alert(s) at this step; and (4) during the Post Mitigation Measures Step, shall send one (1) Mitigation Measure Copyright Alert and shall apply the specified Mitigation Measure, and may, at the Participating ISP's sole discretion, send additional Mitigation Measure Copyright Alerts and apply additional Mitigation Measures, subject to the Subscriber's right to challenge Copyright Alerts at this step.

Each Participating ISP's Copyright Alert Program shall follow the following format:

- (i) Initial Educational Step: Upon receipt of an ISP Notice associated with a Subscriber's account and taking into account the parameters of the Grace Period (if applicable), the Participating ISP shall direct a Copyright Alert to the account holder (an "Educational Step Copyright Alert"). The Educational Step Copyright Alert shall notify the Subscriber of receipt of an ISP Notice alleging P2P Online Infringement and shall include, at a minimum, the information contained in the ISP Notice regarding the alleged infringement and shall inform the Subscriber that: (a) copyright infringement is illegal as well as a violation of the Participating ISP's AUP or TOS, (b) users of the Subscriber's account must not infringe copyrighted works, (c) there are lawful methods of obtaining copyrighted works, (d) continuing and subsequent receipt of Copyright Alerts may result in the Participating ISP taking action by the application of Mitigation Measures, (e) in addition to these Mitigation Measures, the Participating ISP may also adopt, in appropriate circumstances, those measures specifically authorized by section 512 of the DMCA and/or actions specifically provided for in the Participating ISP's AUP and/or

FINAL
7/6/2011

TOS including temporary suspension or termination,¹⁷ (f) the Subscriber will have an opportunity to challenge any Copyright Alerts associated with the Subscriber's account before a Mitigation Measure is applied and may therefore wish to preserve records or information that could be used to show that the Subscriber's conduct was non-infringing, and (g) additional information regarding the Copyright Alert program may be found at CCT's web site. The number of Educational Step Copyright Alerts shall be at the discretion of the Participating ISP, not to exceed two (2) Copyright Alerts per Subscriber account, taking into account the parameters of the Grace Period. The second Educational Step Copyright Alert shall note specifically that it is in fact the Subscriber's second Educational Step Copyright Alert.

If the Participating ISP receives one (1) or more additional ISP Notices attributable to such Subscriber's account during the Grace Period associated with one of the Educational Step Copyright Alerts, the Participating ISP may at its discretion emphasize the educational and warning nature of its Copyright Alert Program by directing to the account holder additional Copyright Alerts that are similar in style to the Educational Step Copyright Alert. Such supplemental Copyright Alerts sent during the Grace Period shall not count toward the limit of two (2) Educational Step Copyright Alerts.

- (ii) Acknowledgement Step: At the Acknowledgement Step, upon receipt of further ISP Notices determined to be associated with a Subscriber's account and taking into account the parameters of the Grace Period, the Participating ISP shall direct two (2) Copyright

¹⁷ The Parties acknowledge and agree that the limitations on ISP liability under the DMCA are conditioned on an ISP's adoption and reasonable implementation of a policy that provides for the termination in appropriate circumstances of subscribers and account holders who are repeat infringers ("DMCA Termination Policy"). Notwithstanding the foregoing, (1) this Agreement does not and is not intended to create any obligation on a Participating ISP to adopt, implement, enforce, or otherwise take any action in furtherance of a DMCA Termination Policy; (2) the adoption, implementation, enforcement, or other action in furtherance of a DMCA Termination Policy is not part of any step of the Copyright Alert program or enforceable under this Agreement; and (3) entering into this Agreement is not, by itself, intended to address whether a Participating ISP has adopted and reasonably implemented a DMCA Termination Policy. This Agreement does not and is not intended to establish any legal inference regarding any ISP that does not participate in the Copyright Alert program or to address whether or not any ISP has adopted and reasonably implemented a DMCA Termination Policy. All references in this Agreement to the possibility of termination of a subscriber account are intended solely as an informational element of the Copyright Alerts required by the Copyright Alert program.

FINAL
7/6/2011

Alerts to the account holder that, as further described below, will require acknowledgement of receipt (but not require the user to acknowledge participation in any allegedly infringing activity) (each such Copyright Alert an “Acknowledgement Step Copyright Alert”). Each such Acknowledgement Step Copyright Alert shall state that the Subscriber, by acknowledging the notice, agrees immediately to cease, and/or agrees to instruct other users of the Subscriber’s account to cease infringing conduct, if any exists. Each such Copyright Alert shall also state that, upon receipt of lawful process requiring production of records or pursuant to a qualifying claim that the Subscriber has made via the Independent Review Program (as defined in Section 4(H) below and Attachment C hereto), the Participating ISP may provide relevant identifying information about the Subscriber and the Subscriber’s infringing conduct to third parties, including Content Owner Representatives or their agents and law enforcement agencies.

The mechanism provided for the Subscriber to acknowledge an Acknowledgement Step Copyright Alert may be in the form of (a) a temporary landing page to which the Subscriber’s browser is directed prior to permitting general access to the Internet (“Landing Page”) that shall state that the Subscriber has received prior warnings regarding P2P Online Infringement, and shall require the user of the Subscriber’s account to acknowledge receipt by clicking through the page prior to accessing additional web pages, (b) a “pop-up” notice which shall be designed to persist until the user of the Subscriber’s account acknowledges receipt by clicking through the pop-up notice, or (c) such other format as determined in the Participating ISP’s reasonable judgment which shall require acknowledgement of receipt of the Acknowledgement Step Copyright Alert.

If the Participating ISP receives one (1) or more additional ISP Notices attributable to such Subscriber’s account during the Grace Period associated with one of the Acknowledgement Step Copyright Alerts, the Participating ISP may at its discretion emphasize the educational and warning nature of its Copyright Alert Program by directing to the account holder additional Copyright Alerts that are similar in style to the Educational Step Copyright Alert or the Acknowledgement Step Copyright Alert. Such supplemental Copyright Alerts sent during the Grace Period shall not count toward the limit of two (2) Acknowledgement Step Copyright Alerts.

- (iii) Mitigation Measures Step: At the Mitigation Measures Step, upon receipt of further ISP Notices determined to be associated with a

FINAL
7/6/2011

Subscriber's account and taking into account the parameters of the Grace Period, the Participating ISP shall direct a Copyright Alert (a "Mitigation Measure Copyright Alert") to the account holder that (a) requires acknowledgement of receipt of the Copyright Alert as described in the Acknowledgement Step, (b) shall state that the Subscriber has received prior warnings regarding alleged P2P Online Infringement, and (c) informs the Subscriber that, per the Participating ISP's AUP and/or TOS and as set forth in prior Copyright Alerts, additional consequences shall be applied upon the Subscriber's account as described more fully in this subparagraph (iii) (each such measure a "Mitigation Measure").

The Mitigation Measure Copyright Alert shall set forth the specific Mitigation Measure to be applied and shall inform the Subscriber that, unless the Subscriber has requested review under one of the dispute resolution mechanisms specified in Section 4(H) below, the Participating ISP shall apply the selected Mitigation Measure after the expiration of a notice period of ten (10) business days or fourteen (14) calendar days from the time the Mitigation Measure Copyright Alert is delivered. The term of the notice period (*i.e.*, ten (10) business days or fourteen (14) calendar days) shall be at the Participating ISP's discretion. If no review is requested by the Subscriber, the Participating ISP shall apply the specified Mitigation Measure on the applicable Subscriber's Internet access service account after such ten (10) business day or fourteen (14) calendar day period has expired.

The Mitigation Measure applied at the Mitigation Measures Step shall be one of the following, determined by the Participating ISP and applied in a manner reasonably calculated, in the Participating ISP's reasonable discretion, to help deter P2P Online Infringement: (a) temporary reduction in uploading and/or downloading transmission speeds; (b) temporary step-down in the Subscriber's service tier to (1) the lowest tier of Internet access service above dial-up service that the Participating ISP makes widely available to residential customers in the Subscriber's community, or (2) an alternative bandwidth throughput rate low enough to significantly impact a Subscriber's broadband Internet access service (*e.g.*, 256 - 640 kbps); (c) temporary redirection to a Landing Page until the Subscriber contacts the Participating ISP to discuss with it the Copyright Alerts; (d) temporary restriction of the Subscriber's Internet access for some reasonable period of time as determined in the Participating ISP's discretion; (e) temporary redirection to a Landing Page for completion of a meaningful educational instruction on copyright; or (f) such other temporary Mitigation Measure as may be applied by the Participating ISP in its

discretion that is designed to be comparable to those Mitigation Measures described above. Participating ISPs shall not be obligated to apply a Mitigation Measure that knowingly disables or is reasonably likely to disable a Subscriber's access to any IP voice service (including over-the-top IP voice service), e-mail account, or any security service, multichannel video programming distribution service or guide, or health service (such as home security or medical monitoring) while a Mitigation Measure is in effect.

The foregoing provisions notwithstanding, the Participating ISP will retain the discretion, on a per Subscriber account basis, (a) to decide whether appropriate circumstances exist to waive such Mitigation Measure (a "Waiver"), provided that the Participating ISP will only issue one (1) such Waiver per Subscriber account, or (b) instead of applying the Mitigation Measure specified in the Mitigation Measure Copyright Alert, to apply an alternate Mitigation Measure on the Subscriber's Internet access service account and to so inform the Subscriber.

If the Participating ISP elects to use a Waiver, the Participating ISP will direct to the account holder a final warning (a "Fifth Warning Copyright Alert") that will contain each of the elements contained in the Mitigation Measure Copyright Alert as described in this Section 4(G)(iii) and will inform the Subscriber that, in the event that the Participating ISP receives one (1) or more further ISP Notices from a Content Owner Representative, the Subscriber's Internet access service account will be subject to a Mitigation Measure per the Participating ISP's AUP and/or TOS and as set forth in prior Copyright Alerts, unless the Subscriber requests review under one of the dispute resolution mechanisms specified in Section 4(H). If, after the expiration of the Grace Period following issuance of a Fifth Warning Copyright Alert, a Participating ISP receives one (1) or more further ISP Notices determined to be related to a Subscriber's account for which a Waiver has been granted, the Participating ISP will proceed with the transmission of a Mitigation Measure Copyright Alert and the associated activities described above.

- (iv) Post Mitigation Measures Step: In the event that a Participating ISP receives a further ISP Notice determined to be associated with a Subscriber's account after a Mitigation Measure has been applied on that Subscriber's account, the Participating ISP shall direct a further Mitigation Measure Copyright Alert to the account holder and after ten (10) business days or fourteen (14) calendar days, as applicable, either re-apply the previous Mitigation Measure or

apply a different Mitigation Measure, unless the Subscriber requests review under one of the dispute resolution mechanisms specified in [Section 4\(H\)](#). The Mitigation Measure Copyright Alert at this step shall also inform the Subscriber that the Subscriber may be subject to a lawsuit for copyright infringement by the Copyright Owners and that continued infringement may, in appropriate circumstances, result in the imposition of action consistent with section 512 of the DMCA and/or actions specifically provided for in the Participating ISP's AUP and/or TOS including temporary suspension or termination. Upon completion of the Post Mitigation Measures Step, a Participating ISP may elect voluntarily to continue forwarding ISP Notices received for that Subscriber account, but is not obligated to do so. The Participating ISP will, however, continue to track and report the number of ISP Notices the Participating ISP receives for that Subscriber's account, so that information is available to a Content Owner Representative if it elects to initiate a copyright infringement action against that Subscriber.

- (v) Reset: If a Participating ISP does not receive an ISP Notice relating to a Subscriber's account within twelve (12) months from the date the Participating ISP last received an ISP Notice relating to that same Subscriber's account, (a) the next ISP Notice associated with that Subscriber's account shall be treated as the first such ISP Notice under the provisions of this Copyright Alert Program and the Subscriber may be afforded an additional Waiver as set forth in [Section 4\(G\)\(iii\)](#) above; and (b) the Participating ISP may expunge all prior ISP Notices and Copyright Alerts from the Subscriber's account.
- (vi) Transmission of Copyright Alerts to Subscribers: Copyright Alerts should be directed by the Participating ISP to the account holder by means that are designed to ensure prompt receipt (*e.g.*, via email, physical mail, auto-dialer notification, ISP account management tool pop-ups requiring user click through, electronic or voice communications with Subscribers or such other means of delivery as the Participating ISP deems commercially practicable), and the Participating ISP shall design such Copyright Alerts in a manner reasonably calculated, in the Participating ISP's discretion, to be received by the Subscriber. Each Copyright Alert after the initial Educational Step Copyright Alert will include the educational and general information required in the Educational Step Copyright Alert and in any other Copyright Alerts that were forwarded to the Subscriber after the Educational Step, together with a summary of the pertinent information regarding the alleged P2P Online Infringement related to prior ISP Notices or a link or

other mechanism by which the Subscriber can access or obtain such information. Each Participating ISP will provide the form of its Copyright Alerts to the Independent Expert as part of the Independent Expert's review of each Participating ISP's Methodology, and will in good faith consider any suggestions from the Independent Expert.

- (vii) Notification of Ability to Request Review: Copyright Alerts directed to account holders at the Mitigation Measures Step and the Post Mitigation Measures Step shall inform the Subscriber of the Subscriber's ability to request review within ten (10) business days or fourteen (14) calendar days, as applicable, under one of the dispute resolution mechanisms described in Section 4(H). If the Subscriber requests such review, the Participating ISP shall, upon receiving notice of the request for such review and pending a final decision via the chosen dispute resolution mechanism, defer taking any further action under its Copyright Alert Program.

H. Independent Review Program

(i) A Subscriber may seek review of a Mitigation Measure Copyright Alert via the dispute resolution program set forth in Attachment C (the "Independent Review Program") or as otherwise permitted in the Participating ISP's AUP or TOS or as permitted by law, at the election of the Subscriber. The Independent Review Program shall allow for the Subscriber to remain anonymous to the Content Owner Representatives and the members of the Participating Content Owners Group, except in cases where the Subscriber elects a defense in which the Subscriber's identity will be disclosed. The decision from the Independent Review Program shall be binding on the Parties solely for purposes of the Notice Process and the affected Copyright Alert Program but shall have no force or effect beyond the Notice Process and the affected Copyright Alert Program, and shall not be deemed to adjudicate any rights outside of this limited context. In any judicial proceeding between a Subscriber and a Copyright Owner concerning subject matter that is or has been the subject of the Independent Review Program, as provided in the procedures governing the Independent Review Program, neither the Subscriber nor the Copyright Owner shall seek to enter into evidence, or otherwise refer to or cite, either the fact of the Independent Review or any outcome of the Independent Review.

(ii) The costs of establishing and administering the Independent Review Program shall be borne fifty percent (50%) by the Participating Content Owners Group and fifty percent (50%) by the Participating ISPs.

I. Generation of Monthly Reports

Within ten (10) business days of the end of each calendar month during the term of this Agreement, each Participating ISP shall provide reporting of non-personally

identifiable information to the Content Owner Representatives identifying, on an anonymized basis and in the format set forth in the Participating ISP's Implementation Agreement, information about those Subscribers who have received Copyright Alert(s) during the applicable calendar month and the total number of alleged P2P Online Infringements by each such Subscriber. Such reporting may be done via Automated Copyright Notification System ("ACNS") standards or other available methods as mutually agreed in the Participating ISP's Implementation Agreement. The Parties may not (i) use or disclose such data to governmental entities (absent lawful process) or other third parties, unless prior approval for each such use or disclosure is received from a majority of the CCI Executive Committee and the data is disclosed only on an aggregated, anonymized basis, or (ii) use such reports or any of the data that is included in or may be extrapolated from such reports to attempt to obtain the identity of a Subscriber; except that (1) the Parties may use the reports or data to analyze the effectiveness of the Copyright Alert program; and (2) the Content Owner Representatives or any other member of the Participating Content Owners Group may use such reports or data as the basis for seeking a Subscriber's identity through a subpoena or order or other lawful process. For the avoidance of doubt, the Parties agree that the Content Owner Representatives may share such reports with the other members of the Participating Content Owners Group, provided such Parties agree to abide by the limitations set forth in this Section 4(I).

5. Technical Operations; Implementation Agreements

A. The Content Owner Representatives and each Participating ISP (and the members of the Participating Content Owners Group, as necessary) will work together in good faith to establish and agree upon standardized forms and procedures for a Notice Process (for example, by incorporating ACNS or other mutually agreeable standard(s), and endeavoring to include identification of Methodologies used, if practical). The foregoing sentence notwithstanding, the Parties acknowledge that a common interface between the Content Owner Representatives and the Participating ISPs may not be technically or financially practical. The Content Owner Representatives and each Participating ISP (and the members of the Participating Content Owners Group, as necessary) will document the standards contemplated in this Section 5(A), notice volumes, and other pertinent details concerning the technical operation of the Notice Process and Copyright Alert Program between the Content Owner Representatives and the applicable Participating ISP in an Implementation Agreement. The Content Owner Representatives and the Participating ISPs shall agree to a form of the Implementation Agreement, including the terms and conditions of such agreement, that shall be used by all of the Participating ISPs. Each Participating ISP and the Content Owner Representatives (and the members of the Participating Content Owners Group, as necessary) shall make reasonable efforts to execute their Implementation Agreement no later than three (3) months after the Effective Date (as defined in Section 8(A) below).

B. Reserved.

C. The MPAA Group and the RIAA Group will allocate the number of ISP Notices that each shall be entitled to send to each Participating ISP per month (i) on behalf of their members, the RIAA Group's members' distributed labels, and those entities set forth in Attachment D hereto; and (ii) on behalf of independent record labels and film production companies that are members of the American Association of Independent Music ("A2IM") and the Independent Film and Television Alliance ("IFTA"), respectively (collectively, the "Independent Content Owners"), provided that IFTA, A2IM, and the Independent Content Owners (as applicable) agree to be bound by written agreement (for so long as such agreement remains in effect) to the terms set forth in Sections 4(C), 4(D), 4(H)(i), 4(I), 5(A), 5(C), 6, 7, 8, 9(E), 9(F), and 10 of this Agreement that apply to all members of the Participating Content Owners Group (collectively or individually) and certain designated provisions of each Participating ISP's Implementation Agreement as set forth therein.

D. Each Participating ISP may temporarily cease processing ISP Notices or reduce the number of ISP Notices being processed if, in the sole discretion of the Participating ISP, (i) the Participating ISP receives more ISP Notices than its business processes and systems can reasonably address, (ii) the Participating ISP receives more calls from Subscribers regarding Copyright Alerts than its designated customer service representatives can reasonably address (taking into account the other demands on Participating ISP customer service representatives for unrelated purposes), or (iii) other demands on the Participating ISP's business processes and systems, such as requests from law enforcement, must be given precedence. If the Participating ISP temporarily ceases processing ISP Notices for any of the foregoing reasons, the Participating ISP shall promptly notify the Content Owner Representatives, subject to any limitations on such notice as may be imposed in law or regulation, and shall work cooperatively with the Content Owner Representatives and, if agreed by all affected Parties, the Independent Expert, to resolve any issues relating to the over-provisioning of ISP Notices.

6. Consent to Receive Notices

A. Entry into this Agreement by a Participating ISP shall constitute consent by that Participating ISP to receive ISP Notices from the Content Owner Representatives (or their service providers) on behalf of the Participating Content Owners Group, those entities set forth in Attachment D (as such attachment may be amended from time to time) (or in the case of the RIAA Group, on behalf of the RIAA Group's members' distributed labels), and the Independent Content Owners upon implementation by the Participating ISP of its Copyright Alert Program, subject to all of the terms and limitations set forth in this Agreement and the Participating ISP's Implementation Agreement. The members of the Participating Content Owners Group may change from time to time upon mutual written agreement of the Parties, provided that MPAA and RIAA shall remain Parties to this Agreement and, provided further, that in no event shall such changes increase the notice volumes applicable to each Participating ISP under this Agreement and each Participating ISP's Implementation Agreement, unless this Agreement or the Participating ISP's Implementation Agreement is modified with the

written consent of the Participating ISP to increase the number of ISP Notices that may be sent. Nothing in this Agreement shall require a Participating ISP to accept notices from any third party or restrain it from doing so. No ISP Notices or other notices of P2P Online Infringement directed to Subscribers shall be sent to the Participating ISP by or on behalf of the members of the Participating Content Owners Group, the Independent Content Owners, and those entities set forth in Attachment D of this Agreement (as such attachment may be amended from time to time) (or in the case of the RIAA Group, on behalf of the RIAA Group's members' distributed labels) except pursuant to this Agreement and the Participating ISP's Implementation Agreement.

B. Prior to the Copyright Alert Program launch date for the applicable Participating ISP, such Participating ISP shall continue to process notices concerning P2P Online Infringement in accordance with such Participating ISP's then current policies or practices or, if applicable, agreements with any member of the Participating Content Owners Group.

7. Force Majeure

No Party shall be liable to any other Party for any delay, failure in performance, loss or damage due to fire, explosion, interruption of power supplies, earthquake, flood, the elements, strike, embargo, labor disputes, failure of public transit or other public infrastructure, acts of civil or military authority, war, terrorism, acts of God, acts of the public enemy, acts or omissions of carriers or suppliers, acts of regulatory or governmental agencies, or other causes beyond such Party's reasonable control, whether or not similar to the foregoing and whether or not the Parties contemplate such circumstances at the time of entering into this Agreement.

8. Term; Withdrawal

A. This Agreement shall become effective upon the date all of the Parties have executed this Agreement (the "Effective Date"). This Agreement shall remain in effect for a period of four (4) years following the Effective Date.

B. Any Party may withdraw as a Party from this Agreement prior to its expiration (i) if such Party reasonably determines that continued participation in this Agreement is not technically, commercially, operationally or otherwise practical; (ii) if such Party is subject to a complaint before any administrative agency, court, or other governmental entity challenging the lawfulness of the Copyright Alert program, a Participating ISP's Copyright Alert Program, the Agreement, or an Implementation Agreement to which it is a party or any conduct taken under such agreements or programs; (iii) if another Party to this Agreement is subject to a complaint before any administrative agency, court, or other governmental entity challenging the lawfulness of the Copyright Alert program, a Participating ISP's Copyright Alert Program, or the Agreement or any conduct taken under such agreements or programs; or (iv) if a government entity enacts or establishes a government-sponsored program or judicial, administrative, or executive process concerning P2P Online Infringement that imposes

materially different obligations than those set forth in this Agreement.

9. Records and Evaluation

A. Consistent with its general policies and business practices for retaining Internet access service subscriber records, each Participating ISP agrees to keep reasonable records pertaining to its Copyright Alert Program. Each Participating ISP also agrees to use reasonable efforts to provide semi-annual reports to CCI of the results of its Copyright Alert Program, which shall include, in an aggregated, anonymized form, non-personally identifiable information regarding the ISP Notices received and Copyright Alerts sent and such other aggregated, anonymized data as the Participating ISPs may from time to time agree to provide.

B. Consistent with its general policies and business practices for retaining records regarding Online Infringement, each Content Owner Representative agrees to keep reasonable records pertaining to its participation in the Notice Process under this Agreement including records of the Methodology(ies) currently and previously in use and the effective date(s) of such use. Each Content Owner Representative agrees to use reasonable efforts to provide semi-annual reports to CCI of the results of its Notice Process, which shall include, in an aggregated, anonymized form, non-personally identifiable information regarding the ISP Notices sent to the Participating ISPs concerning activities relating to P2P Online Infringement by the Participating ISPs' Subscribers and such other aggregated, anonymized data as the Content Owner Representatives may from time to time agree to provide. Such reports shall be in a form to be determined by each Content Owner Representative in its discretion.

C. CCI shall keep confidential all records and data relating to the Notice Process and Copyright Alert Programs. None of the records and data relating to the Notice Process and Copyright Alert Programs shall be made publicly available by CCI without prior approval by a majority of the Executive Committee.

D. CCI shall review on an annual basis, beginning on the twelve (12) month anniversary of the Effective Date and occurring each subsequent year thereafter on the anniversary of the Effective Date, the number of Copyright Alerts sent by the Participating ISPs to each Subscriber's account at each step of the Copyright Alert Programs. Based on the information that CCI receives from the Participating ISPs and the Content Owner Representatives, pursuant to Sections 9(A) and 9(B), in order to assess the effectiveness of the Copyright Alert program, CCI shall assess among other things (i) the proportion of Subscribers of each Participating ISP who ceased receiving Copyright Alerts at each step of the Copyright Alert Program; (ii) the average overall number of P2P Online Infringements detected for Content Owner Representative assets over a weekly or monthly period (in general, and by Participating ISP); (iii) the number of ISP Notices received and the number of corresponding Copyright Alerts sent; (iv) the number and percentage of individual Subscribers who, after receiving one (1) or more Copyright Alerts, did not receive additional Copyright Alerts corresponding to their accounts (in general, and by Participating ISP); (v) the number of Subscribers who

requested a review under the Independent Review Program, and at what step they requested it; and (vi) the number and percentage of Independent Reviews which resulted in a decision in favor of the Subscriber – and why such decisions were made. As part of its annual review, CCI shall also examine whether Copyright Alerts are successfully reaching account holders. The Parties shall consider in good faith any recommendations made by CCI resulting from such review and assessment.

E. The Content Owner Representatives, those members of the Participating Content Owners Group and Independent Content Owners selected by the Content Owner Representatives, and the Participating ISPs shall establish a working group under the auspices of CCI, which will consist of appropriate representatives of each Party, who will meet regularly (at least quarterly during the eighteen (18) months following the Effective Date and then at least semi-annually thereafter) to assist in the initiation and implementation of this Agreement, assess its ongoing operation, and thereafter recommend to the Parties on a non-binding basis any suggested amendments to this Agreement to improve its scope or effectiveness. The working group may consult with the Independent Expert as appropriate.

F. CCI shall maintain any reports or other information provided by any Party hereunder in the strictest confidence and shall not disclose such reports or information to any third party or any Party other than the Party which originated the report or information, absent written consent from the originating Party or as otherwise required by law. In the event CCI receives a subpoena or other legal process seeking the disclosure of such reports or information, CCI shall immediately notify the Party whose reports or information is subject to the subpoena or other legal process and provide such Party with the opportunity to seek a protective order or otherwise to oppose disclosure. If authorized by the Executive Committee, CCI shall also seek a protective order or oppose disclosure.

10. Miscellaneous

A. The Content Owner Representatives, the members of the Participating Content Owners Group, the Independent Content Owners, and the Participating ISPs appreciate that alternatives to obtaining and sharing music, movies, and other copyright-protected works by means other than unlawful digital distribution should be encouraged. The Content Owner Representatives will undertake appropriate efforts to ensure the widespread communication of lawful alternatives for consuming content through online distribution methods and encourage the public to utilize these alternatives. Each Participating ISP will, via Copyright Alerts and other avenues, encourage Subscribers to seek legal alternatives to obtain copyrighted materials.

B. This Agreement shall be governed by the laws of the State of New York, without regard to any conflict of law principles. The Parties hereby consent to the exclusive jurisdiction of any state or federal court sitting in the Borough of Manhattan, New York over any judicial proceedings arising out of or related to this Agreement and agree that all claims in respect of such judicial proceedings shall be heard in such state or

federal courts in the Borough of Manhattan, New York. The Parties further agree that any such proceeding shall be filed in the United States District Court for the Southern District of New York if such court has jurisdiction over the proceeding.

C. Nothing expressed or implied in this Agreement is intended, or may be construed, to confer upon or give any person or entity other than the Parties hereto any rights or remedies hereunder. This Agreement may only be amended by written agreement signed by all Parties hereto.

D. This Agreement is subject to any laws or regulations that may be enacted by Congress or adopted by the Federal Communications Commission (or any other federal or state administrative, regulatory or legislative body). If any future law or regulation makes unlawful any provision of this Agreement, that provision will be severed from this Agreement. If any Participating ISP, Content Owner Representative, or member of the Participating Content Owners Group reasonably concludes that such invalidated provision is material to the Agreement or that severing such provision is otherwise impracticable, such Party may immediately terminate its participation in the Agreement.

E. Headings herein are for convenience of reference only and shall in no way affect interpretation of this Agreement.

F. This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes all proposals, oral or written, all negotiations, conversations or discussions, and all past dealings or industry customs between the parties relating to the subject matter hereof.

G. This Agreement may be executed in two or more counterparts and duplicate originals, each of which will be deemed an original and all of which together will constitute one and the same instrument. An executed copy of this Agreement transmitted via facsimile or email by the executing party and received via facsimile or email by the other party shall have the same legal force as an executed original version of this Agreement.

H. The waiver by a party of any breach of this Agreement by the other party in a particular instance shall not operate as a waiver of subsequent breaches of the same or different kind. Failure of a party to exercise any rights under this Agreement in a particular instance shall not operate as a waiver of such party's right to exercise the same or different rights in subsequent instances.

[The rest of this page is intentionally left blank.]

FINAL
7/6/2011

Agreed as of July 6, 2011:

The Motion Picture Association of America, Inc.

By: Dan Robbins
Name: _____
Title: SVP & Associate GC

The Recording Industry Association of America, Inc.

By: _____
Name: _____
Title: _____

Walt Disney Studios Motion Pictures

By: _____
Name: _____
Title: _____

Paramount Pictures Corporation

By: _____
Name: _____
Title: _____

Sony Pictures Entertainment Inc.

By: _____
Name: _____
Title: _____

Twentieth Century Fox Film Corporation

By: _____
Name: _____
Title: _____

Universal City Studios LLC

By: _____
Name: _____
Title: _____

Warner Bros. Entertainment Inc.

Agreed as of July 6, 2011:

The Motion Picture Association of America, Inc.

By: _____
Name: _____
Title: _____

The Recording Industry Association of America, Inc.

By: Steven M. Marks
Name: Steven M. Marks
Title: EVP & General Counsel

Walt Disney Studios Motion Pictures

By: _____
Name: _____
Title: _____

Paramount Pictures Corporation

By: _____
Name: _____
Title: _____

Sony Pictures Entertainment Inc.

By: _____
Name: _____
Title: _____

Twentieth Century Fox Film Corporation

By: _____
Name: _____
Title: _____

Universal City Studios LLC

By: _____
Name: _____
Title: _____

FINAL
7/6/2011

Agreed as of July 6, 2011:

The Motion Picture Association of America, Inc.

By: _____
Name: _____
Title: _____

The Recording Industry Association of America, Inc.

