AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

ANTI-COUNTERFEITING AMENDMENTS OF 2003

HEARING

BEFORE THE

SUBCOMMITTEE ON COURTS, THE INTERNET, AND INTELLECTUAL PROPERTY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

ON

H.R. 3632

FEBRUARY 12, 2004

Serial No. 61

Printed for the use of the Committee on the Judiciary

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

U.S. GOVERNMENT PRINTING OFFICE

91–752 PDF WASHINGTON : 2004

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) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*

HENRY J. HYDE, Illinois
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
WILLIAM L. JENKINS, Tennessee
CHRIS CANNON, Utah
SPENCER BACHUS, Alabama
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
RIC KELLER, Florida
MELISSA A. HART, Pennsylvania
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
JOHN R. CARTER, Texas
TOM FEENEY, Florida
MARSHA BLACKBURN, Tennessee

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
LINDA T. SÁNCHEZ, California

PHILIP G. KIKO, *Chief of Staff-General Counsel*
PERRY H. APELBAUM, *Minority Chief Counsel*

SUBCOMMITTEE ON COURTS, THE INTERNET, AND INTELLECTUAL PROPERTY

LAMAR SMITH, Texas, *Chairman*

HENRY J. HYDE, Illinois
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
WILLIAM L. JENKINS, Tennessee
SPENCER BACHUS, Alabama
MARK GREEN, Wisconsin
RIC KELLER, Florida
MELISSA A. HART, Pennsylvania
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
JOHN R. CARTER, Texas

HOWARD L. BERMAN, California
JOHN CONYERS, JR., Michigan
RICK BOUCHER, Virginia
ZOE LOFGREN, California
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York

BLAINE MERRITT, *Chief Counsel*
DAVID WHITNEY, *Counsel*
MELISSA L. MCDONALD, *Full Committee Counsel*
ALEC FRENCH, *Minority Counsel*

CONTENTS

FEBRUARY 12, 2004

OPENING STATEMENT

Page

The Honorable Lamar Smith, a Representative in Congress From the State of Texas, and Chairman, Subcommittee on Courts, the Internet, and Intellectual Property 1

The Honorable Howard L. Berman, a Representative in Congress From the State of California, and Ranking Member, Subcommittee on Courts, the Internet, and Intellectual Property 2

WITNESSES

Mr. Richard LaMagna, Senior Manager, Worldwide Investigations, Microsoft
Oral Testimony 5
Prepared Statement 6

Mr. Emery Simon, Counselor, Business Software Alliance (BSA)
Oral Testimony 11
Prepared Statement 12

Mr. Brad Buckles, Executive Vice President, Anti-Piracy, Recording Industry Association of America, Inc. (RIAA)
Oral Testimony 13
Prepared Statement 15

Mr. David Green, Vice President and Counsel, Technology and New Media, Motion Picture Association of America (MPAA)
Oral Testimony 20
Prepared Statement 21

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement of the Honorable Bob Goodlatte, a Representative in Congress From the State of Virginia 31

Prepared Statement of the Honorable John Conyers, Jr., a Representative in Congress From the State of Michigan, and Ranking Member, Committee on the Judiciary 31

Prepared Statement of the Honorable Howard L. Berman, a Representative in Congress From the State of California 32

ANTI-COUNTERFEITING AMENDMENTS OF 2003

THURSDAY, FEBRUARY 12, 2004

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON COURTS, THE INTERNET,
AND INTELLECTUAL PROPERTY,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to call, at 10:05 a.m., in Room 2141, Rayburn House Office Building, Hon. Lamar Smith (Chair of the Subcommittee) presiding.

Mr. SMITH. The Subcommittee on Courts, the Internet, and Intellectual Property will come to order. Today's hearing is on H.R. 3632, the "Anti-counterfeiting Amendments of 2003."

Let me say at the outset we have a sparse attendance today. That is not necessarily due to the a lack of interest in the subject. It is due primarily to the fact that we finished votes for the week yesterday and we are not in session today and, frankly, we are fortunate to have Mr. Berman here.

But, nevertheless, we will establish a record today. This is a hearing; and it will lead, we hope, to a constructive markup in weeks to come. So everything we do here today is important to all of us, either now or in the future.

I am going to recognize both of us for opening statements. Then we will proceed to introducing the witnesses and having questions.

Counterfeiting is deceit, the functional equivalent of a lie. It results in lost profit, lost jobs, and lost tax revenue on a scale that threatens otherwise vibrant industries. Software piracy remains a serious problem throughout the world, accounting for 25 percent of the software used in the United States and 40 percent of the software used worldwide.

The software industry loses $11 billion each year from counterfeiting and other forms of software piracy. These revenue losses translate into lost jobs and a hit on the American economy. Because of the opportunities for high profits and the low risk of prosecution, software counterfeiting has become part of a web of international organized crime.

Although crime groups based in Asia produce the largest quantity of counterfeits, manufacturing and distribution centers exist throughout the world. In fact, California is a major entry and assembly point for counterfeit software and CD-ROMs and components.

For many years, software publishers have attempted to thwart counterfeiting activity by developing physical authentication com-

ponents to help consumers and law enforcement agencies distinguish between genuine software and sophisticated counterfeits. For example, one of our witnesses today represents a company, Microsoft, that packages its product with a certificate of authenticity, or COA, that incorporates special inks, holograms, and microtexts.

As these physical authentication components increase in sophistication, counterfeiters find it increasingly difficult to create counterfeits that look like the genuine components. To bypass this problem, counterfeiters combine genuine components with counterfeit CD-ROMs and packaging, the goal being to deceive the consumer. The genuine components are obtained through theft or other illicit means and then sold as separate commodities through the Internet and other distribution channels.

Genuine COAs and other physical authentication components are in high demand because they significantly increase the marketability and selling price of counterfeit software. Even though standalone COAs have no intrinsic value or legitimate use, they sell for as much as $80 apiece because of their value to counterfeit operations.

Since neither State nor Federal law specifically prohibits trafficking in genuine authentication components, prosecutors in several recent counterfeiting raids in fact have refused to even pursue prosecution.

Federal law does not expressly prohibit such activities, so genuine COAs and other physical authentication components are widely sold throughout the United States with impunity, facilitating the sale of counterfeit software and frustrating efforts to combat an increasingly important link in the counterfeit supply chain.

H.R. 3632 closes this loophole and empowers Federal authorities to prosecute counterfeiting activity on a greater scale with better result.

We have a distinguished panel today that can speak to the need for this legislation and I hope also to receive shortly the views of the Department of Justice as well.

That concludes my opening statement; and the gentleman from California, Mr. Berman, is recognized for his opening statement.

Mr. BERMAN. Thank you very much, Mr. Chairman.

The sheer drama, the theater of a hearing on the Anti-counterfeiting Amendments of 2003 caused me to stay over and attend today's hearing.

In last Congress, similar bills were introduced in both the House and the Senate, but the Subcommittee has never had a chance to analyze this issue. So I am looking forward to hearing from our witnesses.

Each day thieves around the world steal millions of dollars worth of American intellectual property from the rightful owner. American innovation is the cornerstone of the economy. The copyright industry alone employed over 8 million Americans in 2001. Software piracy alone has cost the U.S. economy thousands of jobs and drains almost $11 billion each year.

According to the International Anticounterfeiting Coalition, U.S. Customs seized more than $98 million in counterfeit and pirated goods in 2002, a 58 percent increase over 2001. To exacerbate the problem, counterfeiters of software music, CDs and motion pictures

are no longer limiting themselves to pirating the actual goods. They are now tampering with a component of the goods, the authentication features which are used to ensure the genuineness of the product. This is what the bill is designed to address.

Just 2 weeks ago, Microsoft filed a suit in Federal Court alleging the theft of counterfeit software and related items. The claim alleges that the defendants distributed counterfeit certificate of authenticity labels.

Federal law currently provides a remedy for this type of counterfeiting. However, what it does not do is address the gap in Federal law that fails to address trafficking in genuine labels which are then used, attached—connected with counterfeit or pirated goods.

Last year, the Microsoft witness who is with us today testified before this Subcommittee about the global threat of software counterfeiting. In his written testimony he described the cheap, fake software sold on street corners which is typically marketed as the genuine article to unsuspecting customers who would never knowingly purchase counterfeit goods but love to get genuine goods at 10 percent of what they would otherwise cost them.

To create the look of genuine packaged software, counterfeiters use state-of-the-art technology to create near-perfect copies of CD-ROMs as well as the packaging documentation and other components.

For many years, Microsoft and I am sure many other companies have worked to outpace counterfeiting technology by developing physical features that help consumers and law enforcement agencies distinguish legitimate software from sophisticated counterfeits. However, as software makers have worked hard to ensure protection of their intellectual property, the counterfeiters have worked harder and smarter.

Microsoft has include a certificate of authenticity that incorporates special inks, holograms, and microtext in its software. So far, the counterfeiters have found it impossible to replicate the technology. But as the technology used to protect intellectual property has gotten more sophisticated, so have the counterfeiters. Because physical anticounterfeiting features are increasingly difficult to reproduce, counterfeiters are now combining pirated CD-ROMs and packaging them with the genuine authentication components obtained through fraud or theft.

Through a gap in the law, we have actually created a separate market for merely the authentication components. The bill expands the scope of counterfeit rules to include other physical authentication components such as certificates. In addition, it addresses the situation where genuine certificates are distributed not in connection with the product of the copyright owner or where the label is altered to falsify the number of authorized copies.

The bill also authorizes the forfeiture of equipment used to manufacture these labels, instead of only a pirated product, and provides for civil remedies for violation of the act.

While this bill confronts the concept of trafficking physical components parts, I would be interested in hearing from our witnesses about interpretation or expansion of the bill to include digital components.

In an age where the technology is rapidly developing, it seems to me there is a need to address the evolution of digital authentication features and the potential for copying or counterfeiting them as well. The legal dichotomy of physical and digital should be a distinction without a difference. Whether a physical or digital feature is counterfeited is equally problematic.

I don't intend for this to become another digital management debate. I do, however, wish to address punishing and preventing counterfeiting. Counterfeiters do not only prey on the copyright owners. They prey on the consumers who have certain expectations when buying what appears to be a genuine product.

So if the Chairman is so inclined at some point, I look forward to working with him on these issues before the markup. Thank you, Mr. Chairman; and I yield back.

Mr. SMITH. Thank you, Mr. Berman.

Let me introduce our witnesses today.

The first witness is Rich LaMagna, who is the Senior Manager of Worldwide Investigations at Microsoft, where he manages global antipiracy investigations. He provides policy and operational guidance to members of Microsoft's worldwide anticounterfeiting team. He received a BA from Gettysburg College and a Masters of Arts from Georgetown University. He is a graduate of the Foreign Service Institute and is fluent in Cantonese, Mandarin and French. We will not ask you to demonstrate any of those today.

The next witness is Emery Simon, who is a policy counselor to the Business Software Alliance. BSA members include the leading American software and computer companies in the business of developing creative software solutions for the workplace, school, and the home. Mr. Simon earned a law degree from Georgetown University, a masters degree in international affairs from Johns Hopkins University and a bachelors degree from Queens College.

Our next witness is Brad Buckles, who is Executive Vice President of the Recording Industry Association of America. Mr. Buckles heads RIAA's antipiracy unit, which includes investigators throughout the United States who work with law enforcement agencies to combat piracy. Mr. Buckle retired from his post as Director of the U.S. Bureau of Alcohol Tobacco, Firearms and Explosives after 30 years of service. Before joining the ATF, Mr. Buckles earned his bachelors degree from the University of Wyoming and a law degree from Washburn University.

Our last witness is David Green, who joined the Motion Picture Association of America last year as vice president and counsel of technology and new media. Mr. Green focuses on legal issues related to the Internet and other digital electronic distribution systems. Mr. Green joined MPAA after 16 years at the U.S. Department of Justice. He graduated from Oberlin College and received his law degree from the University of Pennsylvania Law School.

Welcome to you all. We have your complete statements; and, without objection, they will be made a part of the record. Even though we are not in a huge rush today, I would like to ask you to limit your testimony to 5 minutes; and then we will follow up with questions.

We will begin with you, Mr. LaMagna.

STATEMENT OF RICHARD LAMAGNA, SENIOR MANAGER, WORLDWIDE INVESTIGATIONS, MICROSOFT

Mr. LAMAGNA. Thank you, Mr. Chairman. It is a pleasure to be here again.

Mr. Chairman, Members of the Subcommittee, thank you for the opportunity to testify on this important and much-needed anticounterfeiting legislation.

My name is Richard LaMagna, Senior Manager of Worldwide Investigations at Microsoft. I joined Microsoft in 1999 after a 28-year career as a Special Agent with the DEA and the FBI investigating international drug trafficking organizations.

Mr. Chairman, Microsoft supports and commends you for introducing H.R. 3632, the Anti-counterfeiting Amendments Act of 2003, legislation that would prohibit an increasingly pervasive activity that directly facilitates counterfeit software sales. Microsoft views this legislation as the single most important step that Congress can take to fight software counterfeiting in this country.

Software counterfeiting is a particularly pernicious and widespread form of criminal piracy that defrauds American consumers and funds a wide array of organized criminal enterprises. As a founding member of the Business Software Alliance, Microsoft has for many years worked closely with the BSA and law enforcement to halt the manufacture and sale of counterfeit software. These efforts have led to annual seizures of almost $2 billion in counterfeit Microsoft products.

Software counterfeiters go to great lengths to make pirated software look genuine in an effort to deceive the consumer and maximize illicit products. Here is an example of counterfeit Office 97, a version of Microsoft's most popular product suite. Even the most sophisticated consumer would have great difficulty in distinguishing this counterfeit package from the genuine item.

Software counterfeiters use state-of-the-art technology to counterfeit CD-ROMs and packaging that bears all the hallmarks of the genuine products. For many years, Microsoft has worked to develop physical security components that help consumers and law enforcement agencies distinguish legitimate software from sophisticated counterfeits, much in the same way the U.S. Government uses physical security features to authenticate its paper currency. For example, Microsoft's certificate of authenticity, known as the COA, incorporates several proprietary technologies, including special inks and microtext.

Because these physical security components are increasingly difficult to reproduce, counterfeiters are now combining pirate CD-ROMs and packaging with genuine components obtained through theft of fraud.

Mr. LAMAGNA. For the past few years more than a half a million certificates of authenticity, which we call COAs, with a market value of over $50 million have been stolen from manufacturing facilities in the U.S. and Europe. The stolen COAs are then sold to counterfeiters through a variety of brokers and distribution networks, including over the Internet.

Currently Federal law does not provide adequate remedies to prevent trafficking in genuine fiscal security components even though there is no legitimate business purpose for this activity.

The persons who traffic in COAs and other physical security components know full well that the components have no intrinsic value or use other than to facilitate the sale of counterfeit software. Nevertheless, because these brokers carefully remain a few steps removed from the thefts or the counterfeit sales, prosecutors find it impossible to take any legal action even though the components will unquestionably fall into the hands of counterfeiters.

H.R. 3632 would amend section 2318 of title 18 to prohibit trafficking in genuine physical components used by Microsoft and other copyright owners to verify that a copyrighted work is legitimate and not counterfeit. With this narrowly-tailored amendment to section 2318, Federal law enforcement and copyright owners will have the tools needed to prevent trafficking in genuine physical security components.

Microsoft looks forward to working with the Chairman and the Members of this Subcommittee to obtain passage of this important anticounterfeiting legislation. It is imperative that our laws keep pace with developments in software counterfeiting, particularly given the involvement of international organized crime in the counterfeiting trade. Like drug traffickers, software counterfeiters have global networks of well-financed and sophisticated criminal groups capable of producing and distributing billions of dollars worth of counterfeit software each year.

Federal and local law enforcement in California, with the help of Microsoft's investigative team, seized one shipment of software worth over $100 million. The raid disrupted a major international counterfeiting operation financed by criminal groups in Asia.

The anticounterfeiting amendments will help combat the growing threat of international counterfeiting crimes by ensuring that U.S. laws address all aspects of counterfeiting activities.

In closing, Microsoft strongly supports this important legislation and urges this Subcommittee to pursue its swift enactment.

Thank you, Mr. Chairman.

[The prepared statement of Mr. LaMagna follows:]

PREPARED STATEMENT OF RICHARD C. LAMAGNA

Mr. Chairman, Members of the Subcommittee, thank you for the opportunity to testify on this important and much-needed anti-counterfeiting legislation. My name is Rich LaMagna, and I am Senior Manager of Worldwide Investigations at Microsoft Corporation. I joined Microsoft in 1999 after a 28-year career as a Special Agent with the DEA and the FBI investigating international drug trafficking organizations.

Mr. Chairman—Microsoft commends you for your leadership in introducing the Anticounterfeiting Amendments of 2003, legislation that would prohibit a narrowly-defined but pervasive category of activities that directly facilitate counterfeit software sales. Microsoft views this legislation as the single most important step that Congress can take to fight software counterfeiting in this country.

I. THE SCOPE AND IMPACT OF SOFTWARE COUNTERFEITING

A. Economic Contribution of the Commercial Software Industry

Over the past 25 years, computer software has fundamentally reshaped every facet of our lives and helped secure this country's economic leadership. By the late 1990s, the software industry employed more than 800,000 U.S. workers with aggregate wages of $55.6 billion. By the year 2008, the software industry is expected to employ more than 1.3 million workers in the United States alone.

Annually, the software industry contributes more than $28 billion in tax revenues to federal and state governments, benefiting a host of national and community programs. This tax contribution is expected to reach $50 billion by the year 2008. Also

significant is the industry's contribution to the U.S. balance of payments. While the U.S. trade deficit reached new record highs in 2000, the U.S. software industry generated a trade surplus of more than $20 billion. The software industry's growing trade surplus means more jobs and tax revenues for the U.S. economy.

The success of the U.S. software industry is due in large part to this country's historical commitment to strong intellectual property protection. It is no coincidence that the United States—the world's leading advocate for intellectual property rights—is also home to the world's largest software industry. The software industry's continued growth and economic contributions are directly dependent on our ability as an industry and a nation to eliminate software theft.

B. Economic Impact of Software Piracy and Counterfeiting

For almost fifteen years, the software industry has battled against software theft, recognizing that widespread piracy threatens the very existence of our industry. Despite these efforts, software piracy remains a serious problem throughout the world, accounting for one-quarter of the software used in the United States, and 40 percent of the software used worldwide. In parts of Asia and the former Soviet Republic, piracy rates approach 90 percent, virtually eliminating sales of legitimate software.

The software industry loses $13 billion each year from counterfeiting and other forms of software piracy. Annual seizures of counterfeit Microsoft products exceed $1.7 billion. These revenue losses directly translate into lost jobs and opportunities for the U.S. economy. By the late 1990's, software piracy had cost the U.S. economy more than 109,000 jobs and almost 1 billion in tax revenues; by 2008, piracy-related losses will nearly double, accounting for 175,000 lost jobs and $1.6 billion in lost tax revenues.