By: _____
Name: _____
Title: _____

Walt Disney Studios Motion Pictures

By: 
Name: ALAN BRAVERMAN
Title: EXEC. V-P & GENERAL COUNSEL

Paramount Pictures Corporation

By: _____
Name: _____
Title: _____

Sony Pictures Entertainment Inc.

By: _____
Name: _____
Title: _____

Twentieth Century Fox Film Corporation

By: _____
Name: _____
Title: _____

Universal City Studios LLC

By: _____
Name: _____
Title: _____

Warner Bros. Entertainment Inc.

FINAL
7/6/2011

Agreed as of July 6, 2011:

The Motion Picture Association of America, Inc.

By: _____
Name: _____
Title: _____

The Recording Industry Association of America, Inc.

By: _____
Name: _____
Title: _____

Walt Disney Studios Motion Pictures

By: _____
Name: _____
Title: _____

Paramount Pictures Corporation

By:  _____
Name: MICHAEL D. FRICKLAS
Title: EVD

Sony Pictures Entertainment Inc.

By: _____
Name: _____
Title: _____

Twentieth Century Fox Film Corporation

By: _____
Name: _____
Title: _____

Universal City Studios LLC

By: _____
Name: _____
Title: _____

Warner Bros. Entertainment Inc.

FINAL
7/6/2011

Agreed as of July 6, 2011:

The Motion Picture Association of America, Inc.

By: _____
Name: _____
Title: _____

The Recording Industry Association of America, Inc.

By: _____
Name: _____
Title: _____

Walt Disney Studios Motion Pictures

By: _____
Name: _____
Title: _____

Paramount Pictures Corporation

By: _____
Name: _____
Title: _____

Sony Pictures Entertainment Inc.

By: 
Name: Leah weil
Title: Sr. EVP / General Counsel

Twentieth Century Fox Film Corporation

By: _____
Name: _____
Title: _____

Universal City Studios LLC

By: _____
Name: _____
Title: _____

Warner Bros. Entertainment Inc.

Agreed as of July 6, 2011:

The Motion Picture Association of America, Inc.

By: _____
Name: _____
Title: _____

The Recording Industry Association of America, Inc.

By: _____
Name: _____
Title: _____

Walt Disney Studios Motion Pictures

By: _____
Name: _____
Title: _____

Paramount Pictures Corporation

By: _____
Name: _____
Title: _____

Sony Pictures Entertainment Inc.

By: _____
Name: _____
Title: _____

Twentieth Century Fox Film Corporation

By: Ronald C. Wheeler/Sydneyberg
Name: Ronald C. Wheeler
Title: Assistant Secretary

Universal City Studios LLC

By: _____
Name: _____
Title: _____

Warner Bros. Entertainment Inc.

FINAL
7/6/2011

Agreed as of July 6, 2011:

The Motion Picture Association of America, Inc.

By: _____
Name: _____
Title: _____

The Recording Industry Association of America, Inc.

By: _____
Name: _____
Title: _____

Walt Disney Studios Motion Pictures

By: _____
Name: _____
Title: _____

Paramount Pictures Corporation

By: _____
Name: _____
Title: _____

Sony Pictures Entertainment Inc.

By: _____
Name: _____
Title: _____

Twentieth Century Fox Film Corporation

By: _____
Name: _____
Title: _____

NBCUniversal Media, LLC

By: 
Name: RICHARD COTTON
Title: Executive VP at Hand Counsel

Warner Bros. Entertainment Inc.

FINAL
7/6/2011

By: 
Name: John Rogovin
Title: EVP & General Counsel

UMG Recordings, Inc.

By: _____
Name: _____
Title: _____

Warner Music Group

By: _____
Name: _____
Title: _____

Sony Music Entertainment

By: _____
Name: _____
Title: _____

EMI Music North America

By: _____
Name: _____
Title: _____

SBC Internet Services, Inc., BellSouth Telecommunications, Inc., Southwestern Bell Telephone Company, Pacific Bell Telephone Company, Illinois Bell Telephone Company, Indiana Bell Telephone Company, Incorporated, Michigan Bell Telephone Company, Nevada Bell Telephone Company, The Ohio Bell Telephone Company, Wisconsin Bell, Inc., The Southern New England Telephone Company, and BellSouth Telecommunications, Inc. (the AT&T Inc. companies)

By: _____
Name: _____
Title: _____

Verizon Online LLC, Verizon Online LLC – Maryland, and Verizon Online Pennsylvania Partnership (the Verizon companies)

By: _____
Name: _____
Title: _____

FINAL
7/6/2011

Warner Bros. Entertainment Inc.

By: _____
Name: _____
Title: _____

UMG Recordings, Inc.

By:  _____
Name: Jeffrey Horvath
Title: General Counsel, EUP Business & Legal Affairs

Warner Music Group

By: _____
Name: _____
Title: _____

Sony Music Entertainment

By: _____
Name: _____
Title: _____

EMI Music North America

By: _____
Name: _____
Title: _____

SBC Internet Services, Inc., BellSouth Telecommunications, Inc., Southwestern Bell Telephone Company, Pacific Bell Telephone Company, Illinois Bell Telephone Company, Indiana Bell Telephone Company, Incorporated, Michigan Bell Telephone Company, Nevada Bell Telephone Company, The Ohio Bell Telephone Company, Wisconsin Bell, Inc., The Southern New England Telephone Company, and BellSouth Telecommunications, Inc. (the AT&T Inc. companies)

By: _____
Name: _____
Title: _____

FINAL
7/6/2011

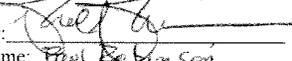
Warner Bros. Entertainment Inc.

By: _____
Name: _____
Title: _____

UMG Recordings, Inc.

By: _____
Name: _____
Title: _____

Warner Music Group Corp.

By: 
Name: Paul Robinson
Title: VP and General Counsel

Sony Music Entertainment

By: _____
Name: _____
Title: _____

EMI Music North America

By: _____
Name: _____
Title: _____

SBC Internet Services, Inc., BellSouth Telecommunications, Inc., Southwestern Bell Telephone Company, Pacific Bell Telephone Company, Illinois Bell Telephone Company, Indiana Bell Telephone Company, Incorporated, Michigan Bell Telephone Company, Nevada Bell Telephone Company, The Ohio Bell Telephone Company, Wisconsin Bell, Inc., The Southern New England Telephone Company, and BellSouth Telecommunications, Inc. (the AT&T Inc. companies)

By: _____
Name: _____
Title: _____

Warner Bros. Entertainment Inc.

By: _____
Name: _____
Title: _____

UMG Recordings, Inc.

By: _____
Name: _____
Title: _____

Warner Music Group

By: _____
Name: _____
Title: _____

Sony Music Entertainment

By: *[Signature]*
Name: *Tulie Swidler*
Title: *SVP, Business Affairs & General Counsel*

EMI Music North America

By: _____
Name: _____
Title: _____

SBC Internet Services, Inc., BellSouth Telecommunications, Inc., Southwestern Bell Telephone Company, Pacific Bell Telephone Company, Illinois Bell Telephone Company, Indiana Bell Telephone Company, Incorporated, Michigan Bell Telephone Company, Nevada Bell Telephone Company, The Ohio Bell Telephone Company, Wisconsin Bell, Inc., The Southern New England Telephone Company, and BellSouth Telecommunications, Inc. (the AT&T Inc. companies)

By: _____
Name: _____
Title: _____

**FINAL
7/6/2011**

Warner Bros. Entertainment Inc.

By: _____
Name: _____
Title: _____

UMG Recordings, Inc.

By: _____
Name: _____
Title: _____

Warner Music Group

By: _____
Name: _____
Title: _____

Sony Music Entertainment

By: _____
Name: _____
Title: _____

EMI Music North America

By: Paul Kahn
Name: PAUL KAHN
Title: CFO

SBC Internet Services, Inc., BellSouth Telecommunications, Inc., Southwestern Bell Telephone Company, Pacific Bell Telephone Company, Illinois Bell Telephone Company, Indiana Bell Telephone Company, Incorporated, Michigan Bell Telephone Company, Nevada Bell Telephone Company, The Ohio Bell Telephone Company, Wisconsin Bell, Inc., The Southern New England Telephone Company, and BellSouth Telecommunications, Inc. (the AT&T Inc. companies)

By: _____
Name: _____
Title: _____

FINAL
7/6/2011

Warner Bros. Entertainment Inc.

By: _____
Name: _____
Title: _____

UMG Recordings, Inc.

By: _____
Name: _____
Title: _____

Warner Music Group

By: _____
Name: _____
Title: _____

Sony Music Entertainment

By: _____
Name: _____
Title: _____

EMI Music North America

By: _____
Name: _____
Title: _____

SBC Internet Services, Inc., BellSouth Telecommunications, Inc., Southwestern Bell Telephone Company, Pacific Bell Telephone Company, Illinois Bell Telephone Company, Indiana Bell Telephone Company, Incorporated, Michigan Bell Telephone Company, Nevada Bell Telephone Company, The Ohio Bell Telephone Company, Wisconsin Bell, Inc., The Southern New England Telephone Company, and BellSouth Telecommunications, Inc. (the AT&T Inc. companies)

By: Wayne Watts
Name: Wayne Watts
Title: Sr. Exec Vice President & General Counsel
AT&T Inc.

FINAL
7/6/2011

Verizon Online LLC, Verizon Online LLC – Maryland, and Verizon Online
Pennsylvania Partnership (the Verizon companies)

By: Randal S. Mitch
Name: Randal S. Mitch
Title: EVP & General Counsel

Comcast Cable Communications Management, LLC

By: _____
Name: _____
Title: _____

CSC Holdings, LLC

By: _____
Name: _____
Title: _____

Time Warner Cable Inc.

By: _____
Name: _____
Title: _____

FINAL
7/6/2011

Verizon Online LLC, Verizon Online LLC – Maryland, and Verizon Online
Pennsylvania Partnership (the Verizon companies)

By: _____
Name: _____
Title: _____

Comcast Cable Communications Management, LLC

By: *Catherine Argiris*
Name: *CATHERINE ARGIRIS*
Title: *SVP GM Communications and Data Services*

CSC Holdings, LLC

By: _____
Name: _____
Title: _____

Time Warner Cable Inc.

By: _____
Name: _____
Title: _____

FINAL
7/6/2011

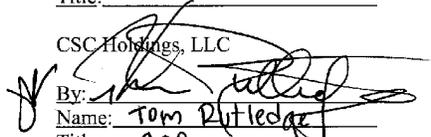
Verizon Online LLC, Verizon Online LLC – Maryland, and Verizon Online
Pennsylvania Partnership (the Verizon companies)

By: _____
Name: _____
Title: _____

Comcast Cable Communications Management, LLC

By: _____
Name: _____
Title: _____

CSC Holdings, LLC

By: 
Name: Tom Rutledge
Title: COO

Time Warner Cable Inc.

By: _____
Name: _____
Title: _____

FINAL
7/6/2011

Verizon Online LLC, Verizon Online LLC – Maryland, and Verizon Online
Pennsylvania Partnership (the Verizon companies)

By: _____
Name: _____
Title: _____

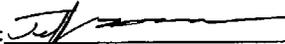
Comcast Cable Communications Management, LLC

By: _____
Name: _____
Title: _____

CSC Holdings, LLC

By: _____
Name: _____
Title: _____

Time Warner Cable Inc.

By: 
Name: JEFF ZARNEN
Title: SVP & DEPUTY GC

Attachment A – Participating ISPs

The Participating ISPs are the following: SBC Internet Services, Inc., BellSouth Telecommunications, Inc., Southwestern Bell Telephone Company, Pacific Bell Telephone Company, Illinois Bell Telephone Company, Indiana Bell Telephone Company, Incorporated, Michigan Bell Telephone Company, Nevada Bell Telephone Company, The Ohio Bell Telephone Company, Wisconsin Bell, Inc., The Southern New England Telephone Company, and BellSouth Telecommunications, Inc. (the AT&T Inc. companies); Verizon Online LLC, Verizon Online LLC – Maryland, and Verizon Online Pennsylvania Partnership (the Verizon companies); Comcast Cable Communications Management, LLC; CSC Holdings, LLC (solely with respect to its cable systems operating in New York, New Jersey, and Connecticut) (the Cablevision systems); and Time Warner Cable Inc.

Attachment B – Participating Content Owners Group

The members of the Participating Content Owners Group are the following:

1. MPAA and the following MPAA members: Walt Disney Studios Motion Pictures, Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corporation, Universal City Studios LLC, and Warner Bros. Entertainment Inc., and their successors and assigns.
2. RIAA and the following RIAA members: UMG Recordings, Inc., Warner Music Group, Sony Music Entertainment, and EMI Music North America, and their successors and assigns.

Attachment C – Independent Review Program

The Independent Review Program described below is intended to provide an alternative, fast, efficient and low-cost means for Subscribers and Copyright Owners to obtain independent resolution of genuine disputes that may occur in connection with the Copyright Alert program outlined in the Agreement. Its purpose is to provide a Subscriber with a non-exclusive procedure to seek review of Copyright Alerts associated with the Subscriber's account in the event a Mitigation Measure is about to be applied on the Subscriber's account.

The Independent Review process shall be just one avenue of appeal for Subscribers challenging such measure. This Independent Review process does not prevent Subscribers or Copyright Owners from addressing disputes through the courts, and that is the proper forum for addressing issues that are beyond the scope of this Independent Review process.

1. **Grounds for Independent Review**. Once a Subscriber has received a Copyright Alert stating that a Mitigation Measure is about to be applied, the Subscriber may request an Independent Review of that Copyright Alert and prior Copyright Alerts (as described in paragraph 4.1.4) on the following grounds:

- (i) **Misidentification of Account** – that the ISP account has been incorrectly identified as one through which acts of alleged copyright infringement have occurred.
- (ii) **Unauthorized Use of Account** – that the alleged activity was the result of the unauthorized use of the Subscriber's account of which the Subscriber was unaware and that the Subscriber could not reasonably have prevented.
- (iii) **Authorization** – that the use of the work made by the Subscriber was authorized by its Copyright Owner.
- (iv) **Fair Use** – that the Subscriber's reproducing the copyrighted work(s) and distributing it/them over a P2P network is defensible as a fair use.
- (vi) **Misidentification of File** – that the file in question does not consist primarily of the alleged copyrighted work at issue.
- (vii) **Work Published Before 1923** – that the alleged copyrighted work was published prior to 1923.

All determinations shall be made by an independent "**Reviewer**" as described below, and the determinations shall have the effect set forth herein.

2. **Standard of Review**.

2.1. Misidentification of Account. A Subscriber shall prevail on this defense if the Participating ISP's and/or Copyright Owner's records indicate, upon Independent Review, that a factual error was made in (1) identifying the IP address at which the alleged copyright infringement occurred and/or (2) correlating the identified IP address to the Subscriber's account. In reviewing the Participating ISP's or Copyright Owner's records, automated systems for capturing IP addresses or other information in accordance with Methodologies have a rebuttable presumption that they work in accordance with their specifications, unless the Independent Expert's review of any such Content Owner Representative Methodology resulted in a Finding of Inadequacy in which event such rebuttable presumption shall not apply to such Content Owner Representative Methodology.

2.2. Unauthorized Use of Account. A Subscriber shall prevail on this defense if the Subscriber adequately and credibly demonstrates that the alleged activity was the result of unauthorized use of the Subscriber's account by someone who is not a member or invitee of the household (*e.g.*, via an unsecured wireless router or a hacked Internet connection) of which the Subscriber was unaware and that the Subscriber could not reasonably have prevented. The foregoing sentence notwithstanding, the Reviewer may in his or her discretion conclude that a Subscriber is entitled to prevail under this defense despite the Subscriber's failure to secure a wireless router if the Reviewer otherwise concludes that the Subscriber adequately and credibly demonstrates that the alleged activity was the result of unauthorized use of the Subscriber's account by someone who is not a member or invitee of the household of which the Subscriber was unaware. In determining whether this standard has been satisfied, the Reviewer shall consider the evidence in light of the educational messages previously provided by the Participating ISP. Except as set forth herein, this defense may be asserted by a Subscriber only one (1) time to give the Subscriber the opportunity to take steps to prevent future unauthorized use of the Subscriber's account. Any subsequent assertion of this defense by a Subscriber shall be denied as barred, unless the Subscriber can show by clear and convincing evidence that the unauthorized use occurred despite reasonable steps to secure the Internet account and that the breach of such security could not reasonably have been avoided.

2.3. Authorization. A Subscriber shall prevail on this defense if the Subscriber adequately and credibly demonstrates with written or other documented evidence that the Subscriber's alleged activity was actually specifically authorized by the Copyright Owner or its authorized representative. Such written or other documented evidence typically must include a true and unaltered copy of the agreement or communication asserted to grant the claimed authorization. Such evidence shall not be deemed adequate and credible if, among other things, (i) the evidence on its face does not support a claim of authorization, (ii) the evidence does not appear authentic, or (iii) a reasonable person in the Subscriber's position would not have concluded that the communication was in fact authorizing the specific use made of the work and that such authorization came from the actual Copyright Owner or by someone authorized to act on his/her behalf. The defense shall fail if the Copyright Owner has demonstrated: (x) that the specific use of the work made by the Subscriber was not in fact authorized by the Copyright Owner; (y) if the

alleged authorization did not come directly from the Copyright Owner, that the person purporting to grant authorization was not authorized to act on behalf of the Copyright Owner for purposes of authorizing the specific use made of the work by the Subscriber, or (z) that the documentary evidence submitted by the Subscriber likely is not authentic or has been altered in a material manner.

2.4. Fair Use. A Subscriber shall prevail on this defense if the Subscriber adequately and credibly demonstrates fair use of the copyrighted work under prevailing principles of copyright law (which shall be identified as described in section 6).

2.5. Misidentification of File. A Subscriber shall prevail on this defense if the Subscriber adequately and credibly demonstrates that a factual error was made in identifying the file at issue as consisting primarily of the alleged copyrighted work. In making this determination, the Content Owner Representative Methodology used to identify the file shall have a rebuttable presumption that it works in accordance with its specifications, unless the Independent Expert's review of any such Content Owner Representative Methodology resulted in a Finding of Inadequacy in which event such rebuttable presumption shall not apply to such Content Owner Representative Methodology.

2.6. Work Published Before 1923. A Subscriber shall prevail on this defense if the Subscriber adequately and credibly demonstrates that the alleged copyrighted work in question was actually published prior to 1923.

3. Effect of Decision. If the Reviewer's decision is in favor of the Subscriber for a particular Copyright Alert, that Copyright Alert shall be deemed invalid, the filing fee described in paragraph 4.1.6 shall be promptly refunded to the Subscriber, and the Participating ISP shall remove that Copyright Alert from the Subscriber's account records and refrain from applying any Mitigation Measures based on the invalidated Copyright Alert(s). All other Copyright Alerts shall remain valid, and shall count toward future Mitigation Measures. If the Reviewer's decision for a particular Copyright Alert is in favor of the Copyright Owner, that Copyright Alert shall be deemed valid, and if applicable, the Mitigation Measure shall be applied promptly. The Reviewer's decision will be binding solely for the purposes of the Copyright Alert program. By participating in the Independent Review, the Subscriber, the Participating ISP, and the Copyright Owner agree to waive all rights to challenge the Reviewer's decision for purposes of the Copyright Alert program. The Reviewer's decision shall have no effect outside of the Copyright Alert program, shall not act as res judicata or collateral estoppel or any similar bar, and shall not have any precedential impact for other Independent Reviews with respect to other Subscribers within the Copyright Alert program. In any judicial proceeding between a Subscriber and a Copyright Owner concerning subject matter that is or has been the subject of Independent Review, neither the Subscriber nor the Copyright Owner shall seek to enter into evidence, or otherwise refer to or cite, either the fact of the Independent Review or any outcome of the Independent Review.

4. Independent Review Procedure.

4.1. How to Initiate an Independent Review.

4.1.1. *ACIR Form.* When the Participating ISP sends a Copyright Alert stating that the Subscriber's account is subject to a Mitigation Measure, the Participating ISP will also make available to the Subscriber access to an online Application to Commence Independent Review ("ACIR") form and related materials. The ACIR form and related materials will permit the Subscriber to review all of the Copyright Alerts applicable to the Subscriber's account that have not previously been subject to review, as further described in paragraph 4.1.4. The ACIR form will identify all of the information necessary for the Subscriber to invoke an Independent Review, including each defense asserted as to each work identified in a Copyright Alert under review, and also include space for provision of the Subscriber's contact information.

4.1.2. *Authorization.* The ACIR form will contain an authorization by the Subscriber to disclose relevant personal information to the Reviewer and to the Participating ISP. Such information includes: (1) information contained on the ACIR form, (2) information in the Participating ISP's possession, custody or control identifying the Subscriber or relating to any Copyright Alert sent to the Subscriber by the Participating ISP concerning alleged infringement, (3) information regarding the Participating ISP's matching of the IP address in an ISP Notice to the Subscriber's account, and (4) details of actions taken or proposed to be taken as Mitigation Measures by the Participating ISP with respect to the Subscriber's account. Except as explained in the next sentence or as required by judicial order or other legal process, all Subscriber personal information will be held in confidence and not disclosed to the Copyright Owner. If the Subscriber's defense is based on authorization, then the Reviewer may, in his or her discretion, disclose to the Copyright Owner only such personal information concerning the Subscriber as is reasonably necessary to permit the Copyright Owner to rebut a claim of authorization if that information is required for such purposes. The ACIR form will contain an authorization by the Subscriber to disclose relevant personal information to the Copyright Owner in the circumstances described in the immediately preceding sentence.

4.1.3. *Information Required.* The Subscriber must (1) identify the defenses asserted as to each work identified in each Copyright Alert at issue by checking the proper boxes on the ACIR form, (2) explain the specific basis for each defense, and (3) provide the corresponding back-up material to support such grounds. In the case of a defense of authorization, the ACIR form must be accompanied by the applicable written or other documented evidence that the Subscriber's alleged activity was specifically authorized by the Copyright Owner or its authorized representative, as described in paragraph 2.3. In the case of a defense of fair use, the ACIR form must (1) be accompanied by a true and unaltered copy of each content file that the Subscriber asserts to be a fair use under prevailing principles of copyright law; and (2) an explanation of each use

the Subscriber made of the file, including any distribution or downloading identified in the Copyright Alert(s), and the basis for claiming each such use as a fair use.

4.1.4. *Copyright Alerts Subject to Review.* The Subscriber shall have the right to invoke Independent Review for the last Copyright Alert sent as well as prior Copyright Alerts, provided that the right to have a particular Copyright Alert reviewed shall be waived if that right is not invoked the first time the Copyright Alert becomes eligible to be reviewed. Accordingly, when a Subscriber first receives a Mitigation Measure Copyright Alert, the Subscriber may invoke the Independent Review process as to any prior Copyright Alert, but if any of those Copyright Alerts is not reviewed at that time it will thereafter be unreviewable.

4.1.5. *Multiple Works Identified in a Copyright Alert.* In cases in which a Copyright Alert alleges infringing activity with respect to multiple works, the Independent Review process may be invoked by a Subscriber only if the Subscriber offers a defense as to every work cited in the Copyright Alert. A Copyright Alert will be considered valid and provide a basis for the application of a Mitigation Measure if the Subscriber is found to have no valid defense as to any one work cited in the Copyright Alert, unless the Independent Review establishes a pattern of invalid allegations in the Copyright Alert sufficient to cast substantial doubt on the Copyright Alert's remaining allegations.

4.1.6. *Filing Fee.* The Subscriber shall be required to pay a filing fee of thirty-five dollars (\$35) in order to invoke the Independent Review, unless the Subscriber qualifies for a waiver or reduction in the filing fee in accordance with the procedures of the Administering Organization (as defined in paragraph 5.1 below). This fee will be refunded to the Subscriber in the event that the Reviewer decides in favor of the Subscriber as to any Copyright Alert eligible for review.

4.1.7. *Deadline.* The ACIR form, related materials and filing fee ("ACIR Package") must be submitted electronically within ten (10) business days after receipt of the relevant Copyright Alert. Except as contemplated in paragraph 5.6 below, failure to properly submit an ACIR form by the due date shall be deemed a waiver of the right to seek Independent Review regarding the applicable Mitigation Measure.

4.1.8. *Submission of ACIR Package.* The Subscriber must submit the ACIR Package to the Administering Organization. The Administering Organization shall immediately send a copy of the ACIR Package to the applicable Participating ISP.

4.1.9. *Effect of Filing for Independent Review.* A Subscriber's filing of the ACIR form stays implementation of any Mitigation Measure. A Subscriber's failure to file an ACIR or otherwise challenge an allegation of copyright

infringement shall not be construed as an admission or waiver in any other forum or context.

4.2 Process for Independent Review.

4.2.1. *Selection of Reviewer.* All Independent Reviews shall be resolved by one (1) individual serving as an independent Reviewer. The Reviewer will be selected by the Administering Organization from a panel of neutrals, as further described in paragraph 5.2.

4.2.2. *Initial Review of ACIR Package.* A Reviewer will review the ACIR package within five (5) business days of receipt to determine whether it is substantially complete. To be considered substantially complete, (1) the ACIR Package must include a substantially completed ACIR form; (2) the ACIR form must assert a defense as to each work identified in the relevant Copyright Alert subject to Independent Review; (3) for each defense asserted as to each work, the ACIR Package must include sufficient information as described in paragraph 4.1.3 to permit the Independent Review to proceed meaningfully and to potentially result in a decision in favor of the Subscriber; and (4) the ACIR Package must include the required payment as provided in paragraph 4.1.6. If the ACIR Package is not substantially complete, the case will be denied. The first time an ACIR Package is denied, such a denial shall be without prejudice to afford the Subscriber one additional opportunity to correct any mistakes or omissions in the ACIR Package. In such a case, the Reviewer shall notify the Subscriber of the relevant defects and afford the Subscriber five (5) business days to remedy the defects by submitting a substantially complete ACIR Package. Otherwise (except as provided in paragraph 5.6 below), such a denial shall be with prejudice. Either a denial without prejudice that is not remedied within 5 business days or a denial with prejudice shall have the same effects as a denial on the merits (see section 3).

4.2.3. *Verification that Defense of Unauthorized Use of Account is not Barred.* In the case of any defense of unauthorized use of account, the Reviewer's initial review will also consider whether that defense is barred because the Administering Organization's records indicate that the Subscriber previously asserted that defense in another Independent Review. If so, the defense shall be denied, unless the Subscriber can show by clear and convincing evidence that the unauthorized use occurred despite reasonable steps to secure the Internet account and that the breach of such security could not reasonably have been avoided. If for any reason the Administering Organization's records are inconclusive as to this question, the Reviewer will request clarification from the Participating ISP pursuant to paragraph 4.2.4.

4.2.4. *Collection of Standard Information from Participating ISP and Copyright Owner.* If the ACIR Package is substantially complete, the Reviewer will, if needed, request standard relevant information from the Participating ISP

and/or Copyright Owner to assess the grounds for review. Details of the standard information to be provided by the Participating ISP and/or Copyright Owner for different types of defenses shall be determined by mutual agreement of representatives of the Administering Organization, Participating ISPs and Copyright Owners as implementation proceeds, with the goal of having provision of this standard information be a straightforward and largely automated process. In the case of a defense of misidentification of account, information to be provided by the Participating ISP is anticipated to consist of information in the Participating ISP's possession, custody, or control relating to (1) ISP Notices received by the Participating ISP and matched to the Subscriber's account, (2) Copyright Alerts sent to the Subscriber by the Participating ISP, and (3) the Participating ISP's matching of IP addresses on ISP Notices received by the Participating ISP to the Subscriber's account. Information to be provided by the Copyright Owner is anticipated to consist of all or part of the evidence package(s) (*i.e.*, information relating to the alleged access to copyrighted material) for one (1) or more Copyright Alerts that are the subject of the Independent Review. The Participating ISP and Copyright Owner, as applicable, will provide the relevant information to the Reviewer within ten (10) business days after receipt of the request.

4.2.5. *First Substantive Review.* Within five (5) business days from receipt of the relevant standard information from the Participating ISP and/or the Copyright Owner, the Reviewer will review the case record substantively to determine if additional information from the Participating ISP and/or Copyright Owner is required, or whether it is apparent without soliciting further information that the Subscriber will not prevail as to all works cited in any one (1) or more Copyright Alerts.

4.2.6. *Supplemental Information.* The Reviewer shall have the discretion to request supplemental information from the Participating ISP, Copyright Owner or Subscriber within the five (5) business day period referred to in paragraph 4.2.5, if such information would likely be material to a just resolution of the Independent Review. If the Reviewer makes such a request, the applicable party(ies) shall have ten (10) business days to respond. If the Subscriber asserts a defense of authorization or fair use and the Reviewer determines that the defense may have merit, then the Copyright Owner shall receive all relevant information about the defense from the Reviewer and be afforded an opportunity to provide evidence to rebut the defense within ten (10) business days from receipt of such information. Such information shall include (1) in the case of a defense of authorization, all substantiating evidence and explanation submitted by the Subscriber as to each relevant work and the Subscriber's identifying information, unless the Reviewer concludes that the Copyright Owner does not need to know the identity of the Subscriber to evaluate the Subscriber's claim that his or her activity was authorized; and (2) in the case of a defense of fair use, the content file submitted by the Subscriber as to each relevant work and an explanation of why the Subscriber believes each use of that content file to be a fair use.

4.2.7. *Final Assessment and Issuance of Decision.* Within ten (10) business days of receipt of all requested information, including any supplemental information provided pursuant to paragraph 4.2.6, or passage of the relevant time to provide supplemental information in the event no supplemental information is received, the Reviewer shall assess the complete case record and enter a final decision. In doing so, the Reviewer shall determine the relevance, materiality and weight of all evidence based on the available record. The proceedings will take place exclusively on the written record, and there shall be no live hearings. For a Copyright Alert alleging infringement of multiple copyrighted works, in order to find in favor of the Subscriber with respect to the Copyright Alert, the Reviewer must consider and find in favor of the Subscriber as to a defense for each individual work referenced in the Copyright Alert or must find a pattern of invalid allegations in the Copyright Alert sufficient to cast substantial doubt on all allegations in the Copyright Alert. Upon reaching a final decision, the Reviewer will notify the Subscriber, Participating ISP and Copyright Owner of the outcome, and if the decision is a denial of the Subscriber's defense, the Reviewer will also include a short description of the rationale for the denial.