II. TRENDS IN SOFTWARE COUNTERFEITING OPERATIONS

Unlike the cheap fakes sold on street corners, counterfeit software is typically marketed as genuine product to unsuspecting consumers who would never knowingly purchase illegal products. To create the look of genuine packaged software, counterfeiters use state-of-the-art technology to create near-perfect copies of Microsoft CD-ROMs, packaging, documentation and other components. Because counterfeiters bear none of the R&D, marketing or support costs that determine the price of legitimate software, these criminal operations are able to reap enormous profits from the sale of counterfeits.

A. Trafficking in Physical Anti-counterfeiting Features

For many years, Microsoft has worked to outpace counterfeiting technology by developing physical product features that help consumers and law enforcement agencies distinguish legitimate software from sophisticated counterfeits, much in the same way the US Government authenticates its paper currency. For example, Microsoft packaging has for many years included a certificate of authenticity ("COA") that incorporates special inks, holograms and micro-text. Microsoft has invested several millions of dollars to develop an edge-to-edge hologram that covers the entire surface of the CD-ROM. (Examples of these features are included in Attachment A to this testimony.) The edge-to-edge hologram involves a highly sophisticated, proprietary technology that is etched into recent versions of Microsoft Office.

Because these physical anti-counterfeiting features are increasingly difficult to reproduce, counterfeiters are now combining pirate CD-ROMs and packaging with genuine components obtained through theft or fraud. In recent years, more than 100 robberies of authorized replicators in the US and Europe have netted 540,000 Microsoft COAs with an estimated value of $50 million. According to our sources, genuine COAs, end user manuals, end user license agreements and other physical components are in high demand among counterfeiters because they significantly increase the marketability and selling price of counterfeit software.

So far, counterfeiters have found it impossible to replicate the edge-to-edge technology. As an alternative, they have developed holographic stickers that, when attached to the CD-ROM, closely resemble the look of the edge-to-edge hologram. Recent versions of these fake stickers found in Asia are of such high quality, few consumers would be able to detect the counterfeit.

B. Anticounterfeiting Amendments of 2003

Currently, federal law does not provide adequate civil and criminal remedies to prevent trafficking in genuine physical security components, even though there is no legitimate business purpose for this activity. The persons who traffic in COAs and other physical security components know fully well that the components have no intrinsic value or use other than to facilitate the sale of counterfeit software. Nevertheless, because these brokers are a few steps removed from the component

thefts or the counterfeit sales, prosecutors find it impossible to take any legal action, even though the components will unquestionably fall into the hands of counterfeiters.

H.R. 3632 would amend Section 2318 of Title 18 to prohibit trafficking in genuine physical security components used by Microsoft and other copyright owners to verify that a copyrighted work is legitimate and not counterfeit. With this narrowly-tailored amendment to Section 2318, federal law enforcement and copyright owners will have the tools needed to prevent trafficking in genuine physical security components. Microsoft looks forward to working with the Chairman and the Members of this Subcommittee to obtain passage of this important anti-counterfeiting legislation.

III. INVOLVEMENT OF ORGANIZED CRIME IN SOFTWARE COUNTERFEITING OPERATIONS

Because of the enormous opportunities for profits and the low risk of prosecution or significant punishment, software counterfeiting has become part of an intricate web of international organized crime. Although Asian crime groups produce the largest quantity of sophisticated counterfeits, manufacturing and distribution centers exist throughout the world. In fact, California is a major entry and assembly point for counterfeit software CD-ROMs and components.

The federal government explicitly acknowledged the growing involvement of organized crime when it created a new "Intellectual Property Rights Initiative" in 1999 to strengthen enforcement against intellectual property crime. At a congressional hearing, former Customs Commissioner Ray Kelly stated that—

> *Our investigations have shown that organized criminal groups are heavily involved in trademark counterfeiting and copyright piracy. They often use the proceeds obtained from these illicit activities to finance other, more violent crimes. These groups have operated with relative impunity. They have little fear of being caught—for good reason. If apprehended, they face minimal punishment. We must make them pay a heavier price.*

Global counterfeiting flourishes because counterfeiters face little risk of prosecution or meaningful punishment. In the United States, Microsoft and other intellectual property owners have worked closely with Congress and federal authorities to ensure that counterfeiting laws, enforcement, and penalties keep pace with counterfeiting crimes. In recent years, these efforts have led to important reforms, including improved sentencing guidelines for intellectual property crime, increased appropriations for IP-related law enforcement activities, and the creation of the FBI Cyber Division.

In addition, Microsoft invests millions of dollars each year to assist law enforcement in investigating criminal counterfeiting operations. Microsoft's worldwide anti-piracy team consists of more than 100 attorneys, forensic experts, and in-house and outside investigators, who work closely with law enforcement agencies in this country and throughout the world to investigate and prosecute international networks of criminal counterfeiters. In the United States, Microsoft's investigative team has worked closely with federal and local law enforcement to bring about several important counterfeiting seizures, many of which involved organized crime:

- In February 2000, the FBI and LA Sheriff's Office led 12 raids against suspected criminal counterfeiters, resulting in the arrest of 12 individuals. Law enforcement officials seized several thousand counterfeit copies of Microsoft software, worth more than $5 million. The persons arrested were part of a well-organized international counterfeiting operation, with ties to Asian organized crime.
- In November 2001, the LA Sheriff's office, aided by U.S. Customs, the Secret Service and Microsoft investigators, executed one of the most significant raid and seizure of Microsoft software and components in U.S. history, with an estimated retail value of $100 million. The raid interrupted a major counterfeit software distribution pipeline that moved containers of counterfeit software and other illegal components from Taiwan through the Port of Los Angeles. Taiwanese authorities later confirmed that the counterfeiting operation was financed by Asian criminal groups.
- In April 2002, the FBI and several other federal and local law enforcement agencies dismantled a highly organized international counterfeiting ring, with assembly and distribution arms in Northern California, Washington and Oregon and direct ties to Asian criminal groups. The undercover investigation, known as "Operation Cyberstorm," led to the arrest of 28 individuals and the seizure of approximately $100 million in counterfeit software and components.

The counterfeiters were also involved in money laundering and credit card fraud.

These cases demonstrate the critical importance of close, multilateral cooperation between industry and law enforcement. For example, in the 2001 raid described above, Taiwanese authorities worked closely with US law enforcement and Microsoft to investigate and prosecute the Asian leaders of the operation. Unfortunately, few foreign law enforcement agencies share this commitment to anti-counterfeiting enforcement; and, as a result, the foreign criminals that finance and control worldwide counterfeiting operations are rarely prosecuted or punished.

In closing, we face a daunting challenge. How can we successfully fight a well-financed, global network of counterfeiting rings, when the criminals who control these operations bear little risk of prosecution and meaningful punishment outside the United States? Clearly, we cannot succeed, until all governments recognize that software counterfeiting is a serious crime that demands the same level of enforcement and cooperation that we bring to other global organized crime activities. We encourage federal law enforcement agencies to join together in sending a clear, unified, and unequivocal message to foreign authorities that software counterfeiting is a major crime priority that demands tough penalties, a sustained commitment of law enforcement resources, and multilateral cooperation among national authorities and industry.

Moreover, we urge the Subcommittee to support the Anticounterfeiting Amendments of 2003. This important legislation will help combat the growing threat of international counterfeiting crimes by ensuring that U.S. laws address all aspects of counterfeiting activities.

Thank you.

Attachment A

<u>Examples of Microsoft Anti-counterfeiting Features</u>

Certificate of Authenticity

CD-ROM Edge-to-Edge Hologram

Mr. SMITH. Thank you, Mr. LaMagna.
Mr. Simon?

STATEMENT OF EMERY SIMON, COUNSELOR, BUSINESS SOFTWARE ALLIANCE (BSA)

Mr. SIMON. Good morning, Mr. Chairman, Mr. Smith and Members of the Subcommittee. Thank you for the opportunity to appear before you today on a matter of great importance to the software industry, the widespread distribution and sale of counterfeit software to American consumer. I am Emery Simon and I appear today on behalf of the BSA.

Let me say at the outset clearly, BSA strongly support enactment of H.R. 3632 as introduced, and commends you, Mr. Chairman, for having introduced this bill. Its enactment will provide software companies with an important tool to combat piracy and counterfeiting by closing a deficiency in the law, namely, the illicit use of legitimate authentication means to mislead the public into thinking they are acquiring genuine software products when they are not. This practice hurts consumers as well as the reputation of BSA member companies. I think both of those are points worth emphasizing. The consumer thinks that he or she is getting a decent good product, when in fact they are not.

The bill addresses a specific and serious problem. By itself it will not stop piracy and counterfeiting, but it is an important step and it should be enacted promptly. The fact that it does not address all aspects of the piracy problem, for example, online piracy, which is not the goal of this bill, should not be an excuse for postponing its enactment.

BSA represent the world's leading developers of software, hardware and Internet technologies. For more than 15 years BSA member companies have worked to reduce piracy rates through a combination of education, enforcement and law reform. Today BSA's enforcement program extends to more than 65 countries around the world including the United States. Because computer software is a high-value good, it represents the greatest share of pirated American intellectual property on a dollar basis.

Congressional attention to the piracy problem has been invaluable in meeting the serious challenges faced by copyright owners in the past. Enactment of the Anti-counterfeiting Amendments of 2003 will help publishers of software and other copyrighted works assure their important contributions to the economy can continue.

I would like to provide the Subcommittee with a sense of the scope and severity of the software piracy and counterfeiting problem. Software industry growth, fueled by the ever-increasing demand for software has become a powerful economic force in the United States, contributing each year hundreds of thousands of skilled, high-paid jobs, tens of billions of dollars in tax revenue. Globally, four out of every ten, 40 percent, of the software programs are pirated. According to an economic study BSA recently commissioned, reducing the 40 percent rate by just 10 percent to 30 percent will result in dramatic good things, the creation of 1.5 million jobs, increased economic growth of about $400 billion we estimate, and additional tax receipts at the Federal, State and local level of $64 billion.

In recent years we've seen a dramatic increase in the amount of counterfeiting software imported into the United States from overseas, especially from Asia. Moreover, international counterfeiting rings, many of which have ties to organized crime, as you mentioned, Mr. Chairman, are significantly more sophisticated in their methods of producing look-alike software. Unlike the obvious fakes sold on street corners, counterfeit software is marketed as genuine product to unsuspecting consumers. To create the look of genuine packaged software counterfeiters attach the industry's state-of-the-art physical security features to counterfeit software and packaging to create near-perfect copies capable of deceiving even the most sophisticated American consumer. The genuine physical security features, for example, certificate of authenticity, enter the marketplace through theft primarily or fraud, and are sold to counterfeiters through a variety of middlemen.

BSA applauds the recent efforts by the Federal law enforcement agencies to devote more resources to fighting counterfeiting. The aggressive pursuit of international organized criminal counterfeiting rings is extremely important, but it's also important to pursue these at home, and this legislation will help greatly.

Thank you very much, Mr. Chairman.

[The prepared statement of Mr. Simon follows:]

PREPARED STATEMENT OF EMERY SIMON

Good morning. Chairman Smith and Members of the Subcommittee, thank you for the opportunity to appear before you today to testify on a matter of great concern to the software industry—the widespread distribution and sale of counterfeit software to American consumers. My name is Emery Simon and I appear before you today on behalf of the Business Software Alliance.[1]

BSA represents the world's leading developers of software, hardware, and Internet technologies. For more than fifteen years, BSA member companies have worked to reduce crippling piracy rates through a combination of education, enforcement and law reform. Today, BSA's enforcement program extends to more than 65 countries around the world, including the United States. Because computer software is a high-value good, it represents the greatest share of pirated American intellectual property on a dollar basis.

Congressional attention to the piracy problem has been invaluable in meeting the serious challenges faced by copyright owners in the past. Enactment of the Chairman's bill, the "Anti-counterfeiting Amendments of 2003," will help ensure that publishers of software and other copyrighted works can continue to make important contributions to the U.S. economy.

Today I would like to give the Subcommittee some statistics that provide a sense of the scope and severity of the software piracy and counterfeiting problem. Software industry growth, fueled by the ever-increasing demand for software, has become a powerful economic force in the United States, contributing each year hundreds of thousands of skilled, highly paid jobs and tens of billions of dollars in tax revenues. Globally, 4 out of 10 software programs—40%—are pirated. According to an economic impact study by IDC commissioned by BSA in 2003, reducing the 40% worldwide piracy rate by 10 percentage points to 30%, will result in the creation of an additional 1.5 million jobs, increased economic growth of $400 billion and an additional $64 billion in new taxes to help governments fund public programs like education, health care and law enforcement.

Software theft, including counterfeiting, causes severe economic harm, threatening creative industries while inhibiting the development of e-commerce. Losses due to software piracy and counterfeiting are on the rise, estimated at nearly $11 billion in 2001, and rising to $13 billion in 2002. The economic impact of software piracy extends far beyond the confines of the software industry, harming economies

[1] BSA members include Adobe, Apple, Autodesk, Avid, Bentley Systems, Borland, Cisco Systems, CNC Software/Mastercam, HP, IBM, Intel, Intuit, Internet Security Systems, Macromedia, Microsoft, Network Associates, PeopleSoft, RSA Security, SolidWorks, Sybase, Symantec and VERITAS Software.

worldwide in the form of greatly diminished tax revenues, a substantial number of lost jobs, and losses in education, infrastructure, and research and development.

In 1998 alone, software piracy cost the U.S. economy 109,000 jobs, $4.5 billion in wages and nearly $991 million in tax revenues. By 2008, those numbers will rise to 175,000 lost jobs, over $7 billion in lost wages and more than $1 billion in lost tax revenues. Better management of this problem could produce 1 million additional jobs and nearly $25 billion in additional government revenues worldwide by next year.

In recent years, we have seen a dramatic increase in the amount of counterfeit software imported into the U.S. from overseas, especially from Asia. Moreover, international counterfeiting rings, many of which have ties to organized crime groups, are significantly more sophisticated in their methods of producing "look alike" software and components. Unlike the obvious fakes sold on street corners, counterfeit software is marketed as genuine product to unsuspecting consumers. To create the look of genuine packaged software, counterfeiters attach the industry's state-of-the-art physical security features to counterfeit software and packaging to create near-perfect copies capable of deceiving even the most sophisticated American consumer. These genuine physical security features—for example, certificates of authenticity—enter the marketplace through theft or fraud and are sold to counterfeiters through a variety of middlemen.

Software counterfeiting is a most profitable crime. And yet the sale of physical security features to facilitate widespread counterfeiting is not a criminal offense.

BSA applauds the recent efforts by federal law enforcement agencies to devote more resources to fighting counterfeiting. The aggressive pursuit of international, organized criminal counterfeiting rings is extremely important to our members.

At the same time, U.S. anti-counterfeiting laws need to keep pace with the evolving nature of the software counterfeiting problem, so that our law enforcement agencies have the tools necessary to investigate and prosecute important links in the counterfeit supply chain. The Chairman's bill, the "Anti-counterfeiting Amendments of 2003" would provide law enforcement with an important weapon in the battle against counterfeiting in this country.

Mr. SMITH. Thank you, Mr. Simon.

Mr. Buckles.

STATEMENT OF BRAD BUCKLES, EXECUTIVE VICE PRESIDENT, ANTI-PIRACY, RECORDING INDUSTRY ASSOCIATION OF AMERICA, INC. (RIAA)

Mr. BUCKLES. Mr. Chairman, Members of the Subcommittee, on behalf of the Recording Industry Association of America, I want to thank you for inviting me to appear before the Subcommittee today on this important piece of legislation.

In my capacity as the head of the Anti-Piracy Unit at RIAA, I'm charged with leading the recording music industry's efforts to combat the distribution of illegal recorded music in U.S. commerce. The RIAA represents over 500 sound recording companies that are responsible for manufacturing over 90 percent of all of the legitimate sound recordings released every year in the United States.

Major and independent record companies release approximately 30,000 new albums in the United States and abroad each year. The artists who create the music are supported by a cast of thousands of people who work behind the scenes as producers, sound technicians, studio musicians, as well as artist development, marketing, promotion and distribution people. They are further supported by even more people who work in pressing plants, warehouses and record stores.

We therefore cannot afford to allow such an important component of our economy to fall prey to the ongoing piracy that we are currently seeing. The creative industries represented at this table collectively make an enormous contribution to the vitality of the

American economy, but collectively we also face an attack by piracy to a degree never before witnessed.

At the RIAA we've seen an exploding growth in piracy over the past 5 years, and we estimate that hundreds of millions of dollars are lost every year to music piracy in the domestic physical market alone. This number is increasing every year and does not include the estimated losses from piracy on the Internet through unauthorized peer-to-peer services.

As you recognized, Mr. Chairman, the extreme large profit margins and comparatively lesser likelihood of criminal prosecutions has not gone unnoticed by criminal enterprises. We commend the Subcommittee to being the first to investigate this problem last session with a hearing dedicated to the involvement of crime syndicate and terrorist groups with CD and DVD piracy, which provides quick and untraceable cash to carry out nefarious activities.

Some music piracy takes the form of rather undisguised pirated product. They use readily-available computer CD-burning technology, employ comparatively crude graphics in packaging, and make very little effort to appear authentic. Other forms of piracy, however, are far more insidious. They involve more sophisticated efforts to actually counterfeit the music CD product as a whole. This form of piracy employs a more expensive CD pressing technology, high-quality graphics and packaging, and make the final product appear to look like the real one. They can command a much higher price. If done well, they can pass for legitimate. In these cases, not only is the music industry harmed, but consumers are deceived into believing that they too are buying the real thing.

In an effort to combat the financial hemorrhaging being experienced, content owners have begun employing various authentication components to confirm the legitimacy of their products. These take the form of holograms or certificates of authenticity that help the consumer and law enforcement distinguish between legitimate and illegal products.

Unfortunately, these efforts are beginning to break down as criminals are becoming increasingly adept at finding ways to pirate these authentication components. Whether through the theft of legitimately created authentication components, or through the illegal manufacture of look-alike of authentication components, the illegal use of these materials is causing the sound recording industry harm in several ways. It undermines are ability to present—to use these authentication components as symbols of authenticity. They cause further damage to copyright and trademark owners whose intellectual property is affiliated with illegal product. And third, they defraud loyal music consumers who believe they are purchasing the real thing and supporting their favorite artists.

For these reasons the RIAA strongly supports the Anti-counterfeiting Amendments of 2003, and we believe that penalties against trafficking and genuine authentication components that will be used on pirated physical products is a good start in addressing the pirate product line that is affecting a large portion of American industries.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Buckles follows:]

PREPARED STATEMENT OF BRAD BUCKLES

Mr. Chairman, Members of the Subcommittee, on behalf of the Recording Industry Association of America ("RIAA"), I want to thank you for inviting me to appear before the Subcommittee on an important piece of legislation before you today. My name is Brad Buckles, and I am Executive Vice President for Anti-Piracy at the RIAA.