4.2.8. *Withdrawal of Notice by Copyright Owner.* A Copyright Owner may withdraw an ISP Notice at any time during the Independent Review process, which shall have the same effect as a finding for the Subscriber as to the withdrawn Copyright Alert (see section 3).

4.2.9. *Communications Among Parties.* Except as specifically described in these rules (e.g., in the case of requests for information as described in paragraphs 4.2.4 and 4.2.6), there will be no communication between the Reviewer and the Participating ISP, Copyright Owner or Subscriber concerning the Independent Review. There is to be absolutely no discovery between the parties to the dispute, and no party shall have any obligation to respond to any request for information or to provide any particular information, except as described herein.

5. Administration of Independent Review Process.

5.1. In General. The Independent Review process shall be coordinated by the administering organization selected by the CCI Executive Committee ("Administering Organization"). The Independent Review process shall be governed exclusively by these rules.

5.2. Selection of Reviewers. The Administering Organization shall have mechanisms for establishing a panel of neutrals and for ensuring their continuing neutrality, their compliance with these rules, and their adherence to the governing principles of copyright law as provided in section 6. Reviewers must be lawyers, but need not necessarily have the legal or case management expertise that would qualify them to act as arbitrators of more complex disputes in a broader-ranging alternative

dispute resolution process. The Administering Organization shall provide Reviewers training in this Independent Review process and governing principles of copyright law determined as described in section 6. Reviewers may be staff employees of the Administering Organization if the volume of disputes subject to the Independent Review process so warrants.

5.3. Automation. The Administering Organization shall implement automated processes for managing the workflow of cases proceeding through the Independent Review process, including means for seeking and obtaining information from Participating ISPs and Copyright Owners in a manner that minimizes the associated workload on Participating ISPs and Copyright Owners and is automated to the maximum extent practicable.

5.4. Records of Subscriber History of Invoking Independent Review. The Administering Organization will maintain a secure database of Subscribers' history of invoking the Independent Review process, which will be available to Reviewers when evaluating future disputes involving the relevant Subscribers. Thus, for example, it should be possible for a Reviewer to determine from this database whether a Subscriber has previously asserted a defense of unauthorized use of account, and a Reviewer may consider a Subscriber's Independent Review history in evaluating the credibility of claims under review.

5.5. Recordkeeping and Review. The CCI Executive Committee and Administering Organization will establish processes for (1) maintaining records concerning proceedings, (2) periodically reviewing anonymous, aggregated information about issues and outcomes so that trends can be identified and addressed if warranted, and (3) confidentially auditing decisions for purposes of evaluating the performance of Reviewers and the Administering Organization. Except to the extent necessary to maintain records of outcomes of proceedings for purposes of operation and review of the Independent Review process or as otherwise expressly set forth herein, Reviewers shall not prepare written decisions in the cases they decide. The Parties to the Agreement agree to negotiate in good faith as to adjustments in the Independent Review process if such adjustments are warranted by actual experience in operating the Independent Review process.

5.6. Provision of Information. Fair and efficient administration of the Independent Review process depends upon timely provision of information requested by the Reviewer at various steps of the process, as described in paragraph 4.2. Whenever these rules set forth a timeframe for provision of information requested by the Reviewer, the Reviewer may grant reasonable extensions of such period (not to exceed ten (10) business days) for substantial good cause shown. In the absence of the requested information at the deadline for providing the same, the following provisions will apply:

5.6.1. *Delays in Providing Standard Information.* If the Reviewer properly requests a standard package of information from a Participating ISP or Copyright Owner, as described in paragraph 4.2.4, and the Participating ISP or

Copyright Owner does not provide the requested information as to some or all claims or works on a timely basis, (1) the Reviewer shall promptly notify the Participating ISP or Copyright Owner and the Participating ISP or Copyright Owner shall have a further five (5) business days to provide the requested information; and (2) the Administering Organization shall reflect such deficiency in reports to be provided periodically to the CCI Executive Committee. Recurring failure of a Participating ISP or Copyright Owner to provide requested standard information during the initial period identified in paragraph 4.2.4, in other than isolated instances, will be considered a breach of its obligations under the Agreement. If a Participating ISP or Copyright Owner does not provide available requested information within a further five (5) business days, (a) the dispute will proceed to the next step of decision making based on the available record without such information, giving the Subscriber the benefit of any doubt concerning the missing requested information; (b) the Administering Organization shall reflect such deficiency in reports to be provided periodically to the CCI Executive Committee; and (c) the Participating ISP or Copyright Owner will be considered in breach of its obligations under the Agreement.

5.6.2. Delays in Providing Supplemental Information. If the Reviewer properly requests supplemental information from a Participating ISP, Copyright Owner or Subscriber pursuant to paragraph 4.2.6, and the Participating ISP, Copyright Owner or Subscriber does not provide the requested information as to some or all claims or works on a timely basis, the dispute will proceed to the next step of decision making based on the available record without such information. If the Reviewer believes that the position of a party to the proceeding other than the one that has failed to provide the requested information is otherwise meritorious, the Reviewer shall give such party the benefit of any doubt concerning the missing requested information.

6. Legal Principles to Be Applied in Independent Review. The Independent Review process will, to the extent relevant, apply prevailing legal principles as determined by United States federal courts. The Administering Organization will commission an accepted, independent expert on copyright law, who is approved by the CCI Executive Committee, to outline prevailing legal principles of fair use for purposes of deciding defenses of fair use, and any other legal principles necessary for resolution of issues within the scope of this Independent Review process. Such outline will be updated from time to time as necessary. If additional material questions of law arise as the Independent Review process is implemented, they may be referred to an accepted, independent expert approved by the CCI Executive Committee as needed. The Administering Organization will advise the Parties to the Agreement of issues referred to, and principles determined by, such an expert, and provide a process for the Parties to the Agreement to provide input concerning the issues, so as to ensure that the expert's determinations are fully-informed and reflect prevailing law as determined by United States federal courts.

Attachment D – MPAA Member Company Affiliates

The MPAA member companies' affiliates are entities under the control of an MPAA member company. For purposes of this Attachment D, "control" is defined as (1) the ownership of at least fifty percent (50%) of the equity or beneficial interest of the controlled entity, (2) the right to vote for or appoint a majority of the board of directors or other governing body of such entity (if the board or governing body may exercise authority with less than a majority, then the right to vote or appoint the number of directors necessary to exercise that authority), or (3) the right or authority to grant, approve or withhold, directly or indirectly, financial resources necessary to the operation of the controlled entity. As of the Effective Date of this Agreement, the following entities are MPAA member company affiliates:

- Disney Enterprises, Inc., entities controlled, directly or indirectly, by Disney Enterprises, Inc. (together, "Disney Enterprises Entities"), and such other entities as have authorized the foregoing to send Copyright Alerts on their behalf with respect to works distributed by Disney Enterprises Entities.
- Fox Entertainment Group, Inc., entities controlled, directly or indirectly, by Fox Entertainment Group, Inc., (together, "Fox Entertainment Entities") and such other entities as have authorized the foregoing to send Copyright Alerts on their behalf with respect to works distributed by Fox Entertainment Entities.
- NBCUniversal Media LLC, entities controlled, directly or indirectly, by NBCUniversal Media LLC, (together, "NBCU Entities") and such other entities as have authorized the foregoing to send Copyright Alerts on their behalf with respect to works distributed by NBCU Entities.
- Sony Pictures Entertainment Inc., entities controlled, directly or indirectly, by Sony Pictures Entertainment Inc. (together, "SPE Entities"), and such other entities as have authorized the foregoing to send Copyright Alerts on their behalf with respect to works distributed by SPE Entities.
- Turner Entertainment Networks, Inc., entities controlled, directly or indirectly, by Turner Entertainment Networks, Inc. (together, "Turner Entities"), and such other entities as have authorized the foregoing to send Copyright Alerts on their behalf with respect to works distributed by Turner Entities.
- Viacom, Inc., entities controlled, directly or indirectly, by Viacom, Inc. (together, "Viacom Entities"), and such other entities as have authorized the foregoing to send notices on their behalf with respect to works distributed by Viacom Entities.
- Walt Disney Studios Motion Pictures, entities controlled, directly or indirectly, by Walt Disney Studios Motion Pictures (together, "Walt Disney Studios Entities"), and such other entities as have authorized the foregoing to send notices on their behalf with respect to works distributed by Walt Disney Studios Entities.
- Warner Bros. Entertainment Inc., entities controlled, directly or indirectly, by Warner Bros. Entertainment Inc. (together, "Warner Bros. Entities"), and such other entities as have authorized the foregoing to send notices on their behalf with respect to works distributed by Warner Bros. Entities.

Annex I

**NGPC Proposal for Implementation of GAC Safeguards
Applicable to All New gTLDs**

19 June 2013

The following is a draft proposal for how ICANN could implement the “GAC Safeguards Applicable to All New gTLDs.” This is an unapproved draft subject to further NGPC consideration.

1. WHOIS Verification and Checks (GAC Register # 2013-04-11-Safeguards-1)

ICANN is concluding its development of a WHOIS tool that gives it the ability to check false, incomplete or inaccurate WHOIS data as the Board previously directed staff in Board Resolutions 2012.11.08.01 - 2012.11.08.02 to begin to “proactively identify potentially inaccurate gTLD data registration in gTLD registry and registrar services, explore using automated tools, and forward potentially inaccurate records to gTLD registrars for action; and 2) publicly report on the resulting actions to encourage improved accuracy.” <<http://www.icann.org/en/groups/board/documents/resolutions-08nov12-en.htm>>

Given these ongoing activities, ICANN (instead of Registry Operators) is well positioned to implement the GAC’s advice that checks identifying registrations in a gTLD with deliberately false, inaccurate or incomplete WHOIS data be conducted at least twice a year. To achieve this, ICANN will perform a periodic sampling of WHOIS data across registries in an effort to identify potentially inaccurate records. ICANN will also maintain statistical reports that identify the number of inaccurate WHOIS records identified. This undertaking by ICANN would not require ICANN to provide special certifications to Registry Operators certifying the accuracy of any WHOIS data. The WHOIS verification

and checks would be focused on the current version of WHOIS requirements, but would eventually broaden to include directory services.

2. Mitigating Abusive Activity (GAC Register # 2013-04-11-Safeguards-2)

ICANN will include a provision in the proposed New gTLD Registry Agreement (as a mandatory Public Interest Commitment in Specification 11) [\(<http://newgtlds.icann.org/en/applicants/agb/base-agreement-specs-29apr13-en.pdf>](http://newgtlds.icann.org/en/applicants/agb/base-agreement-specs-29apr13-en.pdf)) obligating Registry Operators to include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.

Paragraph 2 of the PIC Specification attached as Annex II includes language to implement the GAC advice. Because the Registry Operator does not have a direct contractual relationship with the Registered Name Holder, the language proposed in the PIC Specification would require the Registry Operator to include a provision in its Registry-Registrar Agreement, which in turn requires Registrars to include a provision in their Registration Agreements prohibiting Registered Name Holders from engaging in the abusive activity listed in the GAC advice.

3. Security Checks (GAC Register # 2013-04-11-Safeguards-3)

ICANN will include a provision in the proposed New gTLD Registry Agreement (as a mandatory Public Interest Commitment in Specification 11) requiring Registry Operators periodically to conduct a technical analysis to assess whether domains in its gTLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. The provision will also require Registry Operators to maintain statistical reports

on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operators will maintain these reports for the agreed contracted period and provide them to ICANN upon request. The contents of the reports will be publically available as appropriate.

Because there are multiple ways for a Registry Operator to implement the required security checks, ICANN will solicit community participation (including conferring with the GAC) in a task force or through a policy development process in the GNSO, as appropriate, to develop the framework for Registry Operators to respond to identified security risks that pose an actual risk of harm, notification procedures, and appropriate consequences, including a process for suspending domain names until the matter is resolved, while respecting privacy and confidentiality. The language include in Paragraph 3 of the attached PIC Specification provides the general guidelines for what Registry Operators must do, but omits the specific details from the contractual language to allow for the future development and evolution of the parameters for conducting security checks. This will permit Registry Operators to enter into agreements as soon as possible, while allowing for a careful and fulsome consideration by the community on the implementation details.

4. Documentation (GAC Register # 2013-04-11-Safeguards-4)

As detailed in #1 above, ICANN will maintain statistical reports that identify the number of inaccurate WHOIS records identified as part of the checks to identify registrations with deliberately false, inaccurate or incomplete WHOIS data. Also, as detailed in #3 above, Registry Operators will be required to maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operators will maintain these reports for the agreed contracted period and provide them to ICANN upon request. The contents of the reports will be publically available as appropriate.

5. Making and Handling Complaints (GAC Register # 2013-04-11-Safeguards-5)

Registry Operators will be required to ensure that there is a mechanism for making complaints to the Registry Operator regarding malicious conduct in the TLD. Section 4.1 of Specification 6 of the proposed New gTLD Registry Agreement provides that, “Registry Operator shall provide to ICANN and publish on its website its accurate contact details including a valid email and mailing address as well as a primary contact for handling inquiries related to malicious conduct in the TLD, and will provide ICANN with prompt notice of any changes to such contact details.” Also, Section 2.8 of the proposed New gTLD Registry Agreement provides that a, “Registry Operator shall take reasonable steps to investigate and respond to any reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of the TLD.”

ICANN operates the WHOIS Data Problem Reports System

<<http://www.icann.org/en/resources/compliance/complaints/whois/inaccuracy-form>>,

which is a mechanism for making complaints that WHOIS information is inaccurate.

6. Consequences (GAC Register # 2013-04-11-Safeguards-6)

As indicated in #2 above, ICANN will include a provision in the proposed New gTLD Registry Agreement (as a mandatory Public Interest Commitment in Specification 11) obligating Registry Operators to include a provision in their Registry-Registrar Agreements that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.

Consequences for the demonstrated provision of false WHOIS information are set forth in Section 3.7.7.2 of the 2013 RAA

<<http://www.icann.org/en/resources/registrars/raa/proposed-agreement-22apr13-en.pdf>>:

“A Registered Name Holder's willful provision of inaccurate or unreliable information, its willful failure to update information provided to Registrar within seven (7) days of any change, or its failure to respond for over fifteen (15) days to inquiries by Registrar concerning the accuracy of contact details associated with the Registered Name Holder's registration shall constitute a material breach of the Registered Name Holder-registrar contract and be a basis for suspension and/or cancellation of the Registered Name registration.” Paragraph 1 of the proposed PIC Specification includes a requirement that Registry Operator will use only ICANN accredited registrars that are party to the 2013 RAA so that these consequences are contractually required.



Annex II**Proposed PIC Spec Implementation of GAC Safeguards Applicable to all New
gTLDs
(19 June 2013)**

The following is a preliminary draft reference version of the Beijing GAC safeguards advice for safeguards applicable to all new gTLDs implemented as Public Interest Commitments – for discussion only.

**Specification 11
Public Interest Commitments**

1. Registry Operator will use only ICANN accredited registrars that are party to the Registrar Accreditation Agreement approved by the ICANN Board of Directors on _____, 2013 in registering domain names. A list of such registrars shall be maintained by ICANN on ICANN's website.
 2. Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.
 3. Registry Operator will periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. Registry Operator will maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operator will maintain these reports for the term of the Agreement unless a shorter period is required by law or approved by ICANN, and will provide them to ICANN upon request.
- 

Internet Corporation for Assigned Names and Numbers

GROUPS (/EN/GROUPS) › BOARD (/EN/GROUPS/BOARD) › DOCUMENTS (/EN/GROUPS/BOARD/DOCUMENTS)

Approved Resolutions | Meeting of the New gTLD Program Committee

9

25 June 2013

1. Consent Agenda

- a. Approval of NGPC Meeting Minutes

2. Main Agenda

- a. ALAC (At-Large Advisory Committee) Statement on TMCH/Variants
- b. Safeguards Applicable to all New gTLDs
Rationale for Resolutions 2013.06.25.NG02 – 2013.06.25.NG03
- c. Category 2 Safeguard Advice re Restricted and Exclusive Registry Access
Rationale for Resolutions 2013.06.25.NG04 – 2013.06.25.06
- d. Singular & Plural Versions of the Same String as a TLD (Top Level Domain)
Rationale for Resolution 2013.06.25.NG07
- e. IGO (Intergovernmental Organization) Protection
- f. AOB

1. Consent Agenda:

- a. **Approval of NGPC Meeting Minutes**
Resolved (2013.06.25.NG01), the Board approves the minutes of the 4 June 2013 New gTLD (generic Top Level Domain) Program Committee Meeting.

2. Main Agenda:

- a. ALAC (At-Large Advisory Committee) Statement on TMCH/Variants
No resolution taken.
- b. Safeguards Applicable to all New gTLDs
Whereas, the GAC (Governmental Advisory Committee) met during the ICANN (Internet Corporation for Assigned Names and Numbers) 46 meeting in Beijing and issued a Communiqué on 11 April 2013 ("Beijing Communiqué");
Whereas, the Beijing Communiqué included six (6) elements of safeguard advice applicable to all new gTLDs, which

Approved Resolutions | Meeting of the New gTLD Program Committee |... <http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-2...>

are identified in the [GAC \(Governmental Advisory Committee\)](#) Register of Advice as: (a) 2013-04-11-Safeguards-1, (b) 2013-04-11-Safeguards-2, (c) 2013-04-11-Safeguards-3, (d) 2013-04-11-Safeguards-4, (e) 2013-04-11-Safeguards-5, and (f) 2013-04-11-Safeguards-6 (collectively, the "Safeguards Applicable to All Strings");

Whereas, on 23 April 2013, ICANN (Internet Corporation for Assigned Names and Numbers) initiated a public comment forum to solicit the community's input on how the NGPC should address [GAC \(Governmental Advisory Committee\)](#) advice regarding safeguards applicable to broad categories of New gTLD ([generic Top Level Domain](#)) strings <<http://www.icann.org/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm> (/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm)>;

Whereas, the NGPC met on 8 and 18 May and 4, 11 and 18 June 2013 to consider a plan for responding to the [GAC \(Governmental Advisory Committee\)](#)'s advice on the New gTLD ([generic Top Level Domain](#)) Program, including the Safeguards Applicable to All Strings;

Whereas, the NGPC met on 25 June 2013 to further discuss and consider its plan for responding the [GAC \(Governmental Advisory Committee\)](#)'s advice in the Beijing Communiqué on the New gTLD ([generic Top Level Domain](#)) Program;

Whereas, the NGPC has considered the public comments submitted during the public comment forum, and has determined that its position, as presented in Annex I (/en/groups/board/documents/resolutions-new-gtld-annex-i-agenda-2b-25jun13-en.pdf) [PDF, 72 KB] attached to this Resolution, is consistent with the [GAC \(Governmental Advisory Committee\)](#)'s advice regarding Safeguards Applicable to All Strings;

Whereas, the NGPC proposes revisions to the final draft of the New gTLD ([generic Top Level Domain](#)) Registry Agreement <<http://www.icann.org/en/news/public-comment/base-agreement-29apr13-en.htm> (/en/news/public-comment/base-agreement-29apr13-en.htm)> as presented in Annex II (/en/groups/board/documents/resolutions-new-gtld-annex-ii-agenda-2b-25jun13-en.pdf) [PDF, 64 KB] attached to this Resolution to implement certain elements of the [GAC \(Governmental Advisory Committee\)](#) advice regarding Safeguards Applicable to All Strings; and

Whereas, the NGPC is undertaking this action pursuant to the authority granted to it by the Board on 10 April 2012, to exercise the ICANN (Internet Corporation for Assigned Names and Numbers) Board's authority for any and all issues that may arise relating to the New gTLD ([generic Top Level Domain](#)) Program.

Resolved (2013.06.25.NG02), the NGPC adopts the "NGPC Proposal for Implementation of [GAC \(Governmental Advisory Committee\)](#) Safeguards Applicable to All New gTLDs" (19 June 2013), attached as Annex I (/en/groups/board/documents/resolutions-new-gtld-annex-i-agenda-2b-25jun13-en.pdf) [PDF, 72 KB] to this Resolution, to accept the [GAC \(Governmental Advisory Committee\)](#)'s advice regarding Safeguards Applicable to All Strings.

Resolved (2013.06.25.NG03), the NGPC directs staff to make appropriate changes to the final draft of the New gTLD ([generic Top Level Domain](#)) Registry Agreement, as presented in Annex II (/en/groups/board/documents/resolutions-new-gtld-annex-ii-agenda-2b-25jun13-en.pdf) [PDF, 64 KB] attached to this Resolution, to implement certain elements of the [GAC \(Governmental Advisory Committee\)](#) advice regarding Safeguards Applicable to All Strings.

Rationale for Resolutions 2013.06.25.NG02 – 2013.06.25.NG03

Why the NGPC is addressing the issue?

Article XI, Section 2.1 of the ICANN (Internet Corporation for Assigned Names and Numbers) Bylaws <http://www.icann.org/en/about/governance/bylaws#XI> (/en/about/governance/bylaws#XI) permit the [GAC \(Governmental Advisory Committee\)](#) to "put issues to the Board directly, either by way of comment or prior advice, or by way of specifically recommending action or new policy development or revision to existing policies." The [GAC \(Governmental Advisory Committee\)](#) issued advice to the Board on the New gTLD ([generic Top Level Domain](#)) Program through its Beijing Communiqué dated 11 April 2013. The ICANN (Internet Corporation for Assigned Names and Numbers) Bylaws require the Board to take into account the [GAC \(Governmental Advisory Committee\)](#)'s advice on public policy matters in the formulation and adoption of the policies. If the Board decides to take an action that is not consistent with the [GAC \(Governmental Advisory Committee\)](#) advice, it must inform the [GAC \(Governmental Advisory Committee\)](#) and state the reasons why it decided not to follow the advice. The Board and the [GAC \(Governmental Advisory Committee\)](#) will then try in good faith to find a mutually acceptable solution. If no solution

Approved Resolutions | Meeting of the New gTLD Program Committee |... <http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-2...>

can be found, the Board will state in its final decision why the GAC (Governmental Advisory Committee) advice was not followed.

What is the proposal being considered?

The NGPC is being asked to consider accepting a discrete grouping of the GAC (Governmental Advisory Committee) advice as described in the attached "NGPC Proposal for Implementation of GAC (Governmental Advisory Committee) Safeguards Applicable to All New gTLDs" (Annex I (</en/groups/board/documents/resolutions-new-gtld-annex-i-agenda-2b-25jun13-en.pdf>) [PDF, 72 KB]; 19 June 2013), which includes the six (6) items of safeguard advice from the Beijing Communiqué applicable to all new gTLDs. This advice is identified in the GAC (Governmental Advisory Committee) Register of Advice as: (a) 2013-04-11-Safeguards-1, (b) 2013-04-11-Safeguards-2, (c) 2013-04-11-Safeguards-3, (d) 2013-04-11-Safeguards-4, (e) 2013-04-11-Safeguards-5, and (f) 2013-04-11-Safeguards-6 (collectively, the "Safeguards Applicable to All Strings").

Which stakeholders or others were consulted?

On 23 April 2013, ICANN (Internet Corporation for Assigned Names and Numbers) initiated a public comment forum to solicit input on how the NGPC should address GAC (Governmental Advisory Committee) advice regarding safeguards applicable to broad categories of new gTLD (generic Top Level Domain) strings <http://www.icann.org/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm> (</en/news/public-comment/gac-safeguard-advice-23apr13-en.htm>). The public comment forum closed on 4 June 2013. The NGPC has considered the community's comments in formulating its response to the GAC (Governmental Advisory Committee) advice regarding Safeguards Applicable to All Strings. These comments also will serve as important inputs to the NGPC's future consideration of the other elements of GAC (Governmental Advisory Committee) advice not being considered at this time in the attached annexes.

What concerns or issues were raised by the community?

ICANN (Internet Corporation for Assigned Names and Numbers) received several responses from the community during the course of the public comment forum on broad categories of GAC (Governmental Advisory Committee) safeguard advice. Of comments regarding safeguards applicable to all new gTLDs, approximately 29% of unique commenters expressed opposition whereas approximately 71% expressed support.

Regarding support, commenters expressed general agreement with the safeguards. Those expressing support also expressed concern over the method of implementation and that the GAC (Governmental Advisory Committee) should not dictate the specific procedures for implementation. Supporters also indicated that some of these safeguards are already inherent in the 2013 RAA (Registrar Accreditation Agreement).

In adopting this Resolution, the NGPC specifically acknowledges comments from the community opposed to the NGPC accepting the GAC (Governmental Advisory Committee)'s advice. The NGPC takes note of comments asserting that adopting the GAC (Governmental Advisory Committee) advice threatens the multi-stakeholder policy development process. ICANN (Internet Corporation for Assigned Names and Numbers)'s Bylaws permit the GAC (Governmental Advisory Committee) to "consider and provide advice on the activities of ICANN (Internet Corporation for Assigned Names and Numbers) as they relate to concerns of governments, particularly matters where there may be an interaction between ICANN (Internet Corporation for Assigned Names and Numbers)'s policies and various laws and international agreements or where they may affect public policy issues." (Art. XI, § 2.1.a) The GAC (Governmental Advisory Committee) issued advice to the Board on the New gTLD (generic Top Level Domain) Program through its Beijing Communiqué dated 11 April 2013. The ICANN (Internet Corporation for Assigned Names and Numbers) Bylaws require the Board (and the NGPC) to take into account the GAC (Governmental Advisory Committee)'s advice on public policy matters in the formulation and adoption of the policies, and if the Board (and the NGPC) takes an action that is not consistent with the GAC (Governmental Advisory Committee) advice, it must inform the GAC (Governmental Advisory Committee) and state the reasons why it decided not to follow the advice. The parties must then try in good faith to find a mutually acceptable solution. Thus, the GAC (Governmental Advisory Committee)'s advice is part of the multi-stakeholder process.

The posting of the Beijing Communiqué to solicit public comment on the broad categories of the GAC (Governmental Advisory Committee)'s safeguard advice demonstrates ICANN (Internet Corporation for Assigned Names and

Approved Resolutions | Meeting of the New gTLD Program Committee | ... <http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-2...>

Numbers)'s commitment to a bottom-up, multi-stakeholder model, and provided stakeholders with approximately six weeks (including the public comment and reply periods) to analyze, review and respond to the proposed recommendations. The NGPC views finding a workable solution to the GAC (Governmental Advisory Committee)'s advice as a step forward as the community continues to respond to the needs of registrants, the community and all stakeholders.

The NGPC also took note of the comments from the community in opposition to ICANN (Internet Corporation for Assigned Names and Numbers) implementing the safeguard advice concerning WHOIS verification checks to be performed by registry operators. The NGPC acknowledges the ongoing work in the community on WHOIS verification. In response to these comments in opposition, the NGPC accepted the spirit and intent of the GAC (Governmental Advisory Committee)'s advice on the WHOIS verification checks by having ICANN (Internet Corporation for Assigned Names and Numbers), instead of registry operators, implement the checks. ICANN (Internet Corporation for Assigned Names and Numbers) is concluding its development of a WHOIS tool that gives it the ability to check false, incomplete or inaccurate WHOIS data, as the Board previously directed staff in Board Resolutions 2012.11.08.01 - 2012.11.08.02 to begin to "proactively identify potentially inaccurate gTLD (generic Top Level Domain) data registration in gTLD (generic Top Level Domain) registry and registrar services, explore using automated tools, and forward potentially inaccurate records to gTLD (generic Top Level Domain) registrars for action; and 2) publicly report on the resulting actions to encourage improved accuracy." <<http://www.icann.org/en/groups/board/documents/resolutions-08nov12-en.htm> (<<http://www.icann.org/en/groups/board/documents/resolutions-08nov12-en.htm>)>. Given these ongoing activities, the NGPC determined that ICANN (Internet Corporation for Assigned Names and Numbers) (instead of Registry Operators) is well positioned to implement the GAC (Governmental Advisory Committee)'s advice.

With respect to mitigating abusive activity, the NGPC acknowledges the comments noting that registries do not have relationships with registrants and should not be required to determine whether a registrant is in compliance with applicable laws. To address this concern, the NGPC included language in the PIC Specification that would obligate registry operators to include a provision in their Registry-Registrar Agreements that requires registrars to include in their Registration Agreements a provision prohibiting registered name holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.

With respect to the safeguards regarding security checks, the NGPC considered that the comments in opposition raise important questions about the costs and timing of implementing this measure, and the scope and framework of the security checks. The NGPC is mindful that there are various ways a registry operator could implement the required security checks, and has taken these concerns into consideration in its response to the GAC (Governmental Advisory Committee)'s advice. The NGPC's response directs ICANN (Internet Corporation for Assigned Names and Numbers) to solicit community participation (including conferring with the GAC (Governmental Advisory Committee)) in a task force or through a policy development process in the GNSO (Generic Names Supporting Organization), as appropriate, to develop the framework for Registry Operators to respond to identified security risks that pose an actual risk of harm, notification procedures, and appropriate consequences, including a process for suspending domain names until the matter is resolved, while respecting privacy and confidentiality. The proposed implementation of the GAC (Governmental Advisory Committee)'s advice is phased to account for the commenters' concerns. The proposed language in the PIC Specification will provide the general guidelines for what registry operators must do, but omits the specific details from the contractual language to allow for the future development and evolution of the parameters for conducting security checks.

With respect to consequences in the safeguards applicable to all strings, the NGPC took note of the commenters' concerns that this item of safeguard advice is already addressed in the 2013 RAA (Registrar Accreditation Agreement) and by the WHOIS Data Problem Report system. The GAC (Governmental Advisory Committee)'s concerns are addressed in the existing framework and the NGPC is not proposing to duplicate the existing enforcement models.

The NGPC also takes note of the comments requesting that the GAC (Governmental Advisory Committee) advice be

Approved Resolutions | Meeting of the New gTLD Program Committee |... <http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-2...>

rejected as "last-minute" or "untimely." The commenters asserted that this introduces uncertainty into the Program and the makes material changes to the AGB. As an alternative to accepting the advice, the NGPC considered the timing consequences if the NGPC rejected the advice. The NGPC took note of the procedure for any consultations that might be needed if the Board (and the NGPC) determines to take an action that is not consistent with GAC (Governmental Advisory Committee) advice, which was developed by the ICANN (Internet Corporation for Assigned Names and Numbers) Board-GAC Recommendation Implementation Working Group (BGRI-WG). The procedure was approved by the BGRI-WG in Beijing and would be used for any consultation on this GAC (Governmental Advisory Committee) advice. The procedure says that the consultation process should conclude within six months, but that the GAC (Governmental Advisory Committee) and the Board can agree to a different timetable. On balance, the NGPC determined that entering into a consultation process on this particular section of the safeguard advice would introduce greater uncertainty into the Program than if the NGPC found a workable solution to accept and implement the GAC (Governmental Advisory Committee)'s safeguard advice applicable to all strings.