In my capacity of Director of the Anti-Piracy efforts of the recorded music industry, I oversee a professional staff of full-time employees that represent the "front lines" in our daily battle against piracy. We have ten field offices positioned throughout the country, staffed by a variety of full-time investigators, attorneys, analysts, and administrative support whose sole function is to investigate illegal recorded music distribution and stem the ever-increasing flow of piratical product into the stream of American commerce. Augmenting our full-time staff is a sizeable network of part-time "stringers" and paid informants who provide indispensable input into our investigative efforts.

Prior to joining the RIAA, I served as Director of the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") in the Department of Justice. My years with ATF exposed me to a variety of organized criminal elements undertaking sophisticated and well-orchestrated activities that endangered the American public and cheated U.S. citizens by ravaging the marketplace. In my new capacity with private industry, I can confidently say that the threats facing the U.S. creative community—while somewhat different in nature than those that I witnessed at ATF—are equally threatening to the bedrock of our American institutions, our American culture, and our American economy.

THE VALUE OF MUSIC IN AMERICA

The RIAA represents over 500 sound recording companies that are responsible for manufacturing over 90% of all legitimate sound recordings released every year in the United States. According to some independent estimates, major and independent record companies release approximately 30,000 new albums in the U.S. and abroad every year. Together these companies and hundreds of others like them strive to bring new exciting music to the American consumers and benefit the American economy. While many people think of famous artists when they think of the music industry, most artists barely make a living by selling moderate numbers of albums combined with other sources of income. Artists are supported by a cast of thousands of people who work behind the scenes as producers, sound technicians, and studio musicians, as well as artist development, marketing, promotion and distribution people. They are supported by people who work at the pressing plants, the warehouses, and the record stores. The intellectual property industries in this country (including the movie industry and the software industry represented here today) represent the largest segment of the American economy—at approximately 5% of the gross domestic product. In recent years, it has represented the sector of the economy growing at the fastest rate, and providing the greatest percentage increase in well-paying jobs. The creative industries demonstrate one area where American exports are booming, and in many countries epitomizes their experience of what it means to "be American."

We therefore cannot afford to allow such an important component of our economy fall prey to the ongoing piracy we are currently seeing.

THE PIRACY PROBLEM IN AMERICA

The creative industries, although a substantial contributor to the vitality of the American economy, are currently under attack by piracy to a degree not witnessed previously. Through the advent of digital technology, individuals can now carry out perfect duplication on a mass scale previously reserved to sophisticated manufacturing operations that required the investment of millions of dollars. In recent years, the technology surrounding computers and CD burning, combined with the plummeting cost of the related raw materials (such as blank CD-Rs), has created an environment where substantial CD counterfeiting operations can be funded for under $10,000. And the same digital technology allows for perfect serial copying on a large scale without the degradation of quality that used to accompany analog piracy. In other words, a would-be pirate can create dozens of secondary copies from a single source, and each of these derivative copies can in turn create hundreds or thousands of derivative copies, and so on—with each copy being as clear as the original.

The exploding nature of piracy can be witnessed in the steady increase in seizures that the RIAA has witnessed over the past five years. Approximately 2.5 million

counterfeit or pirate CD-Rs were seized in the first six months of 2003. This number is up 18.1 percent from almost 2.1 million seizures at mid-year 2002. The seizure of CD-R burning equipment during 2003 has demonstrated a similar trend. Likewise, it has been reported that two years ago the annual sales of blank recording media (CD-Rs, etc.) outpaced the sale of legitimate pre-recorded music for the first time. The RIAA estimates that hundreds of millions of dollars are lost every year to domestic sound recording piracy in the physical market alone. This number is increasing every year, and does not include the estimated losses from piracy on the Internet through unauthorized peer-to-peer services.

The ease with which illegal copying can be accomplished, combined with the low entry costs, the extremely large profit margin, and the comparatively lesser likelihood of criminal prosecution has not gone unnoticed by sophisticated criminal enterprises. We are witnessing increasing evidence of ties between physical piracy operations and sophisticated syndicates, including organized crime and international money-laundering rings. Piracy activity is often connected to other illicit activity as well, such as illegal immigration, tax evasion, and fraud. We commend the Subcommittee for being the first to investigate this problem last session with a hearing dedicated to the involvement of crime syndicates and terrorist groups with CD and DVD piracy which provides quick untraceable cash to carry out nefarious activities.

H.R. 3632—A GOOD BEGINNING

In an effort to combat the financial hemorrhaging being experienced by the content owners, many have begun employing various authentication components to confirm the legitimacy of their products to consumers. These components may take the form of holograms or certificates of authenticity, and they help consumers and law enforcement agencies distinguish legitimate product from illegal product. Because it is much more difficult to manufacture these authentication components (especially as compared to manufacturing pirate CDs), they are more difficult for the criminals to pirate, and until recently the presence of such components was a fairly reliable indicator that the affiliated product was legitimate, or that the lack of such an authentication component was an indicator of piracy.

Unfortunately, the criminals are becoming increasingly adept at finding ways to pirate these authentication components, thereby increasing both the attractiveness of their piratical product and the difficulty in detecting fakes. Whether through the theft of legitimately created authentication components, or through the illicit manufacture of look-alike authentication components, the illegal use of such materials is causing the sound recording industry harm in several additional ways. First, their use further complicates the enforcement efforts of the RIAA and its sister organizations worldwide because we can no longer rely on the presence of these authentication components as a true symbol of "authenticity." Second, they cause further damage to copyright or trademark owners whose intellectual property is affiliated with substandard and illegal products and the fake authentication components. Third, theyH.H. provide an incentive for another level of deception and law-breaking as pirates are forced to either mimic these components or obtain them through illegal means in order to affix them to counterfeit product.

For these reasons, the RIAA strongly supports the Anticounterfeiting Amendments Act of 2003. We believe increased penalties against the illicit use of such authentication components on physical products is a good start towards thwarting another step in the "pirate production line" that is affecting a large portion of American industries.

While physical holograms and certificates of authentication are attached to physical products, digital authentication components will obviously need to be attached to digital music products, and the use of such advanced authentication components may well be the key to effective law enforcement in the growing digital music marketplace. Thus, the concepts and principles contained in this bill can be extended, and should be extended, to the digital arena. Certainly, we believe that the illegal use and duplication of digital authentication components are an issue of great concern and ought to be addressed.

However, we also realize that the application of these anticounterfeiting amendments to non-physical product is a more complex undertaking than these amendments which relate solely to physical product. The interplay with other statutes governing digital piracy and digital copyright laws create challenging issues of statutory drafting. In recognition of the importance of making progress on the physical piracy problem as soon as possible, we support the amendments in their current form at this time. We strongly urge the Subcommittee, however, to turn to the issue of digital authentication components in the near future, so that the benefits of digital authentication technology can be fully realized.

ATF NEWS

Bureau of Alcohol, Tobacco, Firearms and Explosives

For Immediate Release FY-03-17

Contact: Joseph G. Green (202) 927-8500 December 9, 2003

Director Buckles Ends Tenure At ATF

Retiring After 30-Year Career

WASHINGTON--Bradley A. Buckles, Director of the U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) will retire from his post effective Jan. 3, 2004, after 30 years of service.

Mr. Buckles will be entering the private sector, which he anticipates will be challenging and rewarding. Mr. Buckles joined ATF in 1974 and rose through the ranks to become Deputy Chief Counsel and in 1996 was appointed Deputy Director. In December 1999, Mr. Buckles was named the fifth Director in ATF's history.

This past January Mr. Buckles was tasked with providing guidance and oversight of ATF's transfer from the U.S. Department of Treasury to the Department of Justice, and the overall responsibility of supervising nearly 4,800 Federal employees. "I am extremely proud to have served many years in the U.S. Department of the Treasury and now as a result of the Homeland Security Act, the Justice Department. Now that ATF is successfully integrated into the Justice family my job is complete," said Buckles. "I have decided that it is the best time for me to move on."

"As a dedicated professional at the Bureau of Alcohol, Tobacco, Firearms and Explosives for nearly 30 years, Bradley A. Buckles has served with integrity and skill. His steadfast leadership of the Bureau's 4,800 employees helped ensure a seamless transfer of the ATF from the Treasury Department to the Justice Department this year. I am grateful for his service and wish him every success in his future endeavors," said Attorney General John Ashcroft.

Mr. Buckles stated that although he is sad to be leaving so many close friends, he is looking forward to meeting his new challenges in addition to spending more time with his family.

###

For Release: December 9, 2003

Contacts: Amy Weiss
Jonathan Lamy
Amanda Collins
202-775-0101

RIAA Taps ATF Chief To Lead Anti-Piracy Unit

WASHINGTON -- The Recording Industry Association of America (RIAA) announced today that it has hired Bradley Buckles, the director of the federal Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), to head its Anti-Piracy Unit.

As Director of ATF for the past four years, Buckles oversaw a prominent agency with a staff of more than 4,800 employees and an $800 million budget. Before becoming the Director in 1999, Buckles served in two different senior leadership posts at the ATF, first as Chief Counsel from 1974 - 1995, then as Deputy Director from 1996 - 1999.

"Brad offers impeccable credentials, the acclaim of his colleagues, and a long and successful career at the upper echelons of law enforcement," said Mitch Bainwol, Chairman and CEO of the RIAA. "He is the perfect match for the RIAA and will be an extraordinary asset to our anti-piracy efforts."

Attorney General John Ashcroft said that, "As a dedicated professional at the Bureau of Alcohol, Tobacco, Firearms and Explosives for nearly 30 years, Bradley A. Buckles has served with integrity and skill. His steadfast leadership of the Bureau's 4,800 employees helped ensure a seamless transfer of the ATF from the Treasury Department to the Justice Department this year. I am grateful for his service and wish him every success in his future endeavors."

At the RIAA, Buckles will lead the organization's Anti-Piracy Unit, which includes investigators in Washington and throughout the country who work with various law enforcement agencies to combat piracy. The technological capability to copy massive numbers of counterfeit CDs with computer burners is transforming music piracy into an increasingly easy, cheap and convenient enterprise.

"Brad's appointment should signal to everyone that we continue to take piracy, here and throughout the world, very seriously," Bainwol added. "Piracy is becoming an increasingly sophisticated, and lucrative criminal venture."

While at the ATF, Buckles served on the Executive Committee of the International Association of Chiefs of Police, the National Policy Board of the Gang Resistance Education and Training Program, and the Board of the National Center for Missing and Exploited Children. Before joining the ATF, Buckles earned his Bachelor's Degree from the University of Wyoming and his law degree from Washburn University.

# # # # #

[The Recording Industry Association of America is the trade group that represents the U.S. recording industry. Its mission is to foster a business and legal climate that supports and promotes our members' creative and financial vitality. Its members are the record companies that comprise the most vibrant national music industry in the world. RIAA® members create, manufacture and/or distribute approximately 90% of all legitimate sound recordings produced and sold in the United States.

In support of this mission, the RIAA works to protect intellectual property rights worldwide and the First Amendment rights of artists; conduct consumer industry and technical research; and monitor and review -- state and federal laws, regulations and policies. The RIAA® also certifies Gold®, Platinum®, Multi-Platinum™, and Diamond sales awards, Los Premios De Oro y Platino™, an award celebrating Latin music sales.]

Mr. SMITH. Thank you, Mr. Buckles.
Mr. Green.

STATEMENT OF DAVID GREEN, VICE PRESIDENT AND COUNSEL, TECHNOLOGY AND NEW MEDIA, MOTION PICTURE ASSOCIATION OF AMERICA (MPAA)

Mr. GREEN. Chairman Smith, Mr. Berman, Ms. Hart, thank you for this opportunity to testify on behalf of the Motion Picture Association of America about this very important anticounterfeiting bill. Over the last 12 months this Subcommittee has held a number of hearings, and its Members have introduced several bills that address the rampant physical and digital piracy of America's intellectual property. We're grateful that this vital economic issue has commanded the Subcommittee's attention.

We are here today to testify in support of H.R. 3632, the "Anticounterfeiting Amendments of 2003." The bill would approve 18 U.S.C. 2318, the Federal Criminal Law prohibiting trafficking in counterfeit labels, by expanding the definition of "counterfeit" to include genuine labeling components that are used in an unauthorized manner. In addition, the bill provides a civil remedy to enable victims of counterfeiting to enforce their own rights, an important supplement to the Federal prosecutorial resources that can realistically be expected to be devoted to this problem.

To make an already valuable bill even better, we ask the Subcommittee to ensure that the prohibition on trafficking and counterfeit labels clearly applies to all authentication features, whether physical or digital, used to determine whether a particular good is counterfeit or genuine. Under this bill, those who traffic in genuine but illicitly used labeling components can no longer escape prosecution. We must be clear that the same behavior in the digital world merits the same consequences.

Let me tell you why this matters. With new technologies proliferating we envision a near-term future where a consumer with a few clicks of the mouse will be able to have any movie ever made delivered digitally right to his or her own computer or television set. But this exciting digital future is threatened by piracy. We and our partners in the information technology, sound recording and consumer electronics industry, are doing our part to combat piracy by devising ways to protect content from being illegally distributed online, but we need the enforcement laws to keep pace with technology.

Microsoft has eloquently testified how their genuine certificates of authentication, created to make life more difficult for pirates, have been stolen and sold to counterfeiters. As we develop similar digital authentication features, we can expect these features to be counterfeited and stolen as well. People can go to jail for up to 5 years for trafficking in holograms or certificates of authentication. This bill should make clear that they do not get off scot free when trafficking in the digital equivalent.

We look forward to working with the Subcommittee and other interested parties to find clarifying language to ensure that the laudable goals of this legislation are fully realized.

I do want to be very clear that the MPAA supports this legislation and wants to see it enacted. I also stress that be advocating

that this statute by forward looking, we are in no way attempting to open a back door for some sort of digital rights management technical mandate or anything like that. This is a law enforcement statute pure and simple. Our goal is the same as that of our friends in the software community, to make sure that our prosecutors' tools are adequate to fight those show are offering counterfeit versions of our products now and in the future.

Thank you, and I look forward to answering any questions you may have.

[The prepared statement of Mr. Green follows:]

PREPARED STATEMENT OF DAVID GREEN

INTRODUCTION

On behalf of Jack Valenti and the seven companies that comprise the Motion Picture Association of America,[1] I very much appreciate this opportunity to testify today on H.R. 3632, the Anti-counterfeiting Amendments of 2003. The movie industry contributes significantly to America's culture and its economy. The livelihoods of nearly one million men and women in America are impacted by the film industry, which entertains millions of consumers every day.

Our ability to continue making these types of contributions, however, is being undermined by wide-scale piracy. World-wide, piracy costs the film industry $3.5 billion annually in hard goods piracy alone. The losses associated with the intensifying problem of Internet piracy are difficult to quantify, but it has been estimated that 400,000 to 600,000 movies are uploaded or downloaded every day on "file-stealing" networks like KaZaA and Gnutella.

We commend the Chairman and this Subcommittee for this hearing and legislation aimed at the piracy problem, and the many other hearings held and bills introduced on this issue over the last twelve months. Movie piracy's victims include not only the movie studios, but also all the actors and behind-the-scenes employees associated with the making of the film. The consumer, whose entertainment choices are narrowed as the legitimate return on investments is stolen, is an additional victim, as is the citizen, whose governments cannot collect the tax revenues associated with the sale of legitimate goods.

H.R. 3632

MPAA supports H.R. 3632. The bill will help protect consumers and producers of intellectual property, the victims of piracy, in two respects.

First, the bill properly expands the definition of "counterfeit label" from merely "an identifying label or container that appears to be genuine, but is not," to genuine labeling components that are illicitly distributed. This expansion is an appropriate response to the growth of trade in and theft of genuine "authentication devices" used to make the counterfeited goods appear legitimate. The new definition will make it easier for federal prosecutors to charge people who may not themselves be distributing the final counterfeit product, but are assisting in the illicit production of those products.

Second, the bill adds a civil remedy for a violation of 18 U.S.C. § 2318. We recognize the reality that federal investigators and prosecutors are pressed with a wide range of important responsibilities, and sometimes will be unable to respond in a timely manner to even serious instances of trafficking in counterfeit labels. In these circumstances, it is important for rightsholders to be able to protect themselves by seeking injunctive relief and damages.

THE IMPORTANCE OF THE DIGITAL FUTURE

H.R. 3632 is a good bill, and we hope to work with the Subcommittee and the stakeholders to make it even better. We are concerned, however, that this bill does not explicitly state that an authentication device can be digital, as well as physical. While we do not read the current language as covering just the physical, we are concerned that the courts could interpret the coverage of section 2318 in such a lim-

[1] Buena Vista Pictures Distribution, Inc. (The Walt Disney Company); Metro-Goldwyn-Mayer Studios Inc.; Paramount Pictures Corporation; Sony Pictures Entertainment Inc.; Twentieth Century Fox Film Corporation; Universal City Studios LLLP; and Warner Bros., a division of Time Warner Entertainment Company, L.P.

ited fashion. The Supreme Court's ruling in *Dowling* v. *United States*, 473 U.S. 207 (1985) (holding that the interstate transportation of stolen property statute did not cover intangible goods such as intellectual property), stands as a reminder that a failure of Congress to be clear as to the scope of coverage may lead the courts, employing the rule of lenity, to interpret a statute too narrowly.

Section 2318 should not be limited to the physical labels; rather, it should be broad enough to encompass the authentication devices of the digital age. Digital distribution, and digital piracy, are upon us, and will loom much larger in the near future. It has become a cliché to note how much the advent of digital communications has revolutionized how we work, how we gather information, and how we are entertained. Yet we at MPAA firmly believe that we are still in the opening moments of the digital age, and that the wonders still to come will make the novel technologies of today seem pale in significance.

MPAA and its member companies are devoting enormous amounts of time and money toward figuring out how to use modern communications tools to deliver movies—in a consumer-friendly manner—right to people's homes. Even today, despite the still-relatively modest numbers of homes that have broadband Internet connections, new services such as MovieLink and CinemaNow are enabling consumers to download movies to their hard drives to watch at a later time. Video-on-demand systems allow consumers to select from a range of modestly-price movies to watch in their living rooms. But this is only the beginning.

The Internet is speeding up. Cal Tech recently reported one experiment called "FAST," which can download a quality DVD movie in *five seconds*. Another experiment, "Internet-2," has dispatched 6.7 gigabytes—well more than a typical DVD movie—halfway around the world in *one minute*. As the experiments of today reach the marketplace of tomorrow, we envision a near-term future where digital delivery grows into a full-fledged partner to the sale of physical DVDs. Ours is a future when any consumer can obtain, with a few clicks of a mouse, any movie ever made, with choices offered as to whether to watch the movie once, or keep it forever as part of a video library.