The complete set of comments can be reviewed at: <http://www.icann.org/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm> ([/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm](#)).

What significant materials did the NGPC review?

As part of its deliberations, the NGPC reviewed the following significant materials and documents:

GAC (Governmental Advisory Committee) Beijing Communiqué: <http://www.icann.org/en/news/correspondence/gac-to-board-18apr13-en.pdf> ([/en/news/correspondence/gac-to-board-18apr13-en.pdf](#)) [PDF, 156 KB]

Public comments in response to broad categories of GAC (Governmental Advisory Committee) safeguard advice: <http://www.icann.org/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm> ([/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm](#))

Report of Public Comments, New gTLD (generic Top Level Domain) Board Committee Consideration of GAC (Governmental Advisory Committee) Safeguard Advice dated 18 June 2013: <http://www.icann.org/en/news/public-comment/report-comments-gac-safeguard-advice-19jun13-en> ([/en/news/public-comment/report-comments-gac-safeguard-advice-19jun13-en](#))

What factors did the NGPC find to be significant?

The Beijing Communiqué generated significant interest from the community and resulted in many comments. The NGPC considered the community comments, the GAC (Governmental Advisory Committee)'s advice transmitted in the Beijing Communiqué, and the procedures established in the AGB for addressing GAC (Governmental Advisory Committee) advice to the New gTLD (generic Top Level Domain) Program.

Are there positive or negative community impacts?

The adoption of the GAC (Governmental Advisory Committee) advice as provided in the attached annexes will assist with resolving the GAC (Governmental Advisory Committee) advice in manner that permits the greatest number of new gTLD (generic Top Level Domain) applications to continue to move forward as soon as possible.

Are there fiscal impacts or ramifications on ICANN (Internet Corporation for Assigned Names and Numbers) (strategic plan, operating plan, budget); the community; and/or the public?

There are no foreseen fiscal impacts associated with the adoption of this resolution.

Are there any security, stability or resiliency issues relating to the DNS (Domain Name System)?

Approval of the proposed resolution will not impact security, stability or resiliency issues relating to the DNS (Domain Name System).

Is this either a defined policy process within ICANN (Internet Corporation for Assigned Names and Numbers)'s Supporting Organizations or ICANN (Internet Corporation for Assigned Names and Numbers)'s Organizational Administrative Function decision requiring public comment or not requiring public comment?

On 23 April 2013, ICANN (Internet Corporation for Assigned Names and Numbers) initiated a public comment forum to solicit input on how the NGPC should address GAC (Governmental Advisory Committee) advice regarding safeguards applicable to broad categories of new gTLD (generic Top Level Domain) strings <http://www.icann.org>

Approved Resolutions | Meeting of the New gTLD Program Committee |... <http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-2.../en/news/public-comment/gac-safeguard-advice-23apr13-en.htm> (/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm). The public comment forum closed on 4 June 2013.

c. Category 2 Safeguard Advice re Restricted and Exclusive Registry Access

Whereas, the GAC (Governmental Advisory Committee) met during the ICANN (Internet Corporation for Assigned Names and Numbers) 46 meeting in Beijing and issued a Communiqué on 11 April 2013 ("Beijing Communiqué");
Whereas, the Beijing Communiqué included Category 2 safeguard advice, which is identified in the GAC (Governmental Advisory Committee) Register of Advice as 2013-04-11-Safeguards-Categories-2 (the "Category 2 Safeguard Advice");

Whereas, on 23 April 2013, ICANN (Internet Corporation for Assigned Names and Numbers) initiated a public comment forum to solicit the community's input on how the NGPC should address GAC (Governmental Advisory Committee) advice regarding safeguards applicable to broad categories of New gTLD (generic Top Level Domain) strings <<http://www.icann.org/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm> (/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm)>;

Whereas, the NGPC met on 8 and 18 May and 4, 11 and 18 June 2013 to consider a plan for responding to the GAC (Governmental Advisory Committee)'s advice on the New gTLD (generic Top Level Domain) Program, including the Category 2 Safeguard Advice;

Whereas, the NGPC met on 25 June 2013 to further discuss and consider its plan for responding to the GAC (Governmental Advisory Committee)'s advice in the Beijing Communiqué on the New gTLD (generic Top Level Domain) Program;

Whereas, the NGPC has considered the public comments submitted during the public comment forum, and proposes revisions to the final draft of the New gTLD (generic Top Level Domain) Registry Agreement <<http://www.icann.org/en/news/public-comment/base-agreement-29apr13-en.htm> (/en/news/public-comment/base-agreement-29apr13-en.htm)> as presented in Annex I (</en/groups/board/documents/resolutions-new-gtld-annex-i-agenda-2c-25jun13-en.pdf>) [PDF, 52 KB] attached to this Resolution to implement the Category 2 Safeguard Advice for applicants not seeking to impose exclusive registry access; and

Whereas, the NGPC is undertaking this action pursuant to the authority granted to it by the Board on 10 April 2012, to exercise the ICANN (Internet Corporation for Assigned Names and Numbers) Board's authority for any and all issues that may arise relating to the New gTLD (generic Top Level Domain) Program.

Resolved (2013.06.25.NG04), the NGPC adopts the "Proposed PIC Spec Implementation of GAC (Governmental Advisory Committee) Category 2 Safeguards" (20 June 2013), attached as Annex I (</en/groups/board/documents/resolutions-new-gtld-annex-i-agenda-2c-25jun13-en.pdf>) [PDF, 52 KB] to this Resolution, to accept and implement the GAC (Governmental Advisory Committee)'s Category 2 Safeguard Advice for applicants not seeking to impose exclusive registry access.

Resolved (2013.06.25.NG05), the NGPC directs staff to make appropriate changes to the final draft of the New gTLD (generic Top Level Domain) Registry Agreement, as presented in Annex I (</en/groups/board/documents/resolutions-new-gtld-annex-i-agenda-2c-25jun13-en.pdf>) [PDF, 52 KB] attached to this Resolution, to implement the GAC (Governmental Advisory Committee)'s Category 2 Safeguard Advice for applicants not seeking to impose exclusive registry access.

Resolved (2013.06.25.NG06), the NGPC directs staff to defer moving forward with the contracting process for applicants seeking to impose exclusive registry access for "generic strings" to a single person or entity and/or that person's or entity's Affiliates (as defined in Section 2.9(c) of the Registry Agreement), pending a dialogue with the GAC (Governmental Advisory Committee).

Rationale for Resolutions 2013.06.25.NG04 – 2013.06.25.06

Why the NGPC is addressing the issue?

Article XI, Section 2.1 of the ICANN (Internet Corporation for Assigned Names and Numbers) Bylaws <http://www.icann.org/en/about/governance/bylaws#XI> (/en/about/governance/bylaws#XI) permit the GAC

Approved Resolutions | Meeting of the New gTLD Program Committee |... <http://www.icann.org/en/groups/board/documents/resolutions-new-gTld-2...>

(Governmental Advisory Committee) to "put issues to the Board directly, either by way of comment or prior advice, or by way of specifically recommending action or new policy development or revision to existing policies." The GAC (Governmental Advisory Committee) issued advice to the Board on the New gTLD (generic Top Level Domain) Program through its Beijing Communiqué dated 11 April 2013. The ICANN (Internet Corporation for Assigned Names and Numbers) Bylaws require the Board to take into account the GAC (Governmental Advisory Committee)'s advice on public policy matters in the formulation and adoption of the policies. If the Board decides to take an action that is not consistent with the GAC (Governmental Advisory Committee) advice, it must inform the GAC (Governmental Advisory Committee) and state the reasons why it decided not to follow the advice. The Board and the GAC (Governmental Advisory Committee) will then try in good faith to find a mutually acceptable solution. If no solution can be found, the Board will state in its final decision why the GAC (Governmental Advisory Committee) advice was not followed.

What is the proposal being considered?

The NGPC is being asked to consider accepting Category 2 safeguard advice identified in the GAC (Governmental Advisory Committee) Register of Advice as 2013-04-11-Safeguards-Categories-2. For applicants not seeking to impose exclusive registry access, the NGPC is being asked to consider including a provision in the PIC Specification in the New gTLD (generic Top Level Domain) Registry Agreement that would require TLDs to operate in a transparent manner consistent with general principles of openness and non-discrimination. Additionally, the proposed PIC Specification would include a provision to preclude registry operators from imposing eligibility criteria that limit registration of a generic string exclusively to a single person or entity and their "affiliates." The term "affiliate" is defined to mean a person or entity that, directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with, the person or entity specified, and "control" (including the terms "controlled by" and "under common control with") means the possession, directly or indirectly, of the power to direct or cause the direction of the management or policies of a person or entity, whether through the ownership of securities, as trustee or executor, by serving as an employee or a member of a board of directors or equivalent governing body, by contract, by credit arrangement or otherwise. [New gTLD (generic Top Level Domain) Registry Agreement § 2.9(c) <http://newgTlds.icann.org/en/applicants/agn/base-agreement-specs-29apr13-en.pdf> (<http://newgTlds.icann.org/en/applicants/agn/base-agreement-specs-29apr13-en.pdf>) [PDF, 600 KB]]

For applicants seeking to impose exclusive registry access for "generic strings", the NGPC is being asked to defer moving forward with the contracting process for these applicants, pending a dialogue with the GAC (Governmental Advisory Committee). The term "generic string" is defined in the PIC Specification to mean "a string consisting of a word or term that denominates or describes a general class of goods, services, groups, organizations or things, as opposed to distinguishing a specific brand of goods, services, groups, organizations or things from those of others."

To implement the advice in this way, the PIC Specification will define exclusive registry access as limiting registration of a generic string exclusively to a single person or entity and their affiliates (as defined above). All applicants would be required to respond by a specified date indicating whether (a) the applicant is prepared to accept the proposed PIC Specification that precludes exclusive registry access or (b) the applicant is unwilling to accept the proposed PIC Specification because the applicant intends to implement exclusive registry access.

Which stakeholders or others were consulted?

On 23 April 2013, ICANN (Internet Corporation for Assigned Names and Numbers) initiated a public comment forum to solicit input on how the NGPC should address GAC (Governmental Advisory Committee) advice regarding safeguards applicable to broad categories of new gTLD (generic Top Level Domain) strings <http://www.icann.org/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm> ([/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm](http://www.icann.org/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm)). The public comment forum closed on 4 June 2013. The NGPC has considered the community comments in formulating its response to the GAC (Governmental Advisory Committee)'s Category 2 Safeguard Advice.

What concerns or issues were raised by the community?

ICANN (Internet Corporation for Assigned Names and Numbers) received several responses from the community during the course of the public comment forum on broad categories of GAC (Governmental Advisory Committee)

Approved Resolutions | Meeting of the New gTLD Program Committee |... <http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-2...>

safeguard advice. Of the limited number of comments specific to the Category 2, Restricted Access safeguards, approximately 60% expressed support versus approximately 40% expressing concern or opposition. Supporting comments generally agreed that, for certain strings, restricted access is warranted. Opposing comments generally indicated that this is unanticipated and wholly new policy without justification and that these strings would be unfairly prejudiced in the consumer marketplace. Of the comments specific to the Category 2, Exclusive Access safeguards, approximately 86% expressed support versus approximately 14% expressing concern or opposition. Supporting comments indicated that exclusive registry access should "serve a public purpose." Others indicated that "closed generics" should not be allowed at all.

In adopting this Resolution, the NGPC specifically acknowledges comments from the community opposed to the NGPC accepting the [GAC \(Governmental Advisory Committee\)](#)'s advice. Opposing commenters generally expressed concern that this is new and unanticipated policy, contrary to the bottom-up process. They also indicated that the concept of public interest is vague and not adequately defined. The NGPC notes that the Beijing Communiqué was published to solicit public comment on the broad categories of the [GAC \(Governmental Advisory Committee\)](#)'s safeguard advice. This demonstrates ICANN (Internet Corporation for Assigned Names and Numbers)'s commitment to a bottom-up, multi-stakeholder model, and provided stakeholders with approximately six weeks (including the public comment and reply periods) to analyze, review and respond to the proposed recommendations. The NGPC views finding a workable solution to the [GAC \(Governmental Advisory Committee\)](#)'s advice as a step forward as the community continues to respond to the needs of registrants, the community and all stakeholders.

For the comments specifically concerning restricted registry access (i.e. Paragraph 1 of the Category 2 Advice), the NGPC takes note of the concerns expressed in the comments regarding the "general rule" that a [TLD \(Top Level Domain\)](#) should be operated in an open manner. The NGPC understands the [GAC \(Governmental Advisory Committee\)](#)'s advice for TLDs for which registration is restricted to generally be operated in an open manner to be a call for transparency, which is fundamental to providing consumers choice in the marketplace, and a goal that ICANN (Internet Corporation for Assigned Names and Numbers) supports. In light of the comments raised, ICANN (Internet Corporation for Assigned Names and Numbers) included new language in the PIC Specification to accept and respond to the [GAC \(Governmental Advisory Committee\)](#) advice regarding restricted access in a way that balances the concerns raised in the public comments with the [GAC \(Governmental Advisory Committee\)](#)'s advice for restricted TLDs. The revised PIC Specification establishes what it means for a [TLD \(Top Level Domain\)](#) to be operated consistent with principals of openness and non-discrimination. Specifically, by establishing, publishing and adhering to clear registration policies, the [TLD \(Top Level Domain\)](#) would fulfill its obligation to be operated in a "transparent manner consistent with general principles of openness and non-discrimination."

With respect to comments specifically regarding exclusive registry access safeguards (i.e. Paragraph 2 of the Category 2 Advice), the NGPC understands that the [GAC \(Governmental Advisory Committee\)](#) and other members of the community have expressed concerns regarding "closed generic" TLDs. In February 2013, the NGPC directed ICANN (Internet Corporation for Assigned Names and Numbers) staff to initiate a public comment period on the issue of closed generic [TLD \(Top Level Domain\)](#) applications so that the NGPC could understand and consider all views and potential ramifications related to closed generic TLDs. <<http://www.icann.org/en/news/announcements/announcement-2-05feb13-en.htm>>. In light of the comments raised in this public comment forum, the closed generics public comment forum, and the [GAC \(Governmental Advisory Committee\)](#) advice, ICANN (Internet Corporation for Assigned Names and Numbers) is proposing a way for a large number of strings to move forward while the community continues to work through the issue.

While respecting the community's comments, the NGPC revised the PIC Specification to address the [GAC \(Governmental Advisory Committee\)](#)'s advice regarding exclusive registry access. The proposed PIC Specification includes a provision to preclude registry operators from imposing eligibility criteria that limit registration of a generic string exclusively to a single person or entity and their "affiliates." The definition for "affiliates" is the definition in Section 2.9(c) of the New gTLD (generic Top Level Domain) Registry Agreement. For applicants seeking to impose exclusive registry access for "generic strings", the NGPC agrees to defer moving forward with the contracting process for these applicants, pending a dialogue with the [GAC \(Governmental Advisory Committee\)](#) to seek clarification

Approved Resolutions | Meeting of the New gTLD Program Committee |... <http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-2...>

regarding aspects of the advice, including key definitions, and its implementation. Revising the PIC Specification in this way permits the greatest number of strings to continue moving forward while recognizing the concerns raised in the community's comments, including additional policy work.

The complete set of public comments can be reviewed at: <http://www.icann.org/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm> (/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm).

What significant materials did the NGPC review?

As part of its deliberations, the NGPC reviewed the following significant materials and documents:

GAC (Governmental Advisory Committee) Beijing Communiqué: <http://www.icann.org/en/news/correspondence/gac-to-board-18apr13-en.pdf> (/en/news/correspondence/gac-to-board-18apr13-en.pdf) [PDF, 156 KB]

Public comments in response to broad categories of GAC (Governmental Advisory Committee) safeguard advice: <http://www.icann.org/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm> (/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm)

Report of Public Comments, New gTLD (generic Top Level Domain) Board Committee Consideration of GAC (Governmental Advisory Committee) Safeguard Advice dated 18 June 2013: <http://www.icann.org/en/news/public-comment/report-comments-gac-safeguard-advice-19jun13-en> (/en/news/public-comment/report-comments-gac-safeguard-advice-19jun13-en)

What factors did the Board find to be significant?

The Beijing Communiqué generated significant interest from the community and stimulated many comments. The NGPC considered the community comments, the GAC (Governmental Advisory Committee)'s advice transmitted in the Beijing Communiqué, and the procedures established in the AGB for addressing GAC (Governmental Advisory Committee) advice to the New gTLD (generic Top Level Domain) Program.

Are there positive or negative community impacts?

The adoption of the GAC (Governmental Advisory Committee) advice as provided in the attached Annex I (/en/groups/board/documents/resolutions-new-gtld-annex-i-agenda-2c-25jun13-en.pdf) [PDF, 52 KB] will assist with resolving the GAC (Governmental Advisory Committee) advice in a manner that permits the greatest number of new gTLD (generic Top Level Domain) applications to continue to move forward as soon as possible. However, applicants seeking to impose exclusive registry access would not be able to progress to the contracting process at this time if the NGPC adopts the proposed Resolution. Those applicants would be on hold pending the outcome of the dialogue with the GAC (Governmental Advisory Committee).

Are there fiscal impacts or ramifications on ICANN (Internet Corporation for Assigned Names and Numbers) (strategic plan, operating plan, budget); the community; and/or the public?

There are no foreseen fiscal impacts associated with the adoption of this resolution.

Are there any security, stability or resiliency issues relating to the DNS (Domain Name System)?

Approval of the proposed resolution will not impact security, stability or resiliency issues relating to the DNS (Domain Name System).

Is this either a defined policy process within ICANN (Internet Corporation for Assigned Names and Numbers)'s Supporting Organizations or ICANN (Internet Corporation for Assigned Names and Numbers)'s Organizational Administrative Function decision requiring public comment or not requiring public comment?

On 23 April 2013, ICANN (Internet Corporation for Assigned Names and Numbers) initiated a public comment forum to solicit input on how the NGPC should address GAC (Governmental Advisory Committee) advice regarding safeguards applicable to broad categories of new gTLD (generic Top Level Domain) strings <http://www.icann.org/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm> (/en/news/public-comment/gac-safeguard-advice-23apr13-en.htm). The public comment forum closed on 4 June 2013.

d. Singular & Plural Versions of the Same String as a TLD (Top Level Domain)

Whereas, the GAC (Governmental Advisory Committee) met during the ICANN (Internet Corporation for Assigned

Approved Resolutions | Meeting of the New gTLD Program Committee |... <http://www.icann.org/cn/groups/board/documents/resolutions-new-gtld-2...>

Names and Numbers) 46 meeting in Beijing and issued a Communiqué on 11 April 2013 ("Beijing Communiqué");

Whereas, the NGPC met on 8 and 18 May and 4 and 11 June 2013, to consider a plan for responding to the GAC (Governmental Advisory Committee)'s advice on the New gTLD (generic Top Level Domain) Program, transmitted to the Board through its Beijing Communiqué;

Whereas, on 4 June 2013, the NGPC took action accepting GAC (Governmental Advisory Committee) advice identified in the GAC (Governmental Advisory Committee) Register of Advice as "2013-04-11-PluralStrings" and agreed to consider whether to allow singular and plural versions of the same string;

Whereas, the NGPC met on 11 June 2013 to consider the GAC (Governmental Advisory Committee) Beijing advice regarding singular and plural versions of the same string; and

Whereas, after careful consideration of the issues, review of the comments raised by the community, the process documents of the expert review panels, and deliberations by the NGPC, the NGPC has determined that no changes to the ABG are needed to address potential consumer confusion specifically resulting from allowing singular and plural versions of the same strings;

Whereas, the NGPC is undertaking this action pursuant to the authority granted to it by the Board on 10 April 2012, to exercise the ICANN (Internet Corporation for Assigned Names and Numbers) Board's authority for any and all issues that may arise relating to the New gTLD (generic Top Level Domain) Program.

Resolved (2013.06.25.NG07), the NGPC has determined that no changes are needed to the existing mechanisms in the Applicant Guidebook to address potential consumer confusion resulting from allowing singular and plural versions of the same string.

Rationale for Resolution 2013.06.25.NG07

Why the NGPC is addressing the issue?

Article XI, Section 2.1 of the ICANN (Internet Corporation for Assigned Names and Numbers) Bylaws (<http://www.icann.org/en/about/governance/bylaws#XI> (/en/about/governance/bylaws#XI)) permit the GAC (Governmental Advisory Committee) to "put issues to the Board directly, either by way of comment or prior advice, or by way of specifically recommending action or new policy development or revision to existing policies." The GAC (Governmental Advisory Committee) issued advice to the Board on the New gTLD (generic Top Level Domain) Program through its Beijing Communiqué dated 11 April 2013. The ICANN (Internet Corporation for Assigned Names and Numbers) Bylaws require the Board to take into account the GAC (Governmental Advisory Committee)'s advice on public policy matters in the formulation and adoption of the policies. If the Board decides to take an action that is not consistent with the GAC (Governmental Advisory Committee) advice, it must inform the GAC (Governmental Advisory Committee) and state the reasons why it decided not to follow the advice. The Board and the GAC (Governmental Advisory Committee) will then try in good faith to find a mutually acceptable solution. If no solution can be found, the Board will state in its final decision why the GAC (Governmental Advisory Committee) advice was not followed.

In its Beijing Communiqué, the GAC (Governmental Advisory Committee) advised the Board that due to potential consumer confusion, the Board should "reconsider its decision to allow singular and plural version of the same strings." On 4 June 2013, the NGPC accepted the GAC (Governmental Advisory Committee)'s advice to consider this issue. The NGPC met on 11 June 2013 to discuss this advice, and to consider whether any changes are needed to the New gTLD (generic Top Level Domain) Program to address singular and plural versions of the same string.

What is the proposal being considered?

The NGPC is considering whether any changes are needed to the New gTLD (generic Top Level Domain) Program (i.e. the Applicant Guidebook) as a result of the NGPC considering whether to allow singular and plural versions of the same strings as requested by the GAC (Governmental Advisory Committee) in its Beijing Communiqué.

Which stakeholders or others were consulted?

On 18 April 2013, ICANN (Internet Corporation for Assigned Names and Numbers) posted the GAC (Governmental Advisory Committee) advice and officially notified applicants of the advice, <http://newgtlds.icann.org>

Approved Resolutions | Meeting of the New gTLD Program Committee | ... <http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-2...>

[/en/announcements-and-media/announcement-18apr13-en](#) (<http://newgtlds.icann.org/en/announcements-and-media/announcement-18apr13-en>) triggering the 21-day applicant response period pursuant to the Applicant Guidebook Module 3.1 <<http://newgtlds.icann.org/en/applicants/gac-advice-responses> (<http://newgtlds.icann.org/en/applicants/gac-advice-responses>)>. The NGPC considered the applicant responses in considering this issue.

To note, a handful of unique applicants, representing nearly 400 application responses, addressed this piece of GAC (Governmental Advisory Committee) advice. Most were against changing the existing policy but with one identified in support of the GAC (Governmental Advisory Committee)'s concern. The supporting applicant has filed a string confusion objection. Those not supporting the GAC (Governmental Advisory Committee)'s concern indicated this topic was agreed as part of the AGB and is addressed in the evaluation processes. The full summary of applicant responses can be reviewed at: <<http://newgtlds.icann.org/en/applicants/gac-advice-responses> (<http://newgtlds.icann.org/en/applicants/gac-advice-responses>)>.

What concerns or issues were raised by the community?

In September 2007, the GNSO (Generic Names Supporting Organization) issued a set of recommendations (approved by the ICANN (Internet Corporation for Assigned Names and Numbers) Board in June 2008) to implement a process to allow for the introduction of new gTLDs. These include a recommendation that new gTLD (generic Top Level Domain) strings must not be confusingly similar to an existing top-level domain or a reserved name. The GNSO (Generic Names Supporting Organization) constituency groups lodged comments during that time, and these comments were considered as part of the approval of the Program. The NGPC considered these community comments as part of its deliberations.

More recently, ICANN (Internet Corporation for Assigned Names and Numbers) posted the GAC (Governmental Advisory Committee)'s Beijing Communiqué and officially notified applicants of the advice, <<http://newgtlds.icann.org/en/announcements-and-media/announcement-18apr13-en> (<http://newgtlds.icann.org/en/announcements-and-media/announcement-18apr13-en>)> triggering the 21-day applicant response period pursuant to the AGB Module 3.1.

Multiple members of the ICANN (Internet Corporation for Assigned Names and Numbers) and New gTLD (generic Top Level Domain) applicant communities have raised concerns to the ICANN (Internet Corporation for Assigned Names and Numbers) Board regarding the GAC (Governmental Advisory Committee)'s advice regarding singular and plural versions of the same string. Some of the concerns raised by the community are as follows:

- Allowing singular and plural versions of the same string amounts to a "serious flaw" in the Program, and the Program should not rely on the self-interest of others to file objections to avoid string confusion.
- The independent panels have ruled and it would not be appropriate for either ICANN (Internet Corporation for Assigned Names and Numbers) or the Board to overturn these decisions. The findings of the independent string similarity review panel should not be upset, absent a finding of misconduct.
- The Board approved the evaluation process, which included independent assessment of each application against AGB criteria, appropriately away from the interests of those with stakes in the outcome.
- ICANN (Internet Corporation for Assigned Names and Numbers) should not change course on this issue, as it would open the door to one stakeholder group undoing independently arrived-at results because it disagrees with the outcome.

The concerns raised by the community highlight the difficulty of the issue and the tension that exists between minimizing user confusion while encouraging creativity, expression and competition. The NGPC weighed these comments during its deliberations on the issue.

What significant materials did the NGPC review?

The NGPC reviewed and considered the following significant materials as part of its consideration of the issue:

- GAC (Governmental Advisory Committee) Beijing Communiqué: <http://www.icann.org/en/news/correspondence/gac-to-board-18apr13-en.pdf> [PDF, 156 KB]
- Applicant responses to GAC (Governmental Advisory Committee) advice: <http://newgtlds.icann.org/en/applicants/gac-advice-responses> (<http://newgtlds.icann.org/en/applicants/gac-advice-responses>)

- String Similarity Contention Sets <<http://www.icann.org/en/news/announcements/announcement-26feb13-en.htm> (/en/news/announcements/announcement-26feb13-en.htm)>

What factors did the NGPC find to be significant?

The NGPC considered several significant factors during its deliberations about whether to allow singular and plural version of the same strings. The NGPC had to balance the competing interests of each factor to arrive at a decision. The following are among the factors the NGPC found to be significant:

- The NGPC considered whether it was appropriate to reject the work of the expert review panel and apply its own judgment to a determination of what rises to the level of probable user confusion. The NGPC considered whether the evaluation process would be undermined if it were to exert its own non-expert opinion and override the determination of the expert panel. It also considered whether taking an action to make program changes would cause a ripple effect and re-open the decisions of all expert panels.

The NGPC considered that the objective of the string similarity review in the AGB is to prevent user confusion and loss of confidence in the DNS (Domain Name System) resulting from delegation of many similar strings. In the AGB, "similar" means strings so similar that they create a probability of user confusion if more than one of the strings is delegated into the root zone. During the policy development and implementation design phases of the New gTLD (generic Top Level Domain) Program, aural and conceptual string similarities were considered. These types of similarity were discussed at length, yet ultimately not agreed to be used as a basis for the analysis of the string similarity panels' consideration because on balance, this could have unanticipated results in limiting the expansion of the DNS (Domain Name System) as well as the reach and utility of the Internet. However, the grounds for string confusion objections include all types of similarity, including visual, aural, or similarity of meaning. All new gTLD (generic Top Level Domain) applicants had standing to file a string confusion objection against another application.

- The NGPC considered the objective function of the string similarity algorithm in the AGB (§ 2.2.1.1.2) and the results it produced. SWORD assisted ICANN (Internet Corporation for Assigned Names and Numbers) with the creation of an algorithm that helped automate the process for objectively assessing similarity among proposed and existing TLD (Top Level Domain) strings. Various patent and trademark offices throughout the world use SWORD's verbal search algorithms. The String Similarity Panel was informed in part by the algorithmic score for the visual similarity between each applied-for string and each of other existing and applied-for TLDs and reserved names. The score provided one objective measure for consideration by the panel, as part of the process of identifying strings likely to result in user confusion. However, this score was only indicative and the panel's final determination was based on careful review and analysis. A full consideration of potential consumer confusion issues is built into the procedures that have been applied in the analysis of the strings.
- The NGPC reflected on existing string similarity in the DNS (Domain Name System) and considered the positive and negative impacts. The NGPC observed that numerous examples of similar strings, including singulars and plurals exist within the DNS (Domain Name System) at the second level. Many of these are not registered to or operated by the same registrant. There are thousands of examples including:

| | |
|-----------|------------|
| auto.com | autos.com |
| car.com | cars.com |
| new.com | news.com |
| store.com | stores.com |

- The NGPC considered the process used by the panel of experts from InterConnect Communications working in conjunction with the University College London to perform a visual similarity review to prevent used confusion and loss of confidence in the DNS (Domain Name System) resulting fro the delegation of similar strings. The panel made its assessments using the standard defined in the Applicant Guidebook: String confusion exists

Approved Resolutions | Meeting of the New gTLD Program Committee |... <http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-2...>

where a string so nearly resembles another visually that it is likely to deceive or cause confusion. For the likelihood of confusion to exist, it must be probable, not merely possible that confusion will arise in the mind of the average, reasonable Internet user. Mere association, in the sense that the string brings another string to mind, is insufficient to find a likelihood of confusion. This panel utilized its independent expertise, including in linguistics, to perform the review against the criteria in the Applicant Guidebook. ICANN (Internet Corporation for Assigned Names and Numbers) did not provide any instructions to the panel outside of the criteria specified in the Applicant Guidebook, including any pre-judgment of whether singular or plural versions of strings should be considered visually similar.

- The NGPC considered whether there were alternative methods to address potential user confusion if singular and plural versions of the same string are allowed to proceed. The NGPC discussed the String Confusion Objection mechanism in the AGB, and noted that string confusion objections are not limited to visual similarity, but may include any type of similarity, including visual, aural, or similarity of meaning. The DRSP panels reviewing string confusion objections use the following standard for assessing string confusion, as specified in the Applicant Guidebook: String confusion exists where a string so nearly resembles another that it is likely to deceive or cause confusion. For a likelihood of confusion to exist, it must be probable, not merely possible that confusion will arise in the mind of the average, reasonable Internet user. Mere association, in the sense that *the string brings another string to mind, is insufficient to find a likelihood of confusion*. The NGPC took note of the fact that in the case of a successful string confusion objection, either the application would not proceed (for an objection by an existing gTLD (generic Top Level Domain) operator) or an existing contention set would be modified to include the application subject to the objection (for an objection by another gTLD (generic Top Level Domain) applicant).
- The NGPC took note of the objections filed during the objection period, which closed on 13 March 2013. All new gTLD (generic Top Level Domain) applicants had standing to file a string confusion objection against another application. By the end of the objection period, a total of 67 string confusion objections were filed (see <http://newgtlds.icann.org/en/program-status/odr/filings> (<http://newgtlds.icann.org/en/program-status/odr/filings>)). Based on staff analysis, there were a total of 26 singular/plural applied-for, English language strings. The strings in these pairs had a total of 21 string similarity objections filed against them.

Are there positive or negative community impacts?

The string similarity review is the implementation of the GNSO (Generic Names Supporting Organization)'s policy recommendation 2: "Strings must not be confusingly similar to an existing top-level domain or a Reserved Name." As noted above, the objective of the string similarity review is to prevent user confusion and loss of confidence in the DNS (Domain Name System) resulting from delegation of many similar strings. A full consideration of potential consumer confusion issues is built into the procedures that have been applied in the analysis of the strings. The adoption of the proposed resolution will assist with continuing to resolve the GAC (Governmental Advisory Committee) advice in manner that permits the greatest number of new gTLD (generic Top Level Domain) applications to continue to move forward as soon as possible.

Are there fiscal impacts or ramifications on ICANN (Internet Corporation for Assigned Names and Numbers) (strategic plan, operating plan, budget); the community; and/or the public?

There are no foreseen fiscal impacts associated with the adoption of this resolution.

Are there any security, stability or resiliency issues relating to the DNS (Domain Name System)?

The security, stability and resiliency issues relating to the DNS (Domain Name System) were considered when the AGB was adopted. The NGPC's decision does not propose any changes to the existing program in the AGB, and thus there are no additional foreseen issues related to the security, stability or resiliency of the DNS (Domain Name System).

Is this either a defined policy process within ICANN (Internet Corporation for Assigned Names and Numbers)'s Supporting Organizations or ICANN (Internet Corporation for Assigned Names and Numbers)'s Organizational Administrative Function decision requiring public comment or not requiring public comment?

Approved Resolutions | Meeting of the New gTLD Program Committee |... <http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-2...>

ICANN (Internet Corporation for Assigned Names and Numbers) posted the GAC (Governmental Advisory Committee) advice and officially notified applicants of the advice on 18 April 2013 <<http://newgtlds.icann.org/en/announcements-and-media/announcement-18apr13-en>>. This triggered the 21-day applicant response period pursuant to the Applicant Guidebook Module 3.1. No additional public comment is required as the NGPC's action does not propose any policy or program changes to the New gTLD (generic Top Level Domain) Program.

e. **IGO (Intergovernmental Organization) Protection**

No resolution taken.

f. **AOB**

No resolution taken.

Published on 27 June 2013

Board (</en/groups/board>)

Meetings (</en/groups/board/meetings>)

Documents (</en/groups/board/documents>)

Board & Chair Self-Appraisal (</en/groups/board/documents/appraisals>)

Board Compensation Election (</en/groups/board/documents/ce>)

Procedure Manual (</en/groups/board/documents/draft-procedure-manual-09oct12-en>)

Resolutions Wiki (<https://community.icann.org/display/tap/ICANN+Board+Resolutions>)

Statements of Interest (</en/groups/board/documents/sois>)

Audit Committee (</en/groups/board/audit>)

Board Governance Committee (</en/groups/board/governance>)

Compensation Committee (</en/groups/board/compensation>)

Executive Committee (</en/groups/board/executive>)

Finance Committee (</en/groups/board/finance>)

Global Relationships Committee (</en/groups/board/global-relationships>)

IANA Committee (</en/groups/board/iana>)

New gTLD Program Committee (</en/groups/board/new-gtld>)

Public and Stakeholder Engagement Committee (</en/groups/board/participation>)

Risk Committee (</en/groups/board/risk>)

Structural Improvements Committee (</en/groups/board/improvements>)

ALAC (<http://www.atlarge.icann.org>)

ASO (<http://aso.icann.org>)

- [ccNSO \(http://ccnso.icann.org\)](http://ccnso.icann.org)
- [GAC \(http://gac.icann.org\)](http://gac.icann.org)
- [GNSO \(http://gnso.icann.org\)](http://gnso.icann.org)
- [IETF \(/en/groups/ietf\)](/en/groups/ietf)
- [NRO \(http://www.nro.net\)](http://www.nro.net)
- [NomCom \(http://nomcom.icann.org\)](http://nomcom.icann.org)
- [RSSAC \(/en/groups/rssac\)](/en/groups/rssac)
- [SSAC \(/en/groups/ssac\)](/en/groups/ssac)
- [Technical Liaison Group \(/en/groups/tlg\)](/en/groups/tlg)
- [Other Groups \(/en/groups/other\)](/en/groups/other)
- [Past Groups \(/en/groups/past\)](/en/groups/past)
- [Organizational Reviews \(/en/groups/reviews\)](/en/groups/reviews)

Stay Connected

- News Alerts: [HTML](#) [Plain Text](#)
- Newsletter: [HTML](#) [Plain Text](#)
- Compliance Newsletter: [HTML](#) [Plain Text](#)
- Policy Update: [HTML](#) [Plain Text](#)

Subscribe

- Follow us @icann (<https://twitter.com/#!/icann/>)
- Videos (<http://www.youtube.com/icannnews>)
- Photos on Flickr (<http://www.flickr.com/photos/icann/>)
- Facebook (<http://www.facebook.com/icannorg>)
- ICANN Blog (<http://blog.icann.org/>)
- Community Wiki (<https://community.icann.org/>)
- Planet ICANN (</en/groups/planet-icann>)
- RSS Feeds (</en/news/rss>)

Approved Resolutions | Meeting of the New gTLD Program Committee |... <http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-2...>

- [GNSO \(http://gnso.icann.org\)](http://gnso.icann.org)
- [RSSAC \(http://en/groups/rssac\)](http://en/groups/rssac)
- [SSAC \(http://en/groups/ssac\)](http://en/groups/ssac)
- [Community Wiki \(http://community.icann.org\)](http://community.icann.org)
- [Meetings \(http://meetings.icann.org\)](http://meetings.icann.org)
- [New gTLDs \(http://newgtlds.icann.org\)](http://newgtlds.icann.org)
- [Help](#)

[\(/en/help\)](#)
[Acronym Helper](#)



**Before the
DEPARTMENT OF COMMERCE
UNITED STATES PATENT AND TRADEMARK OFFICE**

| | | |
|---|--|--|
| <p>In the Matter of</p> <p>Voluntary Best Practices Study</p> | <p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p> | <p>Docket No. PTO-C-2013-0036</p> <p>Submitted August 21, 2013</p> |
|---|--|--|

**COMMENTS OF THE
MOTION PICTURE ASSOCIATION OF AMERICA, INC.**

I. PRELIMINARY COMMENTS

The Motion Picture Association of America, Inc. (“MPAA”) is pleased to provide these comments in response to the Request of the United States Patent and Trademark Office for Public Comments: Voluntary Best Practices Study (Docket No. PTO-C-2013-0036) appearing at 78 Fed. Reg. 37,210 (June 20, 2013).

The MPAA is a not-for-profit trade association founded in 1922 to address issues of concern to the motion picture industry. The MPAA’s member companies are: Paramount Pictures Corp., Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corp., Universal City Studios LLC, Walt Disney Studios Motion Pictures, and Warner Bros. Entertainment Inc. These companies and their affiliates are the leading producers and distributors of filmed entertainment in the theatrical, television, and home-entertainment markets. The MPAA’s members produce, distribute, and own tens of thousands of extremely valuable copyrighted works – works that, unfortunately, are subject to widespread piracy, resulting in billions of dollars annually in financial losses and undermining legitimate business models.

The MPAA’s members employ various strategies and tactics to combat such piracy, which include efforts aimed at educating consumers about intellectual property and piracy and directing them to legitimate offerings, as well as targeting, through appropriate legal means, enterprises seeking to enrich themselves at the expense of content creators and owners. In particular, MPAA members focus on making their works available to consumers in a wide variety of formats, on various platforms, at different price points, to meet consumer demand. In addition, they employ digital rights management technologies to thwart unauthorized copying. They make extensive use of the notice-and-takedown process set forth in Section 512 of the Digital Millennium Copyright Act. They bring copyright infringement lawsuits in federal court. They refer particularly egregious commercial infringers to law-enforcement authorities. And, as

relevant here, they engage in a variety of cooperative, voluntary initiatives with participants in the Internet ecosystem.

To achieve its important societal goal of encouraging creativity – by acting as the “engine of free expression”¹ – it is necessary that the copyright system include “appropriate enforcement mechanisms to combat piracy, so that all stakeholders benefit from the protection afforded by copyright.”² Thus all players in the Internet ecosystem – copyright owners, as well as the various intermediaries that facilitate online commerce and speech – have a responsibility and must play a meaningful role in addressing the problem of rampant piracy on the Web. This is not only true as a matter of law; it is also a matter of corporate ethics and an acknowledgment that stakeholders whose systems, networks and services are used by unrelated third parties to commit wrongdoing are oftentimes best placed to assist in the prevention of that harm.

One form of such cooperation with other players in the ecosystem is taking commercially reasonable, technologically feasible steps to help curb copyright infringement. Therefore, as a general proposition, the MPAA supports – and urges the PTO and other government entities to encourage all relevant parties to support – cooperative, voluntary initiatives. Such initiatives, which range from precatory sets of “best practices” (which can be either unilateral or negotiated among various parties) such as the UGC Principles³ to formal, binding agreements (such as the Copyright Alert System⁴), can, in certain circumstances, improve upon default legal standards (such as the DMCA), and are often preferable to expensive, contentious civil litigation and criminal enforcement actions. But, as we detail below, cooperative, voluntary initiatives are not a panacea, and they are not appropriate to address all forms of piracy. Some voluntary initiatives work well; some have more modest success; and some are simply not effective. As noted below, some players, such as major Internet service providers, via the Copyright Alert System, and user-generated content sites, via the UGC Principles, have shown admirable willingness to enter into voluntary agreements and take concrete and effective anti-piracy measures, and should be applauded for the constructive roles they have played. Unfortunately others, such as the major search engines, have largely refused to take a proactive role in addressing the problems of illegal activity online.

Voluntary initiatives like the ones described below are, and will remain, a complement to – not a substitute for – other anti-piracy initiatives. And it must always be remembered that, when negotiating voluntary agreements, the parties are always bargaining in the shadow of the law. In other words, a party’s willingness to commit to a particular practice will depend to a significant degree on what it perceives to be the legal consequence (or lack thereof) of continuing its current course of action, and not committing to any voluntary agreement. Thus

¹ *Harper & Row, Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 558 (1985).

² The Department of Commerce Internet Policy Task Force, “Copyright Policy, Creativity, and Innovation in the Digital Economy,” Message from Secretary of Commerce Penny Pritzker, July 2103, available at <http://www.uspto.gov/news/publications/copyrightercempaper.pdf>.

³ See *infra*, Section II.E.

⁴ See *infra*, Section II.A; see also comments submitted by the Center for Copyright Information.

improvements in the law are likely to encourage recalcitrant players to engage in voluntary initiatives.

MPAA details below several of the specific initiatives in which it, its members, and other copyright owners have participated in recent years.

II. SPECIFIC INITIATIVES IN WHICH CONTENT OWNERS ARE INVOLVED

A. Copyright Alert System

The Copyright Alert System (“CAS”) is a program to address one specific form of piracy: the use of peer-to-peer networks to download and distribute movies, television shows, and music over the Internet (sometimes referred to as “file-sharing”). The participants are the major movie studios (via the MPAA) and record labels, a large group of independent movie producers and record labels, and five major U.S. ISPs (Comcast, AT&T, Verizon, Cablevision, and Time Warner Cable). Under the CAS, copyright owners scan publicly-accessible peer-to-peer networks to detect unauthorized distributions of their works, and then send notices of such infringements to the ISPs through which these works are being made available. The ISPs then send “Copyright Alerts” to the subscribers associated with such infringing activity. The first alerts are purely educational, informing the subscriber that he/she has been detected engaging in suspected copyright infringement, and providing instructions on how to stop, as well as information about where to legally access movies and music online. But if the subscriber persists in his/her wrongdoing, later Alerts will impose “Mitigation Measures,” which may, depending on the particular ISP, include temporary slowing of Internet access or suspension of service pending completion of an online course or contact with an appropriate ISP representative. At no time is the subscriber’s personal information provided to the copyright owners, and the system includes a dispute-resolution system administered by the American Arbitration Association known as the “Independent Review Program” through which subscribers may challenge Copyright Alerts that they believe were sent in error.

The CAS launched in February 2013, and the participants – including the Center for Copyright Information (“CCI”), the body established to administer the program – are only now beginning to evaluate the results. While it is too soon to comment on the efficacy of the CAS, MPAA will consider the program a success if it fulfills its goal of educating the public about illegal distribution and downloading of copyrighted works, reducing the prevalence of such activity, and ultimately encouraging users to shift from the use of illegal peer-to-peer services to legitimate sources of content, including the hundreds of legitimate digital services that currently distribute content online.⁵ The MPAA and its members are also hopeful that the CAS will serve as a stepping-stone or model for similar cross-industry collaborations to address forms of piracy other than peer-to-peer downloading and distribution.

⁵ Additional information about the CAS and CCI may be found at <http://www.copyrightinformation.org/>.

B. Advertising Networks

The past 15 months have witnessed three significant announcements by players in the online advertising ecosystem in the U.S. meant to address the problem of advertisements placed on sites engaged in piracy:

- On May 3, 2012, the Association of National Advertisers (“ANA”) and the American Association of Advertising Agencies (“4As”), with the support of the Interactive Advertising Bureau (“IAB”) released a Statement of Best Practices that “encourages all marketers to take affirmative steps to address the serious problems of online piracy and counterfeiting.”⁶ The statement specifically advises marketers to include language in their contracts and insertion orders to prevent ads from appearing on “rogue” sites dedicated to infringement of others’ intellectual property rights. As the MPAA stated upon the announcement, “This is a major step forward by the associations representing online advertisers and marketers to help ensure that their ads are not unintentionally providing financial support and credibility for online sites whose primary purpose is to steal and market intellectual property.”

- Only July 15, 2013 several major participants in the online advertising ecosystem, including Google, Yahoo, and AOL, with the support of the IAB, announced a set of best practices to address the problem of advertisements placed on sites engaged in piracy.⁷ While we appreciate the recognition by ad agencies, networks and others of the problem, and applaud the support of the Administration’s Intellectual Property Enforcement Coordinator for initiatives such as this, we are disappointed in the particular set of best practices announced in July, which we consider merely an incremental step forward that addresses only a narrow subset of the problem and places a disproportionate amount of the burden on rightsholders. Absent meaningful proactive steps by players in every sector – advertisers, ad agencies, ad placement services, online ad exchanges and rightsholders – the results will be similarly incremental. It is our hope that all parties will work together and build upon July’s announcement. We encourage the Administration to continue its leadership and convene a meaningful and transparent multi-stakeholder process, with a goal of developing a comprehensive and effective response to significantly reduce the presence of legitimate advertising on illegal Internet sites. We especially encourage an approach that would incorporate information from independent third-party organizations such as DoubleVerify⁸, Integral Ad Science⁹, Veri-Site¹⁰ and whiteBULLET¹¹ regarding the amount of infringement on particular sites, enabling

⁶ See http://www.anaa.org/news/press/Pages/050312_online_piracy.aspx (press release); see also http://www.anaa.org/news/press/Pages/050312_online_piracy.aspx (text of best practices).

⁷ See <http://www.2013ippractices.com/>

⁸ See <http://www.doubleverify.com/>

⁹ See <http://integralads.com/>

¹⁰ See <http://www.veri-site.com/>

¹¹ See <http://www.white-bullet.com/>

advertisers, ad networks and others to make informed decisions about where their ads should appear, thus avoiding placement on sites with high levels of infringement.

- Lastly, on July 25, 2013, the IAB announced its “Quality Assurance Guidelines 2.0.”¹² Unfortunately, these guidelines are largely toothless when it comes to copyright infringement. While the QAG states expressly that “[c]omplaints regarding QAG non-compliance may affect certification ... *IP infringement complaints do not.*” (emphasis added). That is so even though another section of QAG sets forth a “prohibition” on sale of ad inventory on “copyright infringement” sites. Moreover, as with the Google/Yahoo/AOL best practices referenced above, MPAA and its members were also disappointed that these best practices place nearly all of the burden of ensuring that ads do not appear on sites dedicated to piracy upon rightsholders, and do not adequately encourage other players in the ecosystem to assume their share of responsibility for addressing the problem.

In addition to these examples in the U.S., major rightsholders and players in the online advertising ecosystem in the U.K. have entered into voluntary agreements intended to combat the problem of advertising on sites that contain large amounts of infringing material. Pursuant to the program, rightsholders (represented by the Federation Against Copyright Theft, of which MPAA is a member, the British Phonographic Industry, and the Publishers’ Association) submit evidence of infringement to the National Fraud Intelligence Bureau (“NFIB”), a division of the City of London Police. Once NFIB is satisfied that the submitted evidence meets criteria set forth in the agreements, they may attempt to contact the site operators and ask them to address the infringements.¹³ Also, NFIB will, after allowing time for the site operators to respond, provide a register of the targeted websites to representatives of entities within the U.K.-based advertising ecosystem in the hope that this will encourage brand owners, advertisers and those who purchase advertising for them to address the concerns. Although this is a small pilot program in its early days, initial results look promising in terms of responses from website operators as well as a reduction in the volume and variety of advertising observed on a number of the sites, and this may prove to be a useful model for the U.S. to observe.

The varying strengths of these sets of best practices demonstrates that all voluntary initiatives must be evaluated on their own merits; to say as a general matter that voluntary initiatives are generally a good thing is not to say that any particular voluntary initiative will be effective.

C. Payment Processors

Payment processors remain a lynchpin in helping to reduce potential financial gains by the operators of infringing websites. Well-documented and oft-publicized voluntary efforts between rights-holders and payment processors have resulted in the creation of new relationships

¹² See http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-072513 (press release); see also <http://www.iab.net/media/file/QualityAssuranceGuidelines7252013.pdf> (Quality Assurance Guideline Version 2.0).

¹³ See BBC, “London police start to target pirate websites,” June 4, 2013, available at <http://www.bbc.co.uk/news/technology-22768850>

among interested parties, and we applaud the IPEC's efforts to facilitate and encourage these efforts. Consequently, the creation of both systems and processes for addressing the issues have produced meaningful results, at least with respect to sites that traffic in counterfeit hard goods (e.g., pirated DVDs and Blu-ray discs). We have also seen some positive results with respect to sites that traffic in illegal devices and software that circumvent technical protection measures, although our experience with respect to cooperation in that area has been more mixed. In addition to more consistent cooperation, we would like to see greater leadership from the major credit card networks on the problem of so-called "cyberlockers," which are a category of rogue sites engaged in digital piracy that are typically supported by paid subscriptions. The MPAA and its members continue to engage in dialogue with the card networks and other payment processors and welcome greater and more effective measures that can be taken with respect to cyberlockers. Due to the pivotal position that payment processing holds in regards to the online ecosystem, both the MPAA and payment processors must maintain vigilance in this important area while expanding their efforts to address new forms of copyright infringement as they arise.

D. Search Engines

Search engines represent an obvious and pivotal presence within the online ecosystem. Search plays an important role for those seeking out content – including infringing content – as both a discovery and navigational tool. Many users find infringing content through search engines when they were simply looking for that content – quite possibly from a legitimate source. However, "free" options are highlighted for the user, both in suggested search terms (like autocomplete) and in the search results themselves. When one considers the discovery aspect of search – a significant number of users first find a rogue site through search but then navigate directly to that site upon subsequent visits – the importance of search as a contributor to internet piracy becomes clear. Unfortunately, search engines have thus far failed to undertake sufficiently effective action to address their role in directing users to infringing (and otherwise illegal) content. To give one prominent example, Google, the search engine with by far the largest market share, announced in August 2012 that it would alter its search algorithm to begin factoring in takedown notices for Google links to infringing content when displaying search results, *i.e.*, the more takedown notices that Google received leading to infringing content on a particular site, the lower the site would be listed in Google search results, lessening the chance that users would click on links to that site. While at the time we applauded Google's announcement as a step in the right direction, unfortunately the results to date have been disappointing; the evidence demonstrates that Google's algorithm change has *not* resulted in a demonstrable down-listing of pirate sites.¹⁴

MPAA and its members have shared their concerns with search engines. To date however, the search engines have not undertaken the range and depth of efforts required to

¹⁴ A study by the Recording Industry Association of America concluded, "Six months [after the announcement of Google's algorithm change], we have found no evidence that Google's policy has had a demonstrable impact on demoting sites with large amounts of piracy. These sites consistently appear at the top of Google's search results for popular songs or artists." See Recording Industry Association of America, "Six Months Later – A Report Card on Google's Demotion of Pirate Sites," Feb. 21, 2013, available at <http://76.74.24.142/3CF95E01-3836-E6CD-A470-1C2B89DE9723.pdf>.

address these concerns adequately, despite the fact that the leading search engines have repeatedly stated that the theft of intellectual property is a serious problem.¹⁵

E. User Generated Content Sites

In October 2007, a number of leading producers of audiovisual content (including several of the MPAA's members) and operators of websites that host user-generated content ("UGC") signed on to the "Principles for User Generated Content Services" (the "UGC Principles") to address the problem of infringing content hosted on UGC services.¹⁶ Most significantly, the UGC Principles call on UGC sites to implement automated filtering technologies that block the upload of infringing material. From content owners' perspective, the use of automated filters is a major improvement over the baseline DMCA notice-and-takedown system, which often results in the re-posting of infringing content immediately after it is removed. The promulgation of the UGC Principles has played a major role in the widespread adoption of filtering technologies by responsible UGC sites. Even sites that have not themselves signed on to the UGC Principles – most prominently YouTube – have nonetheless deployed filters to identify copyrighted content, providing the rightsholders with the option to block or monetize the content and share revenues. MPAA thus believes that the UGC principles have played a major role in making adoption of filtering technologies a widespread industry practice, not just in the U.S. but also in international territories like China. We encourage the administration to advance the successful and balanced framework of the UGC Principles in its international outreach efforts, especially to encourage similar progress in Russia.

F. Domain Name Registration

Although voluntary initiatives have met with some success domestically, the global nature of the Internet continues to pose challenges for US copyright holders. Notably, the U.S. Government (through NTIA) committed in the 2013 Joint Strategic Plan for Intellectual Property Enforcement to work with the Internet Corporation for Assigned Names and Numbers ("ICANN") – a private sector, non-profit global organization – to improve the new generic top-level domain ("gTLD") program, including through "mechanisms for intellectual property protection."¹⁷

ICANN recently adopted a resolution requiring safeguards to address the problem of Registered Domain Name Holders engaging in practices that are illegal or harmful to Internet

¹⁵ In addition to the down-ranking of sites based on infringement notices described above, other steps MPAA believes search engines should undertake to address their role in directing traffic to infringing material would include: 1) de-indexing (*i.e.*, not listing in search results) sites substantially dedicated to infringement; 2) de-indexing multiple infringements of the same content on the same site; 3) providing "red light" warnings about rogue sites to warn users on the search results page before they permit them to click links they provide to rogue sites (similar to the system Google currently uses to warn users of links to pages that may contain malware); and 4) adjusting "autocomplete" and related features so that they don't suggest queries that lead to rogue sites.

¹⁶ See <http://www.ugcprinciples.com/>

¹⁷ See <http://www.whitehouse.gov/sites/default/files/omb/IPC/2013-us-ipcc-joint-strategic-plan.pdf>

users, including copyright infringement.¹⁸ Although implementation is still in the early stages, MPAA remains optimistic that the new ICANN requirements will be an important tool for combating copyright infringement on a more global level. Currently, content owners are negotiating with new gTLD applicants over which safeguards are most appropriate and how they should be implemented. ICANN enforcement will be critical to the success of the new gTLD program, and it will be important to monitor the effectiveness of safeguards going forward.

III. HOW TO EVALUATE THE EFFECTIVENESS OF VOLUNTARY INITIATIVES

Here, MPAA responds to the questions listed under “Supplementary Information” at the end of the Federal Register Notice.

1. How should “effectiveness” of cooperative voluntary initiatives be defined?

The definition of effectiveness of a voluntary initiative should be defined by the degree to which the goals of the initiative have been met. For example, given the stated goals of the Copyright Alerts System are to (1) educate consumers about the importance of copyright protection and (2) help them find better ways to enjoy digital content, the effectiveness could appropriately be defined as (1) decrease in consumer sharing of copyright infringing files; and (2) increase in consumer accessing of legal digital content – ideally measured relative to a “control” or what they would have been in the absence of the initiative. The latter clause is important because the given metrics may increase or decrease due to other factors; correlation is not causation. Research that best assesses the effectiveness of the initiative should isolate the specific effects of the initiative from other environmental effects.

2. What type of data would be particularly useful for measuring effectiveness of voluntary initiatives aimed at reducing infringement and what would that data show?

The data used to measure the effectiveness of the initiative should also correlate to the goals of the initiative, and should measure whether the goals of the initiative have been met. In the case of “supply” focused initiatives, the measures can involve quantifying changes in supply, and also, potentially, corresponding changes in demand. In the case of “demand” focused initiative, the focus would be on changes in demand for infringing content, and/or potentially changes in demand for legal content. In the CAS example above, the data collected could involve the number of consumers sharing infringing files, the number of infringing files shared, bandwidth consumed by infringement, as well as the number of consumers accessing legal digital content, and/or the amount of legal digital content being accessed, or some derivation. Given the ideal is to measure these metrics relative to a “control” or what they would have been in the absence of the initiative, where possible data should be analyzed in areas that lend themselves to this comparison, such as pre- and post-implementation data, data for other non-affected but comparable jurisdictions, etc. The nature of this data will depend on the initiative.

3. If the data is not readily available, in what ways could it be obtained?

¹⁸ See NGPC Resolution, June 25, 2013, <http://www.icann.org/en/groups/board/documents/resolutions-new-gTLD-25jun13-en.htm#2.c>.

The availability of the data, and the ways it could be obtained, will be highly dependent on the nature of the metrics being tracked. By its nature, illicit behavior is often hard to measure, but various approaches can be employed including surveys, panel measurement, direct measurement in some cases, and sampling techniques. When evaluating measurement studies, the nature and quality of the available data should be assessed. PTO should solicit comments and input from industry and other subject matter experts regarding the accuracy and thoroughness of these studies.

4. Are there particular impediments to measuring effectiveness, at this time or in general, and if so, what are they?

The main impediments in general tend to be the availability of data and the existence of the necessary conditions in the market to isolate the effects of the initiative in question (*i.e.*, a randomized or a natural experiment). Where there are a number of different initiatives and conditions affecting the studied universe, identifying the causal effects of a particular initiative can be challenging and an imperfect process.

5. What mechanisms should be employed to assist in measuring the effectiveness of voluntary initiatives?

As stated above, various approaches can be employed to obtain data, including surveys, panel measurement, direct measurement in some cases, and sampling techniques. Standard statistical and econometric techniques can then be performed to analyze the data.

6. Is there existing data regarding efficacy of particular practices, processes or methodologies for voluntary initiatives, and if so, what is it and what does it show?

While not specifically focused on voluntary initiatives, there is data regarding the efficacy of similar initiatives such as:

- Notice-sending programs to file sharers: “The Effect of Graduated Response Anti-Piracy Laws on Music Sales: Evidence from an Event Study in France.”¹⁹
- Closure of websites providing major infringing content: “Gone in 60 Seconds: The Impact of the Megaupload Shutdown on Movie Sales.”²⁰

An example of a voluntary initiative that has been found to *not* be as effective as intended:

- Search engine algorithm adjustment to take into account the level of infringement notices that a site has received: “Six Months Later – A Report Card on Google’s Demotion of Pirate Sites.”²¹

¹⁹ See http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989240

²⁰ See http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2229349

²¹ See <http://76.74.24.142/3CF95E01-3836-E6CD-A470-1C2B89DE9723.pdf>

The MPAA appreciates this opportunity to provide our views in response to the Federal Register Notice. We look forward to providing further input and working with the PTO going forward.

Respectfully submitted,

Michael O'Leary
Senior Executive Vice President for Global Policy and External Affairs
Motion Picture Association of America, Inc.
1600 Eye St. NW
Washington, DC 20006
(202) 293-1966

Association of American
Publishers, Inc.
www.publishers.org

455 Massachusetts Ave., NW Suite 700
Washington, D.C. 20001
Telephone: (202) 347-3375
Fax: (202) 347-3690



Association of American Publishers
Written Statement
September 30, 2013

U.S. House of Representatives
Committee on the Judiciary
Subcommittee on Courts, Intellectual Property, and the Internet

The Role of Voluntary Agreements in the U.S. Intellectual Property System
Hearing
September 18, 2013

I. Introduction

AAP represents nearly 300 publishers, ranging from major commercial book and journal publishers to small non-profit, university, and scholarly presses. Unlike the common perception of content companies, most publishers in the U.S. are small businesses.¹ Although large and small publishers have a diversity of interests and concerns,² effective copyright protection and enforcement is a shared interest and is crucial to all publishers, regardless of size. AAP and its member publishers thus appreciate this opportunity to provide comments to Congress concerning the “Role of Voluntary Agreements in the U.S. Intellectual Property System.”

Existing voluntary agreements are discussed below to show how, over time, the concepts of effective voluntary agreements or best practices seem to have moved from commitments to undertake proactive measures against the proliferation of illegal content online to less robust agreements or best practices that place heavy burdens on rights holders for relatively little action in return. AAP believes that practical, results-driven, voluntary agreements among key players in the Internet, business, and copyright communities are critical to stemming the problem of rampant online piracy; to maximize their effectiveness, such agreements should focus on

¹ See generally, U.S. Census Bureau, <http://www.census.gov/econ/susb/>.