Of course, legitimate and profound concerns about rampant Internet piracy form a dark cloud obscuring this bright digital future. We are hard at work with our counterparts in the information technology, sound recording and consumer electronics industries to devise ways to protect content from being illicitly distributed online, while providing flexible models for a range of consumer uses. We are confident that, working together, we can reach a solution that allows the legal electronic distribution of movies and other valuable content to flourish.

Even as we strive to bring about this bounty for consumers, we must be aware that the pirates and counterfeiters will try mightily to undo all the good we are trying to achieve. For the physical distribution of its products, some software companies developed hard-to-copy "certificates of authenticity" to stymie counterfeiters, then found their program hijacked by pirates who were buying or stealing these certificates to make their counterfeit goods appear authentic. For the digital distribution of products—such as software, games, music or movies—digital counterparts of these "certificates of authenticity" will be devised to discern whether a work is counterfeit or infringing of any copyright. As soon as we develop these tools, digital outlaws will find a way to traffic in them, facilitating the ability of counterfeiters to defraud consumers into believing that the illegally copied goods they are peddling are legitimate.

We must make sure that the prosecutors of tomorrow have adequate legal weapons at their disposal to attack piracy with the same zeal, whether it occurs in the physical world or online. It makes little sense to have a provision which allows someone to be sent to jail for up to five years for trafficking in counterfeit *physical* labels, while someone who does the same thing digitally gets off scot-free. Rather, the legislation should be technology-neutral, focusing on the function and effect of the counterfeit label being trafficked in, and applied equally whether the counterfeit label being trafficked in takes a digital or a physical form. We would be happy to work on language with the Subcommittee and with others concerned, to ensure the courts will interpret this provision appropriately.

THE "LICENSING" DOCUMENT CLAUSE SHOULD NOT BE LIMITED TO COMPUTER PROGRAMS

In most aspects of this statute, all copyrighted works, whether they are movies, music, or computer programs, are treated the same. In one section, however, a "licensing document" comes within the definition of "counterfeit label" if it is used in connection with a computer program, but not a phonorecord, a copy of a motion pic-

ture, or other work. We think this disparate treatment is unwarranted, and ask the definition be extended to all types of works protected under the statute.

Specifically, Section 2 of H.R. 3632 defines counterfeit labels as, among other things, "a genuine . . . licensing document . . .

> (i) that is used by the copyright owner to verify that a phonorecord, a copy of a computer program, a copy of a motion picture or other audiovisual work, or documentation or packaging is not counterfeit or infringing of any copyright; and
>
> (ii) that is, without the authorization of the copyright owner-
>
> . . .
>
> (II) **in the case of a computer program, altered or removed to falsify the number of authorized copies or users, type of authorized user, or edition or version of the computer program**."

(Emphasis added.)

MPAA agrees with this definition, but not with its limitation to computer programs. Rather, as "Digital Rights Management" (or DRM) comes to the fore, movies, entertainment software and music, as well as computer programs, will increasingly use "licensing" documentation, both physical and digital, to establish the number of authorized copies or users, type of authorized user, or edition or version of the work. Anyone who "traffics" in false licensing information should be covered by the statute, regardless of type of work, and regardless of whether it is physical or digital.

CONCLUSION

We support H.R. 3632 and commend the Chairman and Representatives Keller, Wexler, Goodlatte, Gallegly, and Carter for its introduction. We look forward to working with you on the changes and clarifications discussed above that would make section 2318 a more useful statute for the future. I look forward to answering any questions that you may have.

Mr. SMITH. Thank you, Mr. Green, and thank you all for your testimony, which is, I'm glad to say, uniformly supportive of the legislation, and we will move forward with that.

Mr. Green has made a couple of suggestions which I want to ask our other witnesses about, but before I do, I want to ask sort of a general question. A criticism of this type of legislation a couple of years ago was that it was somehow going to impede the ability of Americans to buy discount items or goods. I just wanted to see if there was any witness today who actually thought that that would be a result of this legislation?

Mr. LAMAGNA. Mr. Chairman, if I might address that?

Mr. SMITH. Yes, Mr. LaMagna.

Mr. LAMAGNA. This will in no way impact upon the consumer's ability to do that. What this law would do, it would be to prevent people from actually deceiving consumers, and will deprive them of the ability to authenticate counterfeit and bad products by using a genuine certificate of authenticity. This will not interfere with the——

Mr. SMITH. That is exactly the point and the goal of the legislation, and I just want to make sure there wasn't any misunderstanding in that regard.

Let me ask everyone——

Mr. SIMON. Mr. Chairman, if I might, just a small point?

Mr. SMITH. Yes, Mr. Simon.

Mr. SIMON. The software industry used to price its products differently in different markets. With the advent of the Internet and the fact that you can now buy a lot of products and download them, the vast majority of software is now priced pretty much the same price regardless of the market. So the incentives for grade-market

goods, which was buying in a low-price market and exporting it to a high-price market, at least for software, have substantially——

Mr. SMITH. There's not much of a gray market out there then.

Mr. LAMAGNA. That is correct, sir.

Mr. SMITH. Okay, thank you, Mr. Simon.

Let me address my next question to everyone other than Mr. Green, because it plays off a couple of suggestions that Mr. Green has made, and then, Mr. Green, I'll ask you to respond as well.

The first suggestion Mr. Green made for a change in the legislation is to expand the bill to cover digital works. Mr. LaMagna, we'll start with you and work down the panel. What is your response to that suggestion?

Mr. LAMAGNA. Mr. Chairman, we share concerns of our colleagues of the motion picture industry, and we fully recognize that this is an issue which must be addressed. With the digital age upon us, we must address some of these issues. However, we feel this is a very complex issue that is something that should be addressed in different fora. We are participating in those fora with other industries, but this particular bill addresses a very narrow problem in which Microsoft is losing money to the tune of millions of dollars, and it really addresses the physical product and is of a different nature entirely.

Mr. SMITH. Thank you, Mr. LaMagna.

Mr. Simon?

Mr. SIMON. Three or four thoughts, Mr. Chairman. First of all, this bill is about authentic, legitimate, kosher, authentication products. It's not about bogus ones or counterfeit ones. The notion that it should be extended to digital, we already use authentication features on digital products. Software is digital.

So maybe what we are thinking about—I think what Mr. Green was thinking about was downloaded software or downloaded movies or downloaded music. So it's really a method of distribution issue rather than whether a product is in digital form or not. So thinking about it in that online worlds, it's hard for me to conceive how one would apply a label like that to a downloaded movie or a downloaded piece of software.

What we do and what a lot of software companies do, a lot of other companies do as well, is we use digital rights management technologies, encryption, access keys, a variety of other things. When those things are hijacked, when those things are hacked, there's already existing law that covers those problems. Sections 1201 and 1202 of the Copyright Act cover those, 1202 in particular. So those are actionable. There is no loophole with respect to those kinds of things.

Now, finally, somehow the forward leaning notion here, anticipating that someday something may develop, I fully recognize that the future is full of hope, but it's unclear. We do have a concrete problem before us, which is this kind of loophole in the law. It's worth fixing. We are only working on the longer-term issues, and I don't think those are issues of authentication features. Those are questions of technological protection measures.

Mr. SMITH. Okay. Mr. Simon, thank you.

Mr. Buckles?

Mr. BUCKLES. As my colleagues have said, I think we all agree that the issues and challenges that we will face in the world of downloading, whether it's music, software of movies, is the same, and I think we all share Mr. Green's concerns about that. I think the disagreement that we might have, or the questions that we would pose, are really ones of process rather than substance. This bill was designed to deal with something very specific that has to do with counterfeiting in the physical world. It's a real and pressing problem that we are all facing. Our concern would be in trying to deal with that real and pressing problem, that it get bogged down in what are really much more complex issues that would develop in trying to solve problems about how the future might work with authentication devices in a digital download world.

Mr. SMITH. Thank you, MR. Buckles.

Mr. Green, I'd still like to hear your response if you'd be brief.

Mr. GREEN. Certainly. As the Chair knows and everybody knows, congressional action takes some time, and we are looking at a world of digital distribution which is not a far-off fantasy, but a near-term reality. As the distribution takes off, there are going to be authentication features just like we've talked about today. Some of them we can imagine, some of them that we can't, but ways that consumers can use and copyright owners can use to know that the product is legitimate and not counterfeit.

As soon as we devise these, there's going to be some pirate out there who are going to be selling them, just like the certificates of authentication in the physical world. So rather than—we have to be able to anticipate that that's going to happen and make clear that our law is technology neutral, and would ban the same conduct whether it takes place in the digital or the physical realm.

Mr. SMITH. Fair enough. Thank you, Mr. Green, and appreciate your answers in regard to that question.

And Mr. Berman is recognized for his questions.

Mr. BERMAN. How do we know there are only two realms? [Laughter.]

Mr. GREEN. There may be others.

Mr. BERMAN. Maybe we should cover them as well.

After making a statement sort of supporting the bill, raising the question of why it shouldn't go forward, the devil in me made me read the bill. Why couldn't someone say, What are you doing? I bought this product, including its authentication feature. I've got a right to do anything I want with this product. I own it now. And if I want to take off the authentication feature and sell it to a collector of authentication features or a collage maker, or anybody else? You're pressing a bill that isn't about my intention to have it affixed to a counterfeit product or anything else. You're just restricting my freedom to do something with a component of a product that I own and I purchased and I paid for, and this is the Government really getting into interference with sort of fundamental rights of people to do with their possession what they want to do.