² AAP’s membership is generally divided among the following publishing sectors: trade (e.g., popular fiction/non-fiction); higher education; elementary and secondary education; and professional and scholarly publishing (e.g., academic and science journals, university presses).

encouraging proactive efforts to prevent piracy.³ Publishers appreciate the work of Congress and the Administration to bring together stakeholders from various segments of the intellectual property ecosystem to create innovative solutions for curtailing piracy and counterfeiting. While much remains to be done, it is encouraging to see interest among payment service providers, advertising entities, Internet service providers, and one hopes, eventually, search engines⁴ in promoting an Internet environment that is conducive to the growth of legitimate content and related services. Given the interdependence of content and technology, and the opportunities for innovation and growth in both, taking active steps to discourage theft of intellectual property on the Internet will, as recently noted by the Intellectual Property Enforcement Coordinator (“IPEC”), “in fact, further encourage the innovation made possible by an open Internet.”⁵ Encouraging investment and innovation is essential to providing the sustainable intellectual property ecosystem required by our Constitution, which directs Congress “to promote the Progress of Science and the useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.”⁶

Despite this constitutional obligation and the emergence of several relevant voluntary agreements, authors of high-quality works receive little if any “secured” time to recoup their investments (let alone make a decent living) because of the lack of meaningful protection online. Today, any individual can find and download an unauthorized copy of virtually any popular copyrighted work they want at any time from among the thousands of different sites on the Internet. Technological advancement has made it possible for individuals to engage in copyright infringement in a manner never previously contemplated by Congress. The persistence and volume⁷ of online piracy represent a serious gap in meaningful copyright protection in the digital environment, and necessitate an unfortunate diversion of resources from core creative endeavors in response. Online piracy significantly threatens the continued viability of all types of publishers and copyright-based industries, as well as millions of local jobs and their contribution to the U.S. economy, while adversely impacting our society and culture in immeasurable ways.⁸

³ AAP is focused in this statement on “online piracy,” e.g., sites that have made it their business to disseminate unauthorized copies of eBooks, journals, and other published materials, rather than on the distinct but still important issues of unauthorized uses of such works by, e.g., educational institutions, or individuals engaging in *ad hoc* infringement.

⁴ Search engines are the main gateway through which a consumer, wittingly or unwittingly, is directed to the sources of infringing content online. However, search engines have yet to commit to meaningful discussions with content creators on how to better refine search protocols to avoid serving up infringing links or sites to consumers. Discussions with search engines would certainly be a welcome development, which should be encouraged by Congress.

⁵ See Press Release, Office of the Intellectual Property Enforcement Coordinator, *Coming Together to Combat Online Piracy and Counterfeiting Network Best Practices*, (Jul. 15, 2013) <http://www.whitehouse.gov/blog/2013/07/15/coming-together-combat-online-piracy-and-counterfeiting>.

⁶ Art. 1 §8 cl. 8, U.S. CONST.

⁷ See generally, NetNames, *Sizing the Piracy Universe*, (Sept. 2013) http://www.netnames.com/UserFiles/netnames-sizing_piracy_universe-report-2_5.pdf; Office of the Intellectual Property Enforcement Coordinator, *2013 Joint Strategic Plan on Intellectual Property Enforcement*, Jun. 2013, <http://www.whitehouse.gov/sites/default/files/omb/IPEC/2013-us-ipeec-joint-strategic-plan.pdf>.

⁸ See Steven E. Siwek, *Copyright Industries in the U.S. Economy: The 2011 Report*, (Nov. 2, 2011), http://www.ipa.com/copyright_us_economy.html.

Although the subject of this inquiry is “the role of voluntary agreements,” the importance of that role can only be understood in the context of what has transpired since Congress’s 1998 enactment of the Digital Millennium Copyright Act (“DMCA”), which was intended to address copyright enforcement in the age of the Internet and other digitally-networked technologies. Since the DMCA’s enactment, unanticipated online business models have emerged that exploit unauthorized copies of third-party copyrighted works on a massive scale in order to lure user traffic to their sites. Typically, there are few consequences for such infringing activity because the DMCA “notice and takedown” mechanism, while well-intentioned when the statute was enacted, is today ill-suited to addressing the sweeping scope of constantly recurring piracy on these sites. At the same time, there have been questionable judicial interpretations of the DMCA’s Internet service provider “safe-harbor” provisions which have encouraged, rather than deterred, the unauthorized exploitation of copyrighted works in this manner and the proliferation of various types of sites offering pirated copyrighted content.⁹ As a result, the DMCA’s “notice-and-takedown” system has been turned into a shield for online bad actors, rendering the notice-sending mechanism ineffective in addressing piracy while imposing burdensome costs on copyright holders.

With statutory copyright protections diminished by the courts and legislative consensus on new statutory enforcement measures proving politically elusive, copyright holders have been urged by Congress and the Administration to turn to private sector solutions with various other stakeholders in an attempt to make some progress in the fight against online piracy. In this context, it is important to note that, as technological solutions (such as content identification technologies) improve, the utility of copyright protection via a notice-and-takedown system that is reactive by nature may diminish. Thus, voluntary agreements should not merely duplicate notice-and-takedown requirements but should move toward a more proactive system that attempts to prevent infringement from occurring.

Neither voluntary agreements nor improved statutory protections will be sufficient on their own to adequately protect copyrighted works. However, steps such as clarifying the eligibility requirements for the ISP “safe harbors” from infringement liability to more closely track the long-standing elements of traditional secondary liability doctrines for copyright infringement¹⁰ might be a means to provide the necessary incentive for stakeholders to voluntarily establish more meaningful commitments to combat piracy, which are necessary supplements to any type of statutory protection. Additionally, there will likely be particular issues where Congress will need to enact additional measures to ensure that illegal activity does not inhibit the growth of legitimate digital content and related services. Only a *combination* of private and public

⁹ There are a variety of major sources of infringing files, such as: 1) one-click host sites (aka cyberlockers), 2) sites which systematically link to the hosts, 3) sites facilitating file-sharing via peer-to-peer networks, and 4) websites which are storefronts selling individual unit copies of pirated works in digital format.

¹⁰ For example, that an ISP, UGC Service, or search engine, etc. that is aware of infringing activity on its site or service should remove or disable that infringement regardless of whether it receives actual notice of the infringement from the copyright holder. If a site or service is aware of infringement, whether through actual knowledge of specific infringements or constructive (i.e., “red flag”) knowledge of the activity, the site or service should be obligated to remove or disable the infringing content.

enforcement mechanisms can reasonably be expected to effectively mitigate rampant online piracy. Below, we provide an overview of the strengths and weaknesses of the current voluntary agreements as viewed by book publishers, along with suggestions for the role of Congress in improving the fight against online piracy.

II. Current Voluntary Agreements

a. Background

AAP notes that the extant voluntary agreements attempt to address online piracy and promote Internet-based availability of high-quality, legitimate content in one of two ways, by either: (1) educating content-users, or (2) directly targeting unlawful activity. While the U.S. Patent and Trademark Office will be conducting the first official examination of the effectiveness of those agreements,¹¹ it appears that they all have limitations in scope and reach that are likely to significantly limit their effectiveness in dealing with specific types of and platforms for online piracy and, ultimately, their effectiveness in deterring and reducing the frequency and magnitude of its occurrence.

Existing voluntary agreements are discussed in chronological order below to show how, over time, the concepts of effective voluntary agreements or best practices seem to have moved from multi-stakeholder commitments to undertake proactive measures against the online proliferation of illegal content to weaker agreements or unilaterally-determined “best practices” that place heavy burdens on rights holders for relatively little action in return. With online piracy continuing to grow,¹² the dilution of voluntary agreements evinces a need for Congress to provide stronger incentives to encourage stakeholders to implement more meaningful agreements.

b. UGC Principles

The “Principles for User Generated Content Services” (“UGC Principles”¹³), concluded in 2007, was the first multi-stakeholder-negotiated voluntary agreement aimed at reducing the

¹¹ See Department of Commerce, *Internet Policy Task Force, Copyright Policy, Creativity, and Innovation in the Digital Economy*, 84 (Jul. 2013), <http://www.uspto.gov/news/publications/copyrightgreenpaper.pdf>.

¹² See generally, Ernesto, *Six-Strikes Fails to Halt U.S. Pirate Bay Growth*, TORRENTFREAK.COM (Sept. 3, 2013) <http://torrentfreak.com/six-strikes-fails-to-halt-u-s-pirate-bay-growth-130903/>; NetNames, *Sizing the Piracy Universe*, (Sept. 2013), http://www.netnames.com/UserFiles/netnames-sizing_piracy_universe-report-2_5.pdf; Department of Commerce, *Internet Policy Task Force, Copyright Policy, Creativity, and Innovation in the Digital Economy*, 84 (Jul. 2013) <http://www.uspto.gov/news/publications/copyrightgreenpaper.pdf>; Office of the Intellectual Property Enforcement Coordinator, *2013 Joint Strategic Plan on Intellectual Property Enforcement*, (Jun. 2013), <http://www.whitehouse.gov/sites/default/files/omb/IP/IPC/2013-us-ipeec-joint-strategic-plan.pdf>.

¹³ See generally, *Principles for User Generated Content Services*, ugcprinciples.com (describing the agreement between: “leading commercial copyright owners (“Copyright Owners”) and services providing user-uploaded audio and video content (“UGC Services”)...to establish these Principles to foster an online environment that promotes the promises and benefits of UGC Services and protects the rights of Copyright Owners.”).

prevalence of pirated content online. Although both content and Internet-industry stakeholders recognized their shared objectives,¹⁴ the threat of secondary liability was a driving factor in the Internet-industry's willingness to negotiate and to take on meaningful commitments to address online piracy.

For example, Principle 3 states that "UGC Services should use effective content identification technology ["filtering"]...with the goal of eliminating from their services *all* infringing user-uploaded audio and video content for which [c]opyright [o]wners have provided [r]eference [m]aterial." This principle is followed by an extensive list of ways in which UGC Services and copyright owners would work together to achieve the goal of eliminating such infringing content. Principle 3 thus represents a joint commitment to directly target unlawful activity in order to eliminate infringing content. However, this filtering commitment only applies to "audio and video content."

The current implementation of YouTube's "Content ID" system to prevent the presence of infringing audio and video content on its site, one of the largest UGC websites in the world with more than 1 billion unique user visits each month and "more than 100 hours of video... uploaded" every minute, points to the value of these UGC Principles when effectively implemented.¹⁵ Although eBook and journal content were not part of the UGC Principles, AAP and its members have provided feedback and reference materials directly to two sites which are focused on the sharing of text-based works, Scribd.com and Wattpad.com, to facilitate their deployment of technical measures to prevent infringing content from being made available via their services.

Scribd.com describes itself as "the world's largest digital library where people can publish, discover, and read books and documents of all kinds on the web or on any mobile device."¹⁶ Scribd's business objectives rely on the fact that "millions of books and documents have been contributed to Scribd by the community and this content reaches an audience of 100 million people around the world every month."¹⁷ To avoid being a destination for infringing materials, Scribd has implemented a copyright protection system that it describes as follows:

Content that is removed from Scribd via a DMCA copyright infringement takedown notice is added to our copyright protection system. This system performs a semantic analysis of the document by analyzing word count, word frequency, letter combinations, spacing, and other criteria. The semantic analysis results in a special encoded file that we

¹⁴ See *id.* (describing the shared objectives of Copyright Owners and UGC Services as: "(1) the elimination of infringing content on UGC Services, (2) the encouragement of uploads of wholly original and authorized user-generated audio and video content, (3) the accommodation of fair use of copyrighted content on UGC Services, and (4) the protection of legitimate interests of user privacy." Also noting that "adhering to [the UGC] Principles will help UGC Services and Copyright Owners achieve those objectives.").

¹⁵ See Google, *How Google Fights Piracy*, GOOGLE.COM (Sept. 2013) <https://docs.google.com/file/d/0BwXvRPFduTN2dVTqYmlSUENUeUE/edit?pli=1>

¹⁶ See About, SCRIBD.COM <http://www.scribd.com/about>.

¹⁷ *Id.*

call a "fingerprint." The encoded fingerprint is stored in a secure database that is inaccessible to the public.

Whenever a new document is uploaded to Scribd, it is analyzed and checked against the "fingerprints" in our copyright database. If there's a significant match, the upload is removed from Scribd. Since the fingerprint system is based on text analysis, it is less effective on documents that do not contain computer-readable text information (such as scanned photos).¹⁸

To improve the functionality of Scribd's filter, certain AAP members provided copies of their works for inclusion in its copyright database. Publishers continue to engage with Scribd on copyright protection concerns.

Wattpad.com describes itself as "the world's largest community for discovering and sharing stories" for free.¹⁹ Their goal is to attract new writers and readers to post and read original content, not third-party works, or as they have put it—"Read what you like. Share what you write."²⁰ Wattpad has worked with publishers to develop a database of book product metadata (such as title, author, etc.) to prevent books not authorized for distribution on Wattpad from being shared via the service.

To be clear, AAP does not endorse any specific or particular technology solution. The above examples are intended to illustrate that responsible website operators have options to prevent their services from being used to distribute pirated content; flexibility in designing appropriate technological measures to achieve their legitimate business objectives; and willing partners in the content industries to provide reference materials and feedback for improving the operation of appropriate technology solutions. Collaboration between copyright owners and Internet services, which was crucial to creating the UCG Principles, will also be critical for ensuring that technological solutions can evolve over time to address the ever changing nature of infringement on the Internet.

c. IACC Payment Processor Portal

Established in 2011, the International Anti-Counterfeiting Coalition's (IACC) Payment Processor Portal (Portal) is a multi-stakeholder agreement that directly targets unlawful activity. The goal of the Portal is to cut off revenue to sites that sell counterfeit products or pirated content. To accomplish this goal, the IPEC helped payment processors, content and product owners negotiate a set of best practices to withdraw payment services from sites selling counterfeit or pirated goods. IACC's Portal vets and consolidates rights holder notices identifying sites that traffic in such illicit goods. Now in its second year of operation, it appears that many payment providers trust the legitimacy of the notices received through the Portal and

¹⁸ Jason, *How Does Scribd Help Protect the Rights of Authors?*, SCRIBD.COM (Feb. 26, 2009) <http://support.scribd.com/entries/25057-How-does-Scribd-help-protect-the-rights-of-authors->.

¹⁹ *About*, WATTPAD.COM <http://www.wattpad.com/about>.

²⁰ Presentation, Allen Lau, Wattpad Company Info, (May 24, 2010) (on file with author) (emphasis added).

are amenable to terminating merchant accounts that have been shown to be engaged in infringing activity.²¹

However, unlike the UGC Principles, which provide general guidelines for how any UGC Service can design its site to deter uploading and distribution of pirated audio and video content, the IACC Portal is a service that content owners must pay a substantial fee²² to use. To date, the Portal has been used primarily to shut down merchants selling *counterfeit products* because payment processors generally require evidence of a specific unlawful sale to terminate a merchant account. Unfortunately, sites making available infringing copies of copyrighted works through sales of “premium” subscriptions (providing advantages to users such as faster downloading speeds and greater file-storage space) are generally outside the scope of the IACC program.²³

d. Copyright Alert System

In early 2013, after years of discussions, the music, movie, and television communities launched the Copyright Alert System (CAS) in partnership with five major U.S. Internet service providers (ISPs). Like the IACC’s Portal, implementation of the CAS requires a commitment of very substantial financial resources, borne by participating rights holders and ISPs. CAS aims to decrease illegal sharing of movies and music through peer-to-peer (P2P) networks by having ISPs pass along notices from participating rights holders to subscribers that appear to be engaged in illegal activity.

The CAS uses a more than generous six-notice educational approach in attempting to deter P2P file-sharing. Once a rights holder’s monitoring service detects infringing behavior over a P2P network, the rights holder notifies the relevant ISP, which forwards an educational notice to the infringer(s). The first 1-2 notices are intended to educate the infringing ISP subscriber about copyright and provide information about legal alternatives for accessing content. If recurring infringing activity is detected, the 3rd and 4th notices require acknowledgment of receipt of the educational message. Not until the 5th or 6th notice will a subscriber be subject to any mitigation measures, such as reduction of bandwidth.

P2P piracy is a problem for publishers, but it is not the only one. One-click host sites (aka cyberlockers) play a larger role in making pirated eBooks and journal articles publicly available by providing online storage for users to upload and share copyrighted content. However, the CAS does not address the dissemination of pirated content through one-click host

²¹ See *The Role of Voluntary Agreements in the U.S. Intellectual Property System*: Hearing Before the House Judiciary Committee Subcommittee on Courts, Intellectual Property and the Internet, 113th Congress (2013) (statement of the International Anti-Counterfeiting Coalition) (providing the most recent enforcement statistics).

²² AAP notes that the Portal and other systems developed by private stakeholders to implement voluntary agreements have substantial development, implementation and maintenance costs, which likely justify the fees charged by IACC and other. However, with many publishers being small businesses, we hope that cost will not serve as a functional barrier to rights holders participating in effective voluntary measures.

²³ It is not uncommon for one-click host sites to offer both free and subscription models for downloading pirated content.

sites, online storefronts, blogs, or other individual websites that likewise account for a significant portion of online piracy.

A one-size-fits-all approach may not be practical or effective. However, finding an effective solution for the different types of online piracy is crucial. Data on the effectiveness of CAS' educational approach to combating P2P piracy is not yet publicly available.²⁴ While government-sponsored graduated response policies that incorporate more restrictive consequences than the CAS for repeat infringers have had some short-term effect on P2P activity in the past, e.g., France's HADOPI, it is unclear whether these models effectively reduce P2P activity over time. It thus remains to be seen whether a private, education-focused initiative will result in any noticeable decline of illegal P2P activity.

e. Ad Network Best Practices

Most recently, in July of this year, the Interactive Advertising Bureau (IAB) and top ad networks (Google, Yahoo!, 24/7 Media, etc) announced the Best Practice Guidelines to Address Piracy and Counterfeiting (Best Practices), which directly target unlawful activity with the objective of "reducing the flow of ad revenue to operators of sites engaged in significant piracy and counterfeiting."²⁵ Yet, despite the fact that eBook piracy websites' business models are often based on the sale of advertising space on their websites rather than on the sale of individual copies, it is unclear whether any rights holder groups were consulted in the development of these "best practices" (as certainly publishing interests were not).²⁶

To be sure, the Best Practices provide a *potentially* useful commitment to completely "remov[e] the website [distributing pirated content] from the Ad Network."²⁷ However, it remains to be seen whether any meaningful change occurs in the manner in which advertisements find their way onto bad actor sites given that the Best Practices clearly favor the ad networks.

Specifically, the Best Practices impose complex notification requirements²⁸ on rights holders in order to initiate the process of requesting that an ad network stop placing ads on a

²⁴ But see, Ernesto, *Six-Strikes Fails to Halt U.S. Pirate Bay Growth*, TORRENTFREAK.COM (Sept. 3, 2013), <http://torrentfreak.com/six-strikes-fails-to-halt-u-s-pirate-bay-growth-130903/>.

²⁵ *Best Practice Guidelines to Address Piracy and Counterfeiting*, (Jul. 15, 2013), <http://www.2013ippractices.com/>.

²⁶ AAP hopes that the Ad Networks will, however, uphold their commitment to "participate in an ongoing dialogue with content creators, rights holders, consumer organizations, and free speech advocates" to ensure that these Best Practices become a meaningful tool in the fight against online piracy. See *Best Practice Guidelines to Address Piracy and Counterfeiting*, General Commitments (d) (Jul. 15, 2013) <http://www.2013ippractices.com/>.

²⁷ See *Best Practice Guidelines to Address Piracy and Counterfeiting*, Complaint Process (h) (Jul. 15, 2013), <http://www.2013ippractices.com/>.

²⁸ Specifically, notices must contain: (1) the specific URLs of the alleged infringements (clearly identifying the "specific products or materials and their location on the website"); (2) the identity, location and contact information for the website; (3) further evidence of infringement, e.g., through screenshots; and (4) a copy of a cease & desist letter or takedown notice previously sent to the website as well as a description of action undertaken by the website. See *Best Practice Guidelines to Address Piracy and Counterfeiting*, Appendix A. (Jul. 15, 2013), <http://www.2013ippractices.com/>.

particular website. As noted above, the current DMCA notice-and-take down system is already fraught with problems and yet, quite inexplicably, here an even more complicated system is envisioned as possibly stopping ad support for sites distributing pirated content. The Best Practices unjustifiably burden rights holders with providing a notice containing the specific URLs for each “specific [pirated] product or material.” This is in addition to requiring the rights holder to provide a copy of DMCA-compliant takedown notices for the same content.

The judicially-created, *de facto* requirement that rights holders identify specific URLs for each DMCA takedown notice already imposes a substantial cost on rights holders and results in little practical reduction of piracy. Doubling this burden for rights holders only impedes enforcement by having ad networks process and take action,²⁹ one-by-one, on potentially millions of separate URLs, which is plainly inefficient.³⁰ Without question, eliminating vital ad revenue that supports sites that are dedicated to distributing pirated content would have a noticeable impact on piracy. However, achieving this goal is unlikely under such complex requirements.

Instead, when a rights holder identifies a particular work, or list of works, that are not legitimately available for free, ads supporting any page containing these works on a website should be disabled instead of requiring continuous searches and unique notices from the copyright owner for each page containing the same underlying work. Adopting this “representative list” approach will save rights holders and ad networks time and money.

Furthermore, if these Best Practices are actually intended to have a meaningful effect on ad-supported online piracy, participants should ensure that their ads stop supporting the worst pirate sites, e.g., Pirate Bay, in any way. All participants in the online advertising ecosystem should be encouraged to work together to develop a comprehensive and effective approach to eliminating legitimate advertising on illegitimate sites, including the use of technological solutions that incorporate information provided by independent third-party verification services³¹ to help enable informed decisions about ad placement.

III. General Principles for Future Voluntary Agreements

While there are many positive features of the existing voluntary agreements, they cannot be the only means for addressing the problem as there simply is no “silver bullet” to stop online piracy. There are, however, a few general principles that AAP believes should be at the core of

²⁹ As noted above, the Ad Networks can choose to “remov[e] the [entire] website from the Ad Network” instead of removing ads from one webpage at a time. However, there is no parallel options (e.g. a representative list of infringements) for rights holders, who must instead include URLs for each and every infringement. See *id.* at (h); Appendix A.

³⁰ As one example of the sheer volume of notices that must be sent to make any impact on piracy, see Google’s Transparency Report on requests for removal of links to infringing material, (<http://www.google.com/transparencyreport/removals/copyright/>), which shows that Google receives *millions* of takedown requests each month, for hundreds of thousands of specific URLs, by thousands of copyright owners.

³¹ For example: VeriSite <http://www.veri-site.com/> and White Bullet, <http://www.white-bullet.com/>.

any effective voluntary agreement or set of best practices. AAP believes that the impact of current and future voluntary agreements would be greater if the following general principles informed the structure and application of such agreements:

1. Best practices are more likely to achieve stated objectives if all relevant stakeholders are active contributors in the development of the best practices from the beginning.
2. Private, voluntary agreements have flexible terms that are more easily modified than statutory prescriptions. Therefore, voluntary agreements should include a process for soliciting feedback from rights holders and other affected stakeholders, and using that feedback to improve the operation and/or effect of the agreement or best practices in a timely manner.³²
3. Compliance with best practices statements, as well as procedures for implementing voluntary agreements, should be transparent. Providing more data to facilitate efforts to measure the implementation and effectiveness of best practices and voluntary agreements will help ensure that stakeholders are not wasting resources on ineffective policies or actions.
4. Voluntary agreements should not require a *quid pro quo* (e.g., removal of pirated content on the condition that right holders license use of their legitimate content to the participants) to undertake responsible actions to eliminate pirated content from websites.
5. Solutions developed as part of voluntary agreements should be practicable and scalable for various types of rights holders, many of which are small businesses.
6. Where applicable, technological solutions should be explored to facilitate efforts to efficiently and effectively combat online piracy. By doing this voluntarily, stakeholders avoid any possibility of a technology mandate.
7. Voluntary agreements should be reasonable, i.e., the time, cost, and effort to comply with or implement such agreements should *not* unduly burden one group or another, but should be shared by rights holders, Internet companies and intermediaries.
8. Respect for privacy, due process, and freedom of speech are critical to maintaining a creative Internet economy, and such values can coexist with effective anti-piracy efforts.

Many of these general principles are common sense and speak for themselves. When solutions to a problem are sought, it is best to involve the relevant parties; to measure whether the actions are having their intended effect; and to evaluate the current strategy to determine if resources are being wasted. Potentially less obvious is that copyright piracy harms more than just “best sellers” and box-office hits. In reality, there are also sites providing pirated textbooks, complex scientific articles, and niche-market books. And, as noted above, most publishers in the U.S. are small businesses that do not have the resources to continually search the Internet for their content, sue multiple (or even single) websites, or take part in expensive voluntary enforcement initiatives. Furthermore, even large publishers do not have unlimited resources to invest in sending millions of takedown notices that fail to reduce piracy, or to join anti-piracy

³² AAP agrees with RIAA that we should “never confuse motion for action” in regard to anti-piracy activities and that what is really important is that anti-piracy measures are effective.

initiatives that pay lip-service to combating piracy but do not provide meaningful incentives for participants to take effective action or measurements of the initiative's ability to reduce piracy.

Lastly, perhaps because we represent an industry dedicated to the dissemination of knowledge, AAP believes the importance of transparency for creating and maintaining effective public and private copyright enforcement mechanisms cannot be stressed enough. Unfortunately, there is currently little transparency about pirated content and anti-piracy measures. However, transparency is necessary for stakeholders to undertake efficient, accurate and effective efforts to reduce online piracy. A number of entities in the online ecosystem (ad networks, ISPs, search engines, one-click host site operators) have or can easily obtain data concerning their own compliance and implementation of voluntary agreements that would be useful in assessing the impact, cost, and reach of such anti-piracy efforts.

IV. Role for Congress

While private parties may be in the best position to negotiate and craft flexible methods for combating online piracy, Congress still has an important role to play in creating meaningful incentives for stakeholders to conclude and implement effective agreements. Moreover, because voluntary agreements are a necessary but not sufficient tool for combating online piracy, Congress may also need to fix the shortcomings of the current statutory copyright enforcement mechanisms (e.g., the eligibility requirements for the ISP "safe harbors" from infringement liability, including: notice-and-takedown, repeat infringer policies, and knowledge standards). There will also be additional issues for which Congress will need to "fill in the gaps" by enacting additional measures to ensure that illegal activity does not inhibit the growth of legitimate digital content and services online.

Furthermore, Congress has an important role to play in ensuring transparency, which has been noticeably absent in the fight against online piracy, despite the importance of sharing information to combat piracy in the digital age. Congress and the Administration may be in the best position to encourage all entities within the Internet and intellectual property communities to share relevant data where doing so would improve anti-piracy tools and be allowed by law. Importantly, Congress would be able to take into account and weigh the harms and benefits of such sharing, and thus ensure that privacy, due process, and freedom of speech are adequately protected.

V. Conclusion

Congress's comprehensive review of the Copyright Act is an opportunity to encourage private stakeholders to develop and implement effective voluntary anti-piracy measures that will complement statutory copyright protections. AAP looks forward to continued engagement with Congress and the various stakeholders to further explore ways to make combating copyright piracy more efficient and effective for all parties involved.

Sincerely,



Allan Adler
General Counsel
Vice President for Government Affairs
Association of American Publishers
455 Massachusetts Ave. NW
Washington, D.C. 20001
Phone: 202/220-4544
Fax: 202/347-3690
Email: adler@publishers.org

Statement of the Alliance for Safe Online Pharmacies
The Role of Voluntary Agreements in the U.S. Intellectual Property System

U.S. House of Representatives
Committee on the Judiciary
Subcommittee on Courts, Intellectual Property, and the Internet

September 18, 2013


 ASOP | ALLIANCE FOR SAFE ONLINE PHARMACIES

The Honorable Bob Goodlatte
 Chairman
 House Judiciary Committee
 2309 Rayburn House Office Building
 Washington, DC 20515

The Honorable Mel Watt
 Ranking Member
 House Judiciary Committee
 2304 Rayburn House Office Building
 Washington, DC 20515

The Honorable Howard Coble
 Chairman
 House Judiciary Subcommittee on Courts,
 Intellectual Property and the Internet
 2188 Rayburn House Office Building
 Washington, DC 20515

The Honorable John Conyers, Jr.
 Ranking Member
 House Judiciary Subcommittee on Courts
 Intellectual Property and the Internet
 2426 Rayburn House Office Building
 Washington, DC 20515

September 24, 2013

Dear Chairman Goodlatte, Chairman Coble, Ranking Member Watt and Ranking Member Conyers:

On behalf of the Alliance for Safe Online Pharmacies (ASOP), thank you for the opportunity to submit the following testimony for the record to supplement your September 18th subcommittee hearing regarding the role of voluntary agreements in the U.S. intellectual property system. ASOP is a nonprofit organization dedicated to protecting patient safety globally and ensuring patient access to safe and legitimate online pharmacies in accordance with applicable laws. For this reason, we are concerned by rogue sites that violate laws and endanger patients; we support strong voluntary practices that help to ensure the internet can be a positive resource for all, while not enabling crimes against public health that are preventable.

Despite the existence of many safe online pharmacies that adhere to laws and safety standards, the Internet has opened the door to thousands of criminal Internet sites posing as legitimate pharmacies and selling potentially unsafe medicines. Indeed, at any one time there are approximately 35-50,000 active online drug sellers, 97% of which do not comply with U.S. laws, putting patients at risk. Illegal online "pharmacy" operations are big business, the largest of which generate between \$1 million and 2.5 million in sales each month.¹

Illegal online drug sellers feign legitimacy and endanger patients. They sell prescription drugs without a prescription, operate without a pharmacy license, and/or peddle counterfeit or otherwise illegitimate drugs with contaminants, such as paint, floor wax, and boric acid. These illegal drug websites create a major health and safety risk to U.S. consumers. For example, a man in Wichita, Kansas died from an accidental overdose of drugs he received from an online "pharmacy" without ever visiting a doctor. Others have suffered brain damage, been hospitalized, or simply not received the healing benefits needed from drugs purchased online.

¹ University of California San Diego, available at: <http://cseweb.ucsd.edu/~savage/papers/UsenixSec11-SMTM.pdf>

Easy access to prescription drugs through illegal online drug sellers has also contributed to a growing prescription drug abuse problem in our nation. This is of particular concern with regard to young people, who are frequently online, unsupervised and vulnerable to the ploys of illegal online drug sellers.

Pharmaceuticals are the 13th most purchased product online, yet today patients are just a click away from online "medicines" that may fail to provide any therapeutic benefit, harm, or even kill a patient. Internet consumers should not have to play Russian roulette with their health. ASOP thanks the House Judiciary Committee for its consideration of the grave implications of this growing threat to public health.

While the U.S. government plays a critical role in protecting patient safety, the U.S. and other governments cannot tackle this international and fast-moving problem alone. Law enforcement actions require substantial time and resources to track the illegal online drug sellers, who can elude authorities while taking in profits and endanger patient lives. While making cases and putting criminals behind bars is essential, Internet commerce companies have the unique ability to protect patients immediately through voluntary actions.

Every Internet intermediary has a role to play to protect consumers through meaningful and appropriate actions addressing illegal online drug sellers' use of their services. These companies witness the threats on their platforms and can address them through prompt voluntary actions without waiting for a court order. Voluntary actions such as terminating service, locking domain names, and otherwise refusing to do business with illegal online drug sellers yield immediate and substantial benefits to patients. In combination with continued domestic and international law enforcement and policy, voluntary agreements will make the Internet safer for patients.

ASOP is grateful for the Subcommittee's work to understand and, where appropriate, help advance voluntary agreements from private sector companies who have the ability to protect patients from illegal and dangerous online drug sellers. Your leadership and oversight are crucial. Private sector companies, including the members of Center for Safe Internet Pharmacies (CSIP) and other e-commerce companies, are beginning to accept their responsibility to protect patient safety online. We strongly support your efforts to strengthen and build upon these ongoing efforts; we urge the Committee to remain a vigilant watchdog of the effectiveness of voluntary agreements that will protect patients.

ASOP recently submitted comments to the United States Patent and Trademark Office regarding the importance of measuring the effectiveness of voluntary agreements. We would like these comments to be submitted for the record by the Committee to supplement the other testimony provided in your hearing. We also offer a list of recent law enforcement actions and survey of reported patient harms as further evidence of the scope of the problem, which may also be submitted for the record to underscore the importance of Congressional oversight.

Thank you again for your leadership and consideration of this important public health issue.

Respectfully,

Alliance for Safe Online Pharmacies



**Testimony for the Record: Subcommittee Hearing on "The Role of Voluntary Agreements in the U.S. Intellectual Property System"
September 18, 2013**

INTRODUCTION

The Alliance for Safe Online Pharmacies (ASOP) appreciates the opportunity to submit the following comments for the record. These comments were previously submitted to USPTO Request for Public Comments on August 21, 2013 (Docket No: PTO-C-2013-0036) regarding the processes, data metrics, and methodologies that could be used to assess the effectiveness of cooperative agreements and other voluntary initiatives to reduce intellectual property infringement that occurs online, including specifically the crimes of illegal online drug sellers.

ASOP is a nonprofit organization with the goal of protecting patient safety and ensuring patient access to safe and legitimate online pharmacies in accordance with applicable laws. ASOP's membership includes the American Pharmacists Association, Eli Lilly & Company, Enforce the Act, European Alliance for Access to Safe Medicines, International Pharmaceutical Federation, LegitScript, Merck, Men's Health Network, National Association of Chain Drug Stores, NeedyMeds, the Partnership at Drug-Free.org, and Takeda Pharmaceuticals.

ASOP believes that patients deserve protection from illegal or illegitimate websites selling or offering to sell drugs purporting to be licensed and compliant pharmacies, while endangering patients' lives. Despite the existence of many safe online pharmacies which do adhere to safety standards, the nature of the Internet has opened the door to thousands of criminal (aka "rogue") Internet sites posing as legitimate pharmacies and selling potentially unsafe medicines. The result: patients are just one click away from purchasing medicine that could have a dangerous or fatal consequence.

A. ASOP SUPPORT FOR VOLUNTARY BEST PRACTICES

ASOP applauds the White House for its continued commitment to a strategy that aims to protect public health and safety and combat illegal online drug sellers that peddle counterfeits and other unsafe products to unsuspecting patients. The Obama Administration and its Intellectual Property Enforcement Coordinator, Victoria Espinel, have made significant strides on this issue, beginning with their initial Joint Strategy in 2010.

The Administration's strategy rightly recognizes and encourages the critical role and responsibility of the private sector in adopting voluntary practices that can better protect consumers and prevent criminal activity that may result in harm or even deaths. In the 2013 strategy, the Administration calls particular attention to the Center for Safe Internet Pharmacies (CSIP), a nonprofit organization comprised of Internet commerce companies, which was established to increase collaboration and actions to reduce the number of rogue online "pharmacies." ASOP agrees that CSIP and other Internet commerce

companies have the unique ability to adopt and commit to enforcing practices that can protect patients in a way no government or other organization can. As such, ASOP greatly appreciates and encourages the Administration's support for CSIP and relevant voluntary actions by the private sector to combat rogue online "pharmacies". ASOP is also supportive of effective oversight and constructive engagement regarding the value of such voluntary practices and how they can be measured, improved, and strengthened as necessary for the benefit of patient safety, public health, and crime prevention.

CSIP and its thirteen member companies have taken the following efforts to date which have helped to raise awareness about the threat and the CSIP organization's own commitment to disrupt this criminal activity:

- Development of a functional infrastructure to facilitate the sharing of information about suspect online pharmacy websites amongst the nonprofit's corporate members;
- Partnership with ASOP, other nonprofits and the US government on education and public messaging;
- Collaboration with FDA on Operation Pangea, an international law enforcement initiative to identify and address illegal online drug sellers;
- Participation in international dialogues with EU and Japan stakeholders; and
- Donation of search engine advertisements which direct consumers to awareness videos, developed in partnership with ASOP and/or the LegitScript pharmacy URL verification tool.

We applaud these activities from CSIP and encourage their increased collaboration to reduce illegal online "pharmacies" and protect patients. However, all stakeholders -- public and private, domestic and international -- must do more to put criminals on the defensive and prevent continued growth of their online presence. There are critical elements that are needed from the private sector, including increased vigilance to monitor and cease business transactions with illegal online "pharmacies," as well as increased collaboration to establish model responsible business practices that can help prevent this growing crime in a more systematic way.

The private sector's involvement in protecting the public health from Internet criminals will not be successful if it is not assessed critically, reviewed, and improved upon. In order to ensure that it is successful and meaningful, it must not be restricted to the policies of a few individual companies or isolated public relations activities. The goal of these voluntary initiatives must be to realize a significant change in the online environment that will either prevent or greatly deter criminals from operating freely as they do in today's environment. The commitment to do this has already been made in principle with the establishment of CSIP and their public announcement to work together to protect the public from these illegal sites. If appropriately measured, their work (and the work of other responsible private sector actors, including those abroad) can change the environment online and realize outcomes that make a difference in patients' lives, now and in the future. Accordingly, ASOP offers the following specific comments on how to assess the effectiveness of voluntary initiatives aimed at combatting illegal online drug sellers.

B. ASOP RESPONSE TO SPECIFIC QUESTIONS IN THE FEDERAL REGISTER NOTICE

Question #1: How should “effectiveness” of cooperative voluntary initiatives be defined?

Specific to the rogue online pharmacy issue, “effectiveness” of voluntary initiatives to combat illegal online drug sellers ought to be defined in terms of the direct impact on the safety of patients/consumers, including:

- a. The “cleanliness” of the Internet pharmacy marketplace (i.e. the number of illegitimate online pharmacies found in search results and other online locations);
- b. Transparency of Internet commerce company corporate policies and development of recommended best practices to monitor and prevent the facilitation of illegal online “pharmacies;”
- c. Increased consumer awareness about the dangers of purchasing from illegal online drug sellers including providing consumers with a list of legitimate online pharmacy websites.

However, only CSIP and other Internet commerce companies have the direct ability to affect the cleanliness of the marketplace. For this reason, ASOP’s comments will focus on how to measure the impact of voluntary actions that could directly improve the safety of the Internet pharmacy marketplace, rather than how to measure the effectiveness of consumer awareness initiatives.

Question #2: What type of data would be particularly useful for measuring effectiveness of voluntary initiatives aimed at reducing infringement and what would that data show?

Specific data regarding key voluntary initiatives of CSIP and its members would provide a useful tool for measure the effectiveness of their efforts, which ASOP strongly supports.

The following suggestions include recommended metrics for measuring the effectiveness of various voluntary practices ongoing today:

1. *Mimicking consumer behavior:*
 - a. Searching terms such as “Buy [insert drug name]” in search engines, social media sites and other Internet platforms and then identifying and quantifying the illegal online pharmacies in those locations (such as on the first two pages of results). This would mimic the behavior of consumers looking online to purchase a prescription medicine. These data have the benefit of being readily available and not sensitive or confidential, and could also be tracked over time for trends and measurement of progress.
2. *Effectiveness of CSIP members’ standards of conduct and/or other voluntary best practices:*
 - a. The measurable outcomes from CSIP members’ own voluntary enforcement activity in 2012 and 2013, other than the aggregate data related to Operation Pangea that has been publicly released, including:
 - i. The percentage of illegal online pharmacy activity on each member’s platform, as evidence members’ commitment to CSIP’s mission and to shed light on what, if any, voluntary policies are working;

- ii. The number of websites blocked/transactions stopped by each sector involved in CSIP, which as a stand-alone number (not a percentage) shows the scope of the problem and how individual policies or best practices being employed by CSIP members are helping to achieve these results and/or curb the threat;
 - iii. Percentage change in the number of solicitations to CSIP companies by illegal online drug seller operators, as evidence of the effect that corporate policies can have on rogue actors' activities (e.g. the rogue actors may stop trying to use XYZ registrar and instead seek out a safe-haven registrar who does not enforce policies against illegal sites);
 - iv. The number of internal appeals by illegal online drug sellers that each company (or sector) has had to respond to, which informs future efforts to establish effective, tailored voluntary enforcement protocols;
- b. The internal policies, strategies and tactics adopted and the resources (internal or external) that have been helpful in creating effective corporate voluntary enforcement programs within CSIP member companies, which will demonstrate to stakeholders what works and what doesn't;
 - c. CSIP's standards for membership (e.g. expectations of voluntary enforcement), to evidence CSIP members' tangible commitments to addressing the issue and to help set standards/best practices against which other Internet commerce companies could be evaluated;
 - d. CSIP's recommendations for what other Internet commerce companies (non-CSIP members) could be doing to help clean up the Internet pharmacy marketplace in order to help export standards/best practices and establish guidelines against which other companies could be evaluated.
3. *Effectiveness of CSIP's "neutral forum for sharing relevant information about illegal Internet pharmacies among members (forum)":*
- a. The type, quantity and frequency of information shared in the forum, e.g. prospective threats or only post-investigation information, to show whether and how such a forum can be used to proactively address rogue activity;
 - b. Information on breadth of participation among members, i.e. what sectors most actively use the forum and at what frequency, to inform how to improve the forum for increased effectiveness across multiple sectors and platforms;
 - c. Data on what CSIP members do in response to shared information, e.g. send warning letters, cut-off transactions, etc., as evidence of the tangible outcomes resulting from the forum;
 - d. Information on how and to what extent the FDA, FBI, DHS or other law enforcement agencies have access to or utilize the forum for sharing information, to show the measurable value of the public-private partnership.
4. *Effectiveness of CSIP's assistance with "law enforcement efforts where appropriate?"*
- a. Data on how CSIP assisted in Operation Pangea in 2012 and 2013, to show the direct additional value of CSIP's involvement:
 - i. Number of leads solely attributable to CSIP members;
 - ii. Number of leads from other sources reviewed or confirmed by CSIP members;

- iii. Number of illegal online drug seller websites shut down by CSIP members (as opposed to taken down in response to law enforcement warning letters or other actions);
- b. Information on other ways CSIP has aided law enforcement efforts, aside from Operation Pangea, to show whether and to what extent the Internet commerce companies are involved in regular or ongoing enforcement efforts:
 - i. Data on how often CSIP liaises with law enforcement to deconflict, share, and take joint action on lead.

Question #3: If the data is not readily available, in what ways could it be obtained?

ASOP recognizes that some of these data may be sensitive and/or may not be readily available to Internet commerce companies, i.e. it may not be currently produced or collected through currently existing business practices or processes. However, for CSIP members who have committed publicly to combating illegal online drug sellers, we would nonetheless expect these companies to establish systems and processes by which to evaluate the effectiveness of their voluntary initiatives. While the Internet commerce companies themselves would best know how to measure the outcomes of their own initiatives, use of the following of systems and processes might be helpful:

1. *Monthly monitoring of the number of:*
 - a. Companies using the platform for both legal Internet pharmacies and illegal online drug sellers business purposes;
 - b. Illegal online drug seller transactions blocked;
 - c. Appeals from illegal online drug sellers seeking to use the platform's services;
 - d. Warning letters and/or compliance bulletins distributed to clients.
2. *Annual (if not monthly) use of a third-party to audit the platform for:*
 - a. Rogue activity;
 - b. Overall cleanliness, e.g. percentage rogues using the company's system for illegal online pharmacy activities.

Question #4: Are there particular impediments to measuring effectiveness, at this time or in general, and if so, what are they?

If measured by the number of illegitimate online pharmacies found in search results and other online locations, ASOP does not have first-hand knowledge of any particular impediments that would prevent Internet commerce companies and/or the government from measuring the effectiveness of voluntary actions.² Nonetheless, we have heard from CSIP that the following issues make it difficult to measure effectiveness:

² We note, however, that if measuring effectiveness were to require test purchases of pharmaceuticals from suspect online drug sellers, then impediments could include the cost and effort needed for such test purchases (including obtaining prescriptions where needed), as well as the analytical lab testing and secure handling and storing of such samples.

1. Due to differences in the sectors involved in CSIP (e.g. payment processors vs. registrars), it is difficult to determine a consistent way to measure and reflect CSIP's effectiveness;
2. Even within a sector (e.g. advertising providers), there are substantial differences in the way each company operates, again creating challenges in measuring "apples to apples;" and
3. Companies, especially smaller organizations, may not have allocated the resources (staff time, budget, etc.) that are needed to measure tangible outcomes.

While these issues may present initial challenges to CSIP's ability to measure the effectiveness of its, and its members', voluntary actions, there is a compelling public health interest in finding ways to do so. In order to vigilantly protect consumers, policymakers, regulators, law enforcement and health groups must be able to assess whether voluntary actions are working or not. If not, these stakeholders owe it to the public to take additional action, whether through new legislation, increased enforcement or other measures. Accordingly, Internet commerce companies must be expected to bear some burden of proof – even if such requires establishing additional systems and processes to measure new data points or the hiring of a third-party monitoring organization – to evidence that their programs are working. Without these data, stakeholders are unable to appropriately evaluate existing practices and determine what, if any, additional actions are warranted to better protect public health.

Question #5: What mechanisms should be employed to assist in measuring the effectiveness of voluntary initiatives?

ASOP encourages the Administration consider the following mechanisms to help evaluate the effectiveness of voluntary initiatives:

1. Mimicking the behavior of consumers looking online to purchase a prescription medicine (see response to Question #2 above) and tracking the "cleanliness" of results over time for trends and measurement of effectiveness;
2. Issuance of official recommendations from the Administration on metrics for measuring the success of voluntary initiatives that have been undertaken already and included in the IPEC strategy (2013), including a procedure to promote accountability for reporting on the outcomes;
3. An annual request for a public report to the Administration or to Congress from companies and organizations who have committed to voluntary initiatives, which would provide year-over-year information from which long-term effectiveness may be evaluated;
4. GAO investigation and/or other government audit of (1) the effectiveness of voluntary initiatives every three years which would take into consideration the Administration's official recommendations (item #1 above) and use the annual reports from companies and organizations as a means of evaluating progress (item #2 above); and (2) the extent to which rogue Internet pharmacies are utilizing companies in the same sectors that have not engaged in voluntary compliance measures; and
5. U.S. Government-organized annual public meeting to facilitate information-sharing about key voluntary initiatives and to increase dialogue among private sector, public sector, and non-government organizations to promote evaluations and improvements.

Question #6: Is there existing data regarding efficacy of particular practices, processes or methodologies for voluntary initiatives, and if so, what is it and what does it show?

ASOP understands that CSIP has made efforts to evaluate the efficacy of particular initiatives the nonprofit and its members have undertaken since 2012. CSIP has reported results available at <http://www.safemedsonline.org/who-we-are/our-results/>.

We applaud these initial outcomes from CSIP. That said, ASOP does not have full information on the methodology used or consistency (“apples to apples” nature) of information provided by CSIP’s members and thus cannot comment on the accuracy of the information provided. Also, these data reflect only the voluntary initiatives taken by the thirteen companies involved in CSIP; there are many other companies (including those based off-shore but who provide services and/or facilitate transactions to U.S. consumers) who should similarly be dedicated to protecting patients and likewise measuring the efficacy of their practices. ASOP is not aware of other existing data.

CONCLUSION

Despite the various recommendations provided herein to increase the effectiveness and impact of CSIP’s actions to date and in the future, and that of its members and future members, ASOP considers CSIP to be a crucial partner in the fight to protect patients and ensure improvements that can bring about a change to the online environment as it relates to reducing the prevalence of illegal online “pharmacies.” CSIP has undertaken a brave and new initiative that will require much learning, evaluation, and adaptation to ensure its success. The willingness to embark upon this initiative is symbolic of the corporate responsibility and forward-thinking nature of its members, and for that, we applaud them and look forward to their continued partnership and commitment to this issue.

The U.S. government plays a critical role in protecting patient safety, enforcing laws, and preventing crime. In the case of illegal online “pharmacies,” voluntary and good corporate practices by Internet commerce companies can provide a solution to advance all of these goals, decreasing the burden on government and reducing threats to patient safety (and associated costs to the health-care system). As such, the voluntary initiatives must be measured effectively to ensure progress and advance the Administration’s overriding goals. We applaud this exercise as a tool to achieve that outcome, and we hope it will be completed and used effectively to advise on next steps and future policy.

We must all work together to protect patients and the public health, public and private sector. ASOP remains committed to playing our role. In order to achieve the most beneficial outcome for patients, we must be able to adapt our rules, regulations, laws, and voluntary corporate policies to accommodate for advances and changes in technology and the availability and wide use of the Internet today. As such, we cannot allow the Internet to be a platform for crime against patients. But we must also remain vigilant to work together in a way that ensures the sustained integrity, free and open nature, and conveniences of the Internet so it continues to be a vital tool for all, enjoyed by all.

LAW ENFORCEMENT ACTIONS AND PATIENT HARMS RELATED TO ILLEGAL ONLINE DRUG SELLERS

Recent Law Enforcement Cases, Prosecutions and Investigations

A few examples of recent U.S. and international law enforcement actions involving online drug sales, in chronological order:

1. In the summer of 2011, U.S. federal agents identified a 41-year-old, Shane Lance. The agents arrested Lance and indicted him on multiple counts, including conspiracy to traffic counterfeit drugs. Last spring, he pleaded guilty to one count of conspiracy to traffic and one count of trafficking, and in November he received his sentence: 10 months in prison and a \$5,100 fine to be paid to Pfizer.³
2. In December of 2012, the State of Oregon fined Hayden Hamilton, founder of ProgressiveRx.com, \$50,000 for operating without an Oregon pharmacy license. The 35-year-old Portland businessman has shipped medicine from India and other countries to customers in the United States and around the world.⁴
3. On April 24, 2012, two men pleaded guilty and were sentenced for smuggling counterfeit and misbranded pharmaceuticals into the U.S. Both men operated an Internet business in Israel that used multiple websites to illegally sell large amounts of prescription drugs to U.S. purchasers. In total, they sent approximately 9,000 separate drug shipments to U.S. purchasers, generating over \$1.4 million in gross proceeds. Ultimately, one man received 10 months in federal prison, was fined \$30,000 and forfeited \$50,000. The other man received one year of probation, was fined \$15,000 and forfeited \$15,000.⁵
4. On August 5, 2012, Chinese government officials seized “more than \$182 million of counterfeit pharmaceuticals last month in the latest attempt to clean up a food and drug market that has been flooded with fakes.” Chinese police arrested more than 2,000 individuals and destroy 1,100 production facilities for producing counterfeit drugs.⁶
5. On August 9, 2012, a Puerto Rican man faced up to 10 years in prison after being found guilty by a jury on U.S. federal charges stemming from his role as a key operative for a drug ring that distributed large quantities of Chinese-made counterfeit pharmaceuticals throughout the United States and worldwide. Special agents with U.S. Immigration and Customs Enforcement’s (ICE) Homeland Security found more than 100,000 pills made to resemble a variety of popular prescription medications, including Viagra, Cialis, Valium, Xanax and Lipitor.⁷

³ “Inside Pfizer’s Fight Against Counterfeit Drugs,” Bloomberg Businessweek (January 17, 2013); available at <http://www.businessweek.com/articles/2013-01-17/inside-pfizers-fight-against-counterfeit-drugs>

⁴ “State fines online pharmacy with Portland ties; Oregon shipments blocked” U.S. Department of Homeland Security (December 21, 2012); available at http://www.oregonlive.com/health/index.ssf/2012/12/state_fines_online_pharmacy_wi.html

⁵ “2 Israeli men sentenced for smuggling counterfeit and misbranded pharmaceuticals into the United States” U.S. Department of Homeland Security (April 24, 2013); available at <http://www.ice.gov/news/releases/1204/120424stlouis.htm>

⁶ “China Arrest 2,000 Individuals and Destroys 1,100 Production Facilities for Making Counterfeit Drugs” Rx-360 (August 5, 2012) available at http://hosted-p0.vresp.com/427409/59c2b9a106/ARCIIVE**#>

⁷ “Man convicted for role in international counterfeit drug distribution scheme

Search continues for organization’s ringleader” U.S. Department of Homeland Security, ICE (August 9, 2012); available at <http://www.ice.gov/news/releases/1208/120809losangeles.htm>

6. On January 9, 2013, a pioneer of the Canadian Internet pharmacy business, Andrew Strempler, 38 years old, was sentenced in U.S. federal court in Miami to four years in prison for conspiracy to commit mail fraud in connection with the sale of foreign and counterfeit medicines to U.S. customers.⁸

7. On March 13, 2013, Edmond Paolucci, 54, of Coventry, Rhode Island and Patrick Cunningham, 44, of Cranston, Rhode Island, admitted to the court that they participated in a conspiracy to repackaging illegal drugs and sell them under various names and labels to consumers who placed orders via the Internet. A significant portion of the proceeds realized from the sale of the illegal drugs was laundered back to individuals in Israel.⁹

8. On March 27, 2013, nine defendants were sentenced for their roles in illegally distributing controlled substances to customers who bought the drugs from illicit Internet pharmacies. The defendants were also collectively ordered to forfeit more than \$94 million in illegal proceeds. Drug Enforcement Administration Acting Special Agent in Charge Bruce C. Balzano stated, "Prescription drug abuse has risen to alarming levels, often times leaving a trail of devastation behind and negatively impacting our communities. The individuals sentenced this week were involved in online pharmacy schemes that were illegally distributing controlled substances."¹⁰

9. On March 27, 2013, three men and one woman have been sentenced in relation to the illegal online supply of prescription only and counterfeit medicines. This follows an undercover operation by the Medicines and Healthcare products Regulatory Agency (MHRA). Searches of the homes of those involved uncovered stashes of counterfeit medication and generic prescription only medicine. This included Viagra, Cialis, diazepam and methadone. A study of a computer also showed email traffic between Andrew Luxton, Samantha Steed, Carl Willis and others indicating the previous supply of illegitimate medicine.¹¹

10. On June 27, 2013 the U.S. FDA reported the successful execution of Operation Pangea VI, a law enforcement initiative resulting in the elimination of 1,677 websites selling illegal prescription drugs. In partnership with the Department of Justice, FDA's Office of Criminal Investigations, Interpol, and authorities from nearly 100 countries took action against 9,600 websites. Dangerous drugs valued at \$41 million were seized.¹²

⁸ "Canadian Internet Pharmacy Founder Gets 4 Years In Counterfeit Drugs Case" Partnership for Safe Medicines (January 18, 2013) available at <http://www.safemedicines.org/2013/01/fake-online-pharmacy-founder-andrew-strempler-guilty-of-mail-fraud-508.html>

⁹ "Two Plead Guilty to Participation in International Conspiracy to Import and Distribute Prescription Drugs and Anabolic Steroids" Department of Justice (March 13, 2013). <http://www.justice.gov/usao/ri/news/2013/mar2013/steroids.html>

¹⁰ "Nine Sentenced For Illegally Distributing Controlled Substances Over The Internet" Department of Justice (March 27, 2013) available at http://www.justice.gov/usao/can/news/2013/2013_03_27_nine.sentenced.press.html

¹¹ "Three men and one woman sentenced in counterfeit medicines case" MHRA (March 27, 2013) available at <http://www.mhra.gov.uk/NewsCentre/Pressreleases/CON254851>

¹² "International operation targets online sale of illicit medicines" Interpol (June 27, 2013); available at <http://www.interpol.int/News-and-media/News-media-releases/2013/P077>

Examples of Patients Harmed by Medications Purchased Online

These are just a few illustrations, in chronological order, of the serious and growing global problem of illegal online drug sellers.

1. On February 12, 2001, U.S. citizen Ryan Haight died from adverse reactions to painkillers that he purchased over the Internet. He was only required to fill out a questionnaire that was "examined" by a doctor who had never met him.¹³
2. On December 17, 2006, Craig Schmidt, a 30-year-old plastics salesman, purchased Xanax (an anxiety drug) and Ultram (a painkiller) from an online drug seller without seeing or speaking to the doctor that prescribed the medications. After taking the drugs, he nearly died and has been left permanently impaired with brain damage that inhibits him from driving or even walking without stumbling.¹⁴
3. Marcia Bergeron, a Canadian resident and US citizen, died in 2006 from heavy metal poisoning caused by the contaminated prescription medications she had purchased from an illicit online pharmacy. Otherwise healthy, the coroner determined that Bergeron died of cardiac arrhythmia caused by metal toxicity from counterfeit medication. According to the coroner, the website where Marcia bought her medicines looked reputable as did the box of pills, but the drugs were actually shipped from overseas and had high levels of lead, titanium, and arsenic, which caused her death.¹⁵
4. On May 22, 2008, a man from Wichita, Kansas died from an accidental overdose of drugs he received from an online pharmacy. He obtained these drugs without ever visiting a doctor. The man's wife described her husband as "an addict --and that the Internet sites that sold him the drugs were his pushers."¹⁶
5. Steven Kovacs was a 22-year old aspiring psychologist in New York when he started buying medication online after first being prescribed Adderall, used to treat attention-deficit hyperactivity disorder, and Xanax, used to treat anxiety. Steven died of a prescription drug overdose on July 8, 2009 after mixing, Adderall, Xanax and OxyContin.¹⁷
6. Lorna Lambden, a 27-year old London paramedic, was found dead in her apartment on December 17, 2010 after she accidentally ingested a fatal dose of medication purchased from an

¹³ "Don't underestimate the danger of drugs from abroad" San Diego Union-Tribune (February 25, 2011); available at <http://www.sandiegouniontribune.com/news/2011/feb/25/dont-underestimate-the-danger-of-drugs-from-abroad/> This medicine was misused. The patient, without a prescription, purchased pain medications over the Internet. He had a serious reaction and died. The patient was only required to fill out a questionnaire that he was "examined" by a doctor who had never met him.

¹⁴ "Online Extra: The Deadly Side Effects of Net Pharmacies" Bloomberg Businessweek (December 18, 2006); available at <http://www.businessweek.com/stories/2006-12-17/online-extra-the-deadly-side-effects-of-net-pharmacies>

¹⁵ "Counterfeit Pills Bought Online Leads to Death, Coroner Confirms," The Times Colonist (July 6, 2007); available at <http://www.canada.com/victoriatimescolonist/news/story.html?id=05142ca2-9796-4868-bf42-76e939915fa5&k=29039> This medicine was contaminated with significantly high levels of metal.

¹⁶ "Widow: My Husband Died from Online Drugs" CNN (May 22, 2008); available at <http://www.cnn.com/2008/HEALTH/05/21/online.drugs/index.html?iref=allsearch> This drug was misused and abused. The medicine was purchased online without a doctor's visit or a prescription.

¹⁷ "Mom, Schumer urge Web Pharmacy Crackdown," Newsday, United States (July 10, 2011); available at <http://www.newsday.com/long-island/mom-schumer-urge-web-pharmacy-crackdown-1.3016581> This medicine was obtained without a prescription and was abused because online prescription drugs were easily accessible.

illicit foreign online pharmacy. The coroner report found four-times the therapeutic level of the drug, Amitriptyline in her blood.¹⁸

7. In January of 2010, 150 patients were admitted to hospitals in Singapore after taking counterfeit Tadalafil and herbal preparations that claimed to cure erectile dysfunction. Seven (7) of the patients were comatose and four (4) subsequently died from the online drugs which contained powerful ingredients used to treat diabetes.¹⁹
8. On June 3, 2011, an emergency room doctor, from Texas, suffered a stroke from ingesting counterfeit Alli from *www.2daydietsshopping.com*. The counterfeit Alli was produced using the controlled substance sibutramine, rather than the approved ingredient orlistat, and then shipped to the US for redistribution. Two individuals operated the site. The first is a Chinese citizen who has been sentenced to 7 years in federal prison, \$504,815.39 in restitution to victims, and deportation following his sentence. The second US citizen received 3 years probation.²⁰
9. On April 4, 2012, a mother and son in Los Angeles were looking for cold medication. They purchased and fell victim to a counterfeit drug "vitamin injection." The victim's heart rate increased rapidly, experienced severe headaches, dramatic weight loss, pass-outs and numbness in lips. The victim was eventually hospitalized.²¹
10. On April 23, 2013, Sarah Houston, a 23-year old medical student in the United Kingdom, obsessed with her weight, purchased DNP, a deadly diet pill, through an online drug seller. The pill, sold as a weight loss aid through many illicit online pharmacies, is actually a pesticide with lethal consequences to humans.²²

¹⁸ "Paramedic died after taking tablets she bought over the Internet to help her sleep," The Daily Mail, United Kingdom (May 20, 2011); available at <http://www.dailymail.co.uk/news/article-1388795/Paramedic-Lorna-Lambden-died-overdosing-sleeping-tablets.html> This medicine was purchased without a prescription and it was misused. The patient took anti-depressants as a sleeping aid.

¹⁹ "Counterfeit Internet Drugs Pose Significant Risks and Discourage Vital Health Checks," Science Daily (January 20, 2010). This contaminated medicine, claimed to cure erectile dysfunction contained a powerful drug used to treat diabetes. <http://www.sciencedaily.com/releases/2010/01/100120085348.htm>

²⁰ "June 3, 2011: Chinese National Sentenced to Federal Prison for Trafficking Counterfeit Pharmaceutical Weight Loss Drug" U.S. Department of Justice (June 3, 2011); available at <http://www.fda.gov/ICECI/CriminalInvestigations/ucm257912.htm>

²¹ "Cracking Down on Counterfeit Drugs" San Diego Union-Tribune (April 4, 2012); available at

<http://www.utsandiego.com/news/2012/apr/04/cracking-down-counterfeit-drugs/?page=1#article> This medicine was contaminated.

²² "Banned slimming drug kills medical student: Coroner attacks online dealers who target the vulnerable" The Daily Mail, United Kingdom (April 22, 2013); available at <http://www.dailymail.co.uk/health/article-2312986/Sarah-Houston-Banned-slimming-drug-DNP-kills-medical-student-coroner-attacks-online-dealers-target-vulnerable.html> This medicine was misused. The patient took both anti-depressants and a pill marketed as a weight loss aid containing lethal ingredients.



Center for Safe Internet Pharmacies

September 24, 2013

Rep. Bob Goodlatte, Chairman
Rep. John Conyers, Jr. Ranking Member
U.S. House Judiciary Committee
2309 Rayburn House Office Building
Washington, DC 20515

**Statement of The Center for Safe Online Pharmacies
Submitted in the Hearing on
"The Role of Voluntary Agreements in the U.S. Intellectual Property
System"
Before to the Subcommittee on Courts, Intellectual Property and the
Internet of
House of Representatives Judiciary Committee
September 18, 2013**

Dear Chairman Goodlatte, Ranking Member Conyers, and Members of the House Judiciary Committee:

The Center for Safe Internet Pharmacies (CSIP) respectfully submits this statement for the record of the September 18, 2013 hearing before the House Judiciary Subcommittee on Courts, Intellectual Property, and the Internet, entitled "The Role of Voluntary Agreements in the U.S. Intellectual Property System."

CSIP was founded in 2011 as a non-profit with the mission to promote and encourage safe online pharmacies. Our organization is dedicated to voluntary collaboration between Internet service providers. Our members, which do not include drug manufacturers nor pharmaceutical companies, fund and support CSIP activities, including sharing data about illegal websites, collaboration with law enforcement entities, and consumer education campaigns. Our member corporations include Google, Microsoft, Yahoo, Visa, MasterCard, American Express, Discover, eNom, GoDaddy, PayPal, Neustar, Facebook, and most recently UPS.

CSIP welcomes the Subcommittee's interest in the important role voluntary industry initiatives play in the online ecosystem. The safe purchasing of prescription drugs is fundamental to protecting consumer health and safety and, if not managed through safe and legal channels, represents a potentially fatal threat to the lives of unknowing consumers. CSIP and its member companies have made enormous progress in addressing illegal pharmaceuticals through voluntary measures.

The voluntary efforts enabled by CSIP are built on unprecedented collaboration



Center for Safe Internet Pharmacies

between the public and private sectors and have yielded positive results. The following are a few examples of the important and effective work CSIP has accomplished:

- In July 2012, CSIP launched a data-sharing portal that enabled our member companies to share information about illegal online pharmaceutical sites. Through this collaboration our members shut down activities of 3,127,235 illegal pharmacy sites.
- In partnership with LegitScript, CSIP provides an online pharmacy checker [tool](#). Consumers can enter a URL to see whether an online pharmacy is legitimate, find patient-assistance programs for affordable medications, or report illegal online pharmacies. This tool also identifies known National Association of Boards of Pharmacy (NABP) certified online pharmacies.
- CSIP participates in Operation Pangea with the FDA, INTERPOL, and other domestic and international law enforcement organizations. Operation Pangea is the largest global Internet-based operation focusing on illicit websites selling fake or counterfeit medicines. In November 2012, CSIP helped in this Operation to shut down more than 18,000 illegal pharmacy websites, and law enforcement officials seized approximately \$10.5 million worth of illegal pharmaceuticals worldwide. In June 2013, CSIP helped shut down 1,677 sites and law enforcement agents seized more than \$41 million worth of counterfeit and illegal drugs.
- CSIP has supported consumer education campaigns by the Food and Drug Administration (FDA)'s *BeSafeRX* and the Partnership for Drugfree.org's *Medicine Abuse Project*, a campaign, which generated a total of 41,265,758 social media impressions.
- As a result of CSIP's partnership with search engine advertisers, the number of illegal drug and pharmacy ads on major search engines like Google and Bing (Microsoft) has declined by 99.9%.

CSIP's voluntary efforts have been enthusiastically supported by both government and private stakeholders. The work of CSIP has been recognized in the 2013 "Joint Strategic Plan for Intellectual Property Enforcement" developed by the Office of Intellectual Property Enforcement Coordinator (IPEC). In addition, the Subcommittee's hearing on the role of voluntary efforts followed the first CSIP sponsored roundtable event held in Washington D.C. on Tuesday, September 17, 2013. This event brought CSIP member companies together with government officials from the Food and Drug Administration's Office of Criminal Investigations, the Office of the U.S. Trade Representative, the U.S. Department



Center for Safe Internet Pharmacies

of Commerce, Interpol, and the Office of the U.S. Intellectual Property Enforcement Coordinator, as well as industry leaders representing the Global Intellectual Property Center, the National Association of Boards of Pharmacy (NABP), the Pharmaceutical Security Institute (PSI), and partner organizations including LegitScript and the Alliance for Safe Online Pharmacies (ASOP), to discuss trends and issues related to illegal online pharmacies and ways to drive collaboration among organizations.

As our efforts have proven, voluntary industry initiatives have an important role to play in addressing this complex issue. CSIP remains committed to engaging in a national discussion about the rise of illegal online pharmacies and the effective role the private sector can play in curbing illegal online pharmacies.

We thank the Subcommittee for convening its hearing and for the opportunity to provide this statement for the record, and we would be pleased to provide the Committee with further information on these initiatives.

Sincerely,

Marjorie Clifton
Executive Director, Center for Safe Internet Pharmacies
info@safemedsonline.org
(202) 510-5275

cc:



September 18, 2013

Honorable Howard Coble
Chairman of the Subcommittee on
Intellectual Property, Competition, and
the Internet
U.S. House Committee on the Judiciary
2188 Rayburn HOB
Washington, DC 20515

Honorable Mel Watt
Ranking Member of the Subcommittee on
Intellectual Property, Competition, and
the Internet
U.S. House Committee on the Judiciary
2304 Rayburn HOB
Washington, DC 20515

Dear Chairman Coble and Ranking Member Watt:

The Digital Media Association ("DiMA")¹ would like to thank you for scheduling today's subcommittee hearing on the "*Role of Voluntary Agreements in the U.S. Intellectual Property System*" and providing us with an opportunity to share our thoughts on this important subject.

DiMA, and our member companies, stand at the forefront of developing new and creative ways to legally distribute entertainment content online. In the past decade, our members have revolutionized the way music can be legally purchased via online music stores. We have launched new and innovative music and video streaming services. We have transformed the traditional reading process through the widespread distribution of e-books. And, most recently, we have partnered with copyright owners to form new licensing opportunities centered upon user-generated content. In sum, our members are constantly exploring new outlets for the legitimate online distribution of digital music, film, television and books.

The byproduct of our success extends beyond specific member company benefit. It also guarantees that copyright owners will continue to be handsomely rewarded for their creative

¹ DiMA is a nationally recognized trade association that represents the legal and policy interests of America's leading online distributors of digital music, film, television and books. A full list of DiMA members can be found at <http://www.digmedia.org/about-dima/members>.

endeavors and consumers will enjoy numerous ways to *legally* access the content of their choosing.

With this in mind, DiMA welcomes the utilization of voluntary agreements to help stem unwanted acts of online infringement. Such agreements when *properly* developed have the potential to offer flexible, yet targeted solutions to online infringement that are often difficult to replicate through the traditional legislative process.

Going forward, however, the key to success in this area will depend greatly upon the ability of participating stakeholders to craft voluntary agreements that are data driven, forward-thinking and industry inclusive. The following section addresses each of these concepts in greater detail.

I. Voluntary agreements should be data-driven.

In recent years, numerous studies have been introduced for purposes of highlighting the rate at which online piracy occurs and the negative impact that it has on the U.S. economy. Yet, when these studies have been reviewed by objective third-party governmental entities the various methodologies employed by the individual researchers have been called into question² – leading other governmental entities to stress the need for additional evidence-based research.³

The lack of reliable data in this area is truly unfortunate. Accurate data can inform policymakers and relevant stakeholders of the true size of the problem associated with online infringement. Once properly developed, data can be used to determine which aspects of online piracy are most problematic; thereby providing a roadmap into which types of online infringement to tackle first. Data can also be used as a benchmark by stakeholders to measure the progress of voluntary agreements in curbing such behavior in the future.

II. Voluntary agreements should not only seek to limit access to infringing materials, but also aspire to reduce demand for infringing content.

Most of the voluntary agreements established to date have been focused primarily on eliminating unauthorized access to copyrighted protected works. The UGC principles agreement, for example, promotes the adoption of filtering technologies aimed at blocking a

² Loren Yager, Observations on Efforts to Quantify the Effects of Counterfeit and Pirated Goods, Government Accountability Office, GAO-10-423 (2010), available at <http://www.gao.gov/assets/310/303057.pdf>.

³ National Research Council, Copyright in the Digital Era: Building Evidence for Policy (2013), available at http://www.nap.edu/catalog.php?record_id=14686.

Letter to Hon. Coble and Hon. Watt, September 18, 2013.

user's ability to upload infringing materials that could otherwise be shared with third-parties.⁴ The advertiser and payment processor agreements each seek to deprive 'rogue' websites of important revenue which often serves as the financial incentive for operating such sites.⁵ And, the ultimate sanctions found in the Copyright Alert System include Internet throttling and possible temporary suspension in an effort to discourage unauthorized access of protected materials.⁶

Efforts to limit access to protected materials have merit, but they represent only a small portion of a truly viable and comprehensive solution for reducing online piracy. Indeed, recent evidence tends to indicate that the *best* way to reduce online infringement, particularly with regard to entertainment content, is through increased licensing initiatives that promise to make such materials more widely available through legitimate online outlets.⁷ Going forward, voluntary initiatives would be well served to address this topic.

III. Voluntary agreements should be structured in a way that guarantees maximum participation.

As mentioned earlier, voluntary agreements have the potential to offer well-informed, targeted solutions to help curb online infringement. The success of such mechanisms, however, will depend heavily upon the ability of conveners of future discussions to encourage a wide swath of relevant stakeholders to participate in future endeavors.

Persuading copyright owners to participate in such negotiations should prove to be quite simple. Convincing others however might be more difficult; particularly if those stakeholders

⁴ See <http://www.ngcprinciples.com/>

⁵ See http://www.aaaa.org/news/press/Pages/050312_online_piracy.aspx; see also <http://www.2013ippractices.com/>

⁶ See <http://www.copyrightinformation.org>

⁷ See Brett Dannaher, Michael D. Smith et al., *Converting Pirates Without Cannibalizing Purchasers: The Impact of Digital Distribution on Physical Sales and Internet Piracy* (2010), available at <http://ssrn.com/abstract=1381827>; see also Mary Madden, *The State of Music Online: Ten Years After Napster* (2009), Pew Internet & American Life Project, at 4, available at <http://pewinternet.org/Reports/2009/9-The-State-of-Music-Online-Ten-Years-After-Napster.aspx>; see also *Adventures in the Netherlands: Spotify, Piracy and the new Dutch Experience* (2013), available at <http://press.spotify.com/us/2013/07/17/adventures-in-netherlands/>; see also *The Washington Post. How CBS sparked more online piracy of its own show* (2013), available at <http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/08/how-cbs-sparked-more-online-piracy-of-its-own-show/>.

Letter to Hon. Coble and Hon. Watt, September 18, 2013.

view their role as nothing more than working to solve a problem caused by unrelated third-parties. In order to alleviate such problems and ensure that all participants are properly motivated, voluntary agreements should include appropriate incentives that benefit all participating stakeholders.

Conclusion

In closing, DiMA and our member companies stand willing and eager to work with members of this committee, other policymakers and representatives of the stakeholder community as they seek to craft voluntary agreements that will help bolster the viability of legitimate outlets for digital content via the elimination of online piracy. DiMA members, collectively, spend several billion dollars annually for the right to legally distribute such content, and to the extent that voluntary agreements can be viewed as a tool to help protect the current pace of growth and innovation within our industry they are a welcome addition.

If you have any questions regarding this correspondence or need any additional information, please do not hesitate to contact me at (202) 639-9502.

Sincerely,

/s/ Gregory Alan Barnes
General Counsel, DiMA

cc: Members of the Subcommittee on Intellectual Property, Competition, and the Internet

Testimony of
Future of Music Coalition
On
“The Role of Voluntary Agreements in the US
Intellectual Property System”
Hearing
House Subcommittee on the Courts, Intellectual
Property and the Internet
September 18, 2013

Testimony of Future of Music Coalition

September 18, 2013

House Subcommittee on the Courts,
Intellectual Property and the Internet
2138 Rayburn Office Building
Washington, DC 20515

September 18, 2013

Dear Chairman Goodlatte, subcommittee Chairmen Coble and Marino and members of the committee:

It is a privilege to submit the following testimony for the record in this hearing on matters relating to voluntary agreements to aid in the enforcement of United States intellectual property (IP) law.

Future of Music Coalition (FMC) is a national nonprofit education, research and advocacy organization for musicians. For 13 years, we have observed changes to traditional industry business models, and sought to inform artists about what these changes could mean for their ability to reach audiences and grow their careers. With regard to music copyrights, FMC recognizes the need to protect the rights of artists, while establishing systems that provide the returns on investment necessary to a diverse and sustainable creative sector.

There is little doubt that rapid developments in digital technology have created tremendous upheaval to traditional music business models and posed any number of challenges to individual creators with regard to their enumerated rights under US copyright law. These developments have, however, also ushered in new opportunities for creative expression and commerce while enabling for the first time in history the ability for artists to publish their work globally and near-instantaneously with the click of a mouse (or the tap of a screen).

It is not necessary to itemize the benefits of networked digital technologies in this testimony. Rather, we will examine why individual creators and independent

rightsholders must be a part of any proposed solutions to copyright enforcement—voluntary or legislative—as these constituencies are the most in need of meaningful protections yet also must retain access to today’s tools of distribution and the innovations still to come.

We are pleased that many of the theoretical concepts advanced at the beginning of the last decade by Future of Music Coalition and our allies in the musician, composer, music manager and independent label communities have come to pass. This is in no small part due to the open structures of the internet, which allow for the development of innovations that are now providing the critical infrastructure of a legitimate digital music marketplace. Today’s musicians and composers have numerous paths to audiences, and fans have an increasing array of fully licensed digital music platforms with deep catalogs of music available at a low cost and with ever-expanding interoperability.

The economics of these various platforms differ, and many are yet to mature. Existing copyright law can, by design or happenstance, aid or hinder the development of legitimate digital music services. We recognize the importance of Congress taking a close look at the current copyright regime with an eye towards optimizing the law to reflect today’s realities and accommodate the future. Intellectual property enforcement is a necessary aspect of this review, and we commend the Subcommittee for holding today’s hearing on how the needs of creators and rightsholders might be balanced with the importance of preserving platforms for speech as well as Congressionally recognized exceptions to existing protections.

There is no doubt that unauthorized distribution and access to expressive works undermines the viability of the legitimate digital marketplace, and effects everything from the perceived and actual value of existing works to the investment in the creation of new works. Enforceable IP protections are essential to the ongoing development of exciting services that can attract users, as well as the propagation of high-quality content on these services. We would advise the subcommittee at the outset, however, that not all musicians and composers are direct beneficiaries of copyright, though many benefit

indirectly from the commercial opportunities generated from copyrighted works.¹ Those who have historically made a living from copyright—such as songwriters—may feel the negative impacts of piracy disproportionately to other music creators. However, we do feel that it is important to recognize that musical artists are diverse and highly specialized and that their collective interests are not always in perfect alignment with industry trade groups and their corporate members.

FMC spends considerable effort to conduct original research into how these developments affect actual music creators. In 2010, FMC launched Artist Revenue Streams—a multi-stage research project to assess whether and how musicians' revenue streams are changing in an evolving music landscape.²

As a small musicians' nonprofit, we are limited in our ability to assess every aspect of the copyright industries and how musicians and composers fit into the overall picture. However, we hope that our work in identifying 42 discreet revenue streams available to music artists and how this compensation breaks down according to a range of factors—from professional affiliation to vocational role to geographical location—proves useful to the subcommittee and anyone curious about how musicians and composers experience these issues.

Another large chunk of our work concerns translating public policy and voluntary agreements to increase artist awareness and understanding of various proposals and initiatives. As this hearing is focused on voluntary agreements and best practices, we will highlight our recent efforts to document and translate these approaches for the benefit of creators and the public.

Pros and Cons of Voluntary Agreements and Initiatives

In the wake of contentious debates around the Stop Online Piracy Act (SOPA) and the PROTECT IP Act (PIPA), it's easy to understand why non-legislative approaches to IP

¹ Thomson, Kristin. "Off the Charts: Examining Musicians' Income from Sound Recordings Artist Revenue Streams." *Artist Revenue Streams*. Future of Music Coalition. 12 June 2012. Web. 25 Sept. 2013.

² Artist Revenue Streams. Future of Music Coalition, 01 Jan. 2010. Web. 25 Sept. 2013.

enforcement are being pursued. When stakeholders can come together to identify shared interests and potential solutions, it may result in an approach that's more collaborative and flexible than a legislative mandate. But there are also strictly practical reasons for pursuing voluntary initiatives. Partisan gridlock in Congress can mean that passing any law is a challenge. If, for example, the executive branch can get parties to the table, there may be a clearer path to implementation. Voluntary agreements may also allow corporations to avoid regulations that they find constraining or objectionable. Still, the threat of legislation can be a spur towards participation, and therefore a path to workable solutions. Aligned incentives can act as a corrective to the expensive and counterproductive combat that too often spills over into legislative branch chambers.

There are, however, some drawbacks to voluntary approaches. First, there is not always a dedicated body to compel transparency and provide oversight. Second, there is the possibility that multi-stakeholder compromise may water down any initiative to the point that it is unlikely to meaningfully impact the problem, should the parties necessary to implementation even agree to whether a problem exists.

Given the alternative, however, it seems clear that voluntary approaches are the best bet for a range of parties to collaborate on solutions that don't inherently disadvantage any one sector, while retaining the flexibility to respond to unanticipated challenges or unforeseen consequences of a given initiative. We commend the lawmakers and officials who have stepped up to the challenge of bringing parties to the table—particularly the Office of the Intellectual Property Enforcement Coordinator (IPEC)—as a means of avoiding the time, monetary and reputation costs of poorly thought-through or overly politicized legislation.

The Copyright Alert System (CAS)

FMC observed closely developments around establishing a protocol for Internet Service Providers (ISPs) and rightsholders to collaborate on a non-legally binding enforcement agenda. Initial reports and the subsequent Memo of Understanding between rightsholders and ISPs indicated that the CAS would not be overly punitive but rather a shared attempt

to educate alleged infringers of the availability of legal platforms with the potential of mitigation measures should a series of warnings—often referred to as “graduated response”—remain unheeded by an internet user. We are sensitive, as are many, to the need to preserve access to a critical lifeline, and were pleased that implementation of the CAS did not include provisions to disconnect Internet users at any point in the process. We also applauded the decision to avoid potentially invasive technologies to monitor the network, but instead rely on public trackers to scan for infringing activity. We would reinforce the notion that transparency and oversight of the CAS is crucial not only to its effectiveness, but also to build trust among communities that have too often come to regard one another with suspicion. As our March 07, 2013 *Billboard* Op-Ed³ pointed out, “[Such] an effort will benefit from transparency in order to build trust among stakeholders and to measure effectiveness. The former is key to making smarter choices around enforcement and growing the legitimate marketplace in a way that benefits not just the big companies, but also creators. In this way, incentives might be better aligned and artists and fans can gain confidence in today’s music ecosystem. Even if it was designed to limit unintended consequences, the CAS must operate in plain sight.”

Payment Processor Best Practices for Online Copyright Infringement

American Express, Discover, MasterCard, PayPal and Visa are among the payment processors who have agreed to adopt voluntary measures to deal with websites trafficking in ill-gotten IP. Rightsholders can now interface with the payment processors regarding alleged infringement of their rights online. The payment processors will then contact the online merchant—a site or service offering the content—about the complaint and respond in a manner consistent with protocols agreed upon in these best practices. This new system hopefully establishes a reasonably open, transparent and efficient mechanism for reporting infringement direct to the payment processor for review and potential action. FMC took the time to describe in some detail the ins-and-outs of these voluntary provisions in order for individual artists to avail themselves of the process.⁴ We have, and

³ Rae, Casey. “Will the Copyright Alert System Break the Internet? By Future of Music Coalition’s Casey Rae.” *Billboard*. N.p., 07 Mar. 2013. Web. 25 Sept. 2013.

⁴ “Payment Processor Best Practices for Online Copyright Infringement.” *Payment Processor Best Practices for Online Copyright Infringement: What It Means for Musicians*. Future of Music Coalition, 24 Oct. 2011. Web. 25 Sept. 2013.

continue to encourage the timely evaluation of this agreement to monitor for potential abuses as well as to identify its successes.

Best Practices for Online Ad Networks

“Best Practices Guidelines for Ad Networks to Address Piracy and Counterfeiting” is a joint effort to reduce the flow of ad revenue to infringing websites. The initiative is supported by the Interactive Advertising Bureau, along with 24/7 Media, Adtegrity, AOL, Condé Nast, Google, Microsoft, Yahoo! and SpotXchange. It is beyond our technical aptitude to comment on the specific aspects of advertising networks germane to a discussion of combatting infringement, but we are impressed at the willingness of participating parties to identify a path forward that does not appear to compromise the flexibility of an important new avenue for legitimate commerce. Perhaps unsurprisingly, there are some in the music community who feel that these agreements do not go far enough.⁵ For our part, FMC encourages a thoughtful, inclusive and deliberate approach to measure the effectiveness of this entirely new protocol before passing judgment on the efficacy of a system that is still in its nascent stages of implementation.

Conclusion

FMC remains committed to advocating for a copyright regime that reflects the balance between creator and those who benefit from exposure and access to a diversity of expression. We support and will continue to participate in ongoing discussions among a range of stakeholders—including the often-overlooked independent sector—regarding mutually beneficial approaches to copyright enforcement. We humbly offer our perspectives and data to the subcommittee and the entire Congress for its consideration as it continues its inquires into the contours of intellectual property in the digital age.

Casey Rae
Interim Executive Director
Future of Music Coalition

⁵ “But This Time We Mean It... Welcome To The Ad Tech Time Machine...” *The Trichordist*. N.p., 24 July 2013. Web. 25 Sept. 2013.

Statement of Microsoft Corporation
Submitted in the Hearing on
“The Role of Voluntary Agreements in the U.S. Intellectual Property System”
Before to the Subcommittee on Courts, Intellectual Property and the Internet of
House of Representatives Judiciary Committee
September 18, 2013

Microsoft appreciates the opportunity to comment on the role of voluntary agreements in intellectual property system, the subject of the Subcommittee’s hearing on September 18, 2013. Microsoft has been deeply involved in several relevant voluntary initiatives, such as the guidelines for advertising networks announced in July 2013 by the U.S. Intellectual Property Enforcement Coordinator (IPEC),¹ the 2012 statement of best practices issued by the Association of National Advertisers (ANA) and American Association of Advertising Agencies (4A),² and the principles for user-generated content services developed by leading media and technology companies in 2007.³ We have also participated in other stakeholder dialogues involving online intellectual property issues around the world. This statement summarizes our experience with efforts like these and why we think they are a positive and useful force in improving the intellectual property system.

Microsoft approaches these issues from dual perspectives, as a copyright owner and as an online service provider. As a copyright owner, we have long relied on the law to protect our core software products like Windows, Microsoft Office and Xbox games and to ensure that our customers enjoy legitimate and safe copies of our software. Our world-class antipiracy team works hard to make enforcement of our intellectual property efficient and effective, and these efforts benefit from voluntary initiatives. For example, our anti-piracy team has relied on the payment processor best practices announced by the IPEC in 2011 to combat counterfeit online sites operated by criminal syndicates by having them cut off from legitimate payment networks.

As an online service provider, we offer services and advertising networks that on occasion can be abused by some engaging in infringing activity. Voluntary initiatives provide companies like Microsoft with a framework to address such activity in practical and pragmatic ways that both benefit rights holders and do not interfere with legitimate activity of customers and partners.

Voluntary initiatives play a vital role because the rapid development of technology continues to present challenges to existing intellectual property laws. For example, copyright laws in the United States and around the world have been updated frequently over the past two decades to address new technologies, including the enactment of the landmark Digital Millennium Copyright Act. Yet new devices, new services, new networks and new business models keep coming, each raising new questions

¹ <http://www.2013ippractices.com/>. See also Victoria Espinel, “Coming Together to Combat Online Piracy and Counterfeiting”, (July 15, 2013) (<http://www.whitehouse.gov/blog/2013/07/15/coming-together-combat-online-piracy-and-counterfeiting>).

² ANA, “Industry Groups Urge Marketers to Take Affirmative Steps to Address Online Piracy and Counterfeiting” (May 3, 2012) <http://www.ana.net/content/show/id/23407>.

³ “Principles for User-Generated Content Services” (Oct. 2007) (<http://ugcprinciples.com/>)

about the applicability even of recent laws. Voluntary agreements play a critical role by filling gaps, avoiding wasteful litigation and giving guidance to stakeholders on how to follow the law in day-to-day operations. They can help stakeholders implement legal rules and adapt to the demands of today's technology and business.

As an example, Microsoft was deeply involved in the "Best Practices Guidelines for Ad Networks to Address Piracy and Counterfeiting", developed recently by ad networks under the auspices of the IPEC.⁴ An online ad network adopting the best practices undertakes, upon receipt of specific notices from rights holders, to exclude websites primarily engaged in piracy and counterfeiting from participating in the network. The best practices also specify that ad networks should maintain a counter-notice system to correct any mistaken takedowns, which is essential to ensuring that legitimate activity is not disrupted. This "notice and takedown" system is built on the same stable foundation as Section 512 of the Digital Millennium Copyright Act, a foundation that has served both to unleash new innovative online services and to enable efficient and effective copyright enforcement online.

Similarly, the 2012 ANA and 4A pledge also makes notice and takedown the primary mechanism to address piracy and counterfeiting. It requires advertising networks to keep pirate and counterfeiting sites from placing or publishing advertisements "in response to reasonable and sufficiently detailed complaints or notices from rights holders and advertisers." This approach strikes the best and most reasonable balance between the legitimate needs of rights holders and the legitimate concerns of online services and advertising networks.

It is important to note that notice and takedown is as integral to Microsoft's online services as it is to the goals Microsoft's own antipiracy efforts, which work closely with online services – large and small – to make notice and takedown work smoothly and effectively.

In sum, voluntary efforts, such as the ad network best practices and ANA/4A pledge, help reinforce that notice and takedown is not just an abstract concept in the intellectual property statutes, but a practical and effective way for online services to address infringement yet still have room to grow and create great customer experiences. Complementing legislation such as the DMCA, the many best practices and other voluntary initiatives undertaken in the past few years provide robust and appropriate measures that promote online enforcement of intellectual property. Voluntary efforts may not solve every online intellectual property issue, but it is important that the existing legal measures and practices are given every chance to address the problem before any new legislation is considered.

Once again, Microsoft appreciates the opportunity to submit this statement to the Subcommittee, and would be pleased to answer any questions Members may have.

⁴ *Microsoft on the Issues*, "Microsoft applauds release of Best Practice Guidelines for Ad Networks to Address Piracy and Counterfeiting" (July 15, 2013) (http://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/07/15/microsoft-applauds-release-of-best-practice-guidelines-for-ad-networks-to-address-piracy-and-counterfeiting.aspx)

Links to Additional Material submitted for the Record

- 1) ANA/4As joint statement of best practices: <http://www.ana.net/content/show/id/23408>
 - 2) IAB Network and Exchanges Quality Assurance Guidelines:
http://www.iab.net/QAGInitiative/overview/quality_assurance_guidelines
 and
http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-072513
 - 3) Ad Network best practices:
<http://www.whitehouse.gov/blog/2013/07/15/coming-together-combat-online-piracy-and-counterfeiting>
<http://www.2013ippractices.com/bestpracticesguidelinesforadnetworkstoaddresspiracyandcounterfeiting.html>
 - 4) The UGC Principles: <http://www.ugcprinciples.com>
 - 5) ISP MOU documents. For more information, the CCI website is
www.copyrightinformation.org
 including a video on how the copyright alert system works, available at
<http://www.copyrightinformation.org/the-copyright-alert-system>
 - 6) Information about the payment processor best practices:
<http://www.whitehouse.gov/sites/default/files/omb/IPEC/2013-us-ipecc-joint-strategic-plan.pdf> (2013 IPEC report)
<http://www.uspto.gov/ip/officechiefecon/PTO-C-2013-0036.pdf#page=33> (IACC comments to PTO request for comments)
<http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf> (IACC 1 year report)
- Complaint procedures available from some of the payment processors who have implemented the best practices:
- <https://www.paypal.com/webapps/mpp/ua/infringementrpt-full?locale.x=en-US>
http://corporate.visa.com/about-visa/security-and-trust/intellectual-property-rights.shtml?ep=v_sym_ReportBrandAbuse
http://www.mastercard.com/us/wce/PDF/MasterCard_Anti-Piracy_Policy.pdf
<http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf>
- 7) The ICANN resolution re: enhanced safeguards for new gTLDs to address, among other things, copyright infringement, and related documents:
<http://www.icann.org/en/groups/board/documents/resolutions-new-gtld-25jun13-en.htm#2.b>