What's your answer to that argument?

Mr. LAMAGNA. Mr. Berman, if I may address that?

Mr. BERMAN. Am I reading the bill wrong? The way I read it, there is no requirement of proof of—is there something in the word

"trafficking" that isn't clear from the bill that includes an intention that I don't read in this bill now?

Mr. LAMAGNA. Well, sir, I think the word "trafficking" implies large-scale sale and distribution. We are clearly not interested in people selling one or two or even five copies for collectors' items or trade, et cetera. What we are seeing, particularly over the Internet, are people who are offering 100, 500.

Mr. BERMAN. I have no doubt about what you're going after, but your bill, on its face, looks like it affects the sale of one or two for collectors.

Mr. LAMAGNA. I really don't think that it's going to be applied in that manner.

Mr. SIMON. Mr. Berman, this bill amends existing law which has embedded in its requirements of knowingly doing these activities for bad purposes.

Mr. BERMAN. It does?

Mr. SIMON. Yes. It's a criminal statute which——

Mr. BERMAN. Well, no——

Mr. SIMON. You're——

Mr. BERMAN. That's the conclusion. Just tell me why it does that.

Mr. SIMON. Well, it is amending a provision of existing law which prohibits the trafficking in unauthentic, counterfeit, forged authentication devices for illicit purposes. And what we're adding simply to it is making it illegal to traffic in legitimate ones as well, again, for the illicit purposes, for deceiving the public, for selling pirated material. But if you're not comfortable with it——

Mr. BERMAN. I'm actually pretty comfortable with it. It was the devil in me. [Laughter.]

I just wondered if Rick Boucher were here, what would he say? [Laughter.]

What about the response of Mr. Green to that—I mean I don't know what fora you're working on this on, but what's wrong with writing this in a technology-neutral way, even if—by the way, the argument that no one has yet figured out how to do something that involves authentication of digital but we're working on that, also means that there's no one trafficking in it who will be trying to keep it. So in other words, are you really adding serious controversy to it by including the digital transmissions with the one—the least conceivable exception I could have is the old ISP liability issue, which can sometimes rear its ugly head, but there are ways to try and deal with that as well. I don't think Mr. Green is out there trying to get a sort of a conduit ISP involved criminally in this statute, I think, who isn't affirmatively marketing or profiting from the trafficking in what could become a digital authentication feature.

Mr. SIMON. If I may respond, Mr. Berman, I think it is relevant that nobody is now using these things. Software companies have examined trying to apply these kinds of features to software products, and we haven't found any that really work very well. So we use DRMs, we use technological protection measures.

The issue why Mr. Green's kind of forward-leaning attitude in this situation I think would be a little bit of a mistake, is because it would create, as you say, some overlap with 512, the ISP liability provisions, some overlap with the anti-circumvention provisions.

Those would be very complicated, frankly, to figure out, and what we would end up doing is spending a lot of time spinning our wheels while this problem persists. So our strong suggestion is: fix this problem. Don't ignore the other one, but fix this problem and we'll continue to work on the——

Mr. BERMAN. What does this have to do with anti-circumvention? This is not an effort to render criminal—I mean this is a bill designed to render criminal the trafficking in authentication documents, not—we already have a DMCA that deals with the issue of circumvention. How does this raise an anti-circumvention? Just elaborate on that a little bit.

Mr. SIMON. There are two provisions of chapter 12, and I—with the Chairman's indulgence.

The anti-circumvention provision is used to control access, and the question is whether an access control feature can also act as an authentication feature. And the answer is, yes, it can, and then you get confusion. Section 512 talks about digital rights management issues, which are a lot of these same issues that arise here, and again, you have overlap. Is it a 512 covered issue—sorry—a 1202 covered issue, or is it an issue covered under this criminal provision? So there's overlap that needs to be worked out, and that's where the complexity arises.

Mr. SMITH. Thank you, Mr. Berman.

The gentlewoman from Pennsylvania, Ms. Hart, whose presence we appreciate, is recognized for her questions.

Ms. HART. Thank you, Mr. Chairman.

I want to thank the gentlemen for their testimony today as well.

I want to direct a question to Mr. LaMagna and Mr. Simon, concerning about what actually, you know, apart from what we're discussing today or maybe including what we're discussing today, what are the biggest challenges that your companies are dealing with when you're combating actual, direct software counterfeiting? Would you rank this as the top issue or one of the top issues? Are there other issues that you would place as basically the biggest challenges when you're trying to combat that counterfeiting?

Mr. LAMAGNA. Ms. Hart, if I may address that. Counterfeiting is definitely one of our biggest problems at Microsoft, and the protection of our intellectual property. And among those, one of the biggest challenges is really public attitudes toward this type of activity. Many people view this as a victimless crime. In simplistic ways of thinking, you know, Microsoft is a very well-known, big, wealthy company, Bill Gates is very wealthy. People make the connection, well, you know, I'm not harming anyone. I'm just causing a few dollars loss to Bill Gates and Microsoft.

The only challenges that we face are worldwide challenges in terms of getting other countries to adopt the same laws and the same enforcement and the same political will to protect intellectual property that we have.

As I think you know, and has been stated, this is an international problem. It does not stop at the borders, and it's very, very difficult to go after these large organized crime enterprises if we do not have worldwide cooperation.

So those are some of the biggest challenges, and certainly this law would go a long way toward addressing some of those problems.

Ms. HART. Thank you.

Mr. Simon, the same?

Mr. SIMON. For the software industry generally, on the counterfeiting problem, this is probably the biggest counterfeiting problem. So it's the misleading the consumer by using what are authentic features to really sell stolen product, pirated product.

Ms. HART. So that the issues that were cited by Mr. LaMagna, those also?

Mr. SIMON. For the general software industry, that is true, yes.

Ms. HART. No other ones that——

Mr. SIMON. We have lots of different piracy issues. We're trying to separate these——

Ms. HART. Piracy from counterfeiting, sure.

Mr. SIMON. Right, where people are simply stealing the software, downloading it, distributing it, or making more copies than they're allowed to make or a variety of other things, we tend to separate these into counterfeiting issues and piracy issues.

Ms. HART. Is there something that you are doing yourselves to try to inform your legitimate customers that they may be victims of a fake product?

Mr. LAMAGNA. Oh, absolutely, Ms. Hart. We have websites. We have a piracy website for Microsoft. We have "how to tell" website to actually walk people through the identification of features to see if they have a genuine product. We have other public information campaigns. We of course work very closely with law enforcement to put out information, and to train them as well in the awareness and enforcement of intellectual property and piracy. So we do have a number of efforts under way to better advise people and make them informed consumers, yes.

Ms. HART. Thank you. I yield back, Mr. Chairman.

Mr. SMITH. Thank you, Ms. Hart. Actually, if you yield to me, I've got one more question.

Ms. HART. I will yield to you my remaining time, Mr. Chairman.

Mr. SMITH. Thank you, Ms. Hart.

Let me ask one more question, and again, I'm going to key off of a suggestion that Mr. Green made in his testimony and ask the other witnesses to respond, and Mr. Green to respond after they have given their answer as well.

This goes to the suggestion Mr. Green made that we change the bill. He says that if the phrase "licensing document" comes within the definition of "counterfeit label" if it is used in connection with a computer program but not a phono record, a copy of a motion picture or other work. We ask that the definition be extended to all types of works protected under the statute.

What do you think of that idea, Mr. LaMagna? Was that clear enough for you or not?

Mr. LAMAGNA. Yes. It was clear, Mr. Chairman, but again, I would go back to our theory, which is this is a very narrowly crafted bill that would address a very specific problem, which is a huge problem for us as I think we've already emphasized. I would be

concerned that any alteration of that would in some way make this a less effective bill.

Mr. SMITH. Okay. Thank you.

Mr. Simon?

Mr. SIMON. I was just looking at the language, Mr. Chairman, of the bill. It is the practice of the software industry to do site licensing. So we'll give a copy to the Committee, and the contract, the license will say that the Committee can make, 30, 40, 50 copies of it. The issue here is when somebody tries to take that contract, alter it, and instead of 30 copies, having 300 copies. So that's a specific issue that, as I understand it, this provision is trying to address. I am not aware of any similar current practice in the motion picture industry, so for me it kind of falls into the same category as Mr. Green's other suggestion, which is it's a practice the industry may engage in in the future, but let's get this thing done now, and if that proves to be a problem, it's always your prerogative to come back to it.

Mr. SMITH. Mr. Simon, thank you.

Mr. Buckles?

Mr. BUCKLES. On this issue I think I would have a tendency to agree with Mr. Green. I think this is still dealing with the physical world. While my colleagues are correct that we do not normally use site licenses in the same way that the software industry does today, I don't think we want to preclude that from being part of the way in which we might be operating in the future. This is still dealing with physical components. I don't think using that same terminology for all three of our businesses in any way would complicate or really expand the nature and scope of this bill.

Mr. SMITH. Thank you, Mr. Buckles.

Mr. Green, you're picking up a little support here.

Mr. GREEN. I continue to agree with myself on this one. [Laughter.]

I don't see any reason why this use should be limited to computer programs. As we get into, again, both a physical and digital future, we may find ourselves with, "you may use this in certain circumstances and not in others." And why computer programs should benefit from that and not our products, I don't see any justifiable reason for it.

Mr. SMITH. We will certainly consider that as we move toward markup.

Mr. Berman is recognized for a final question.

Mr. BERMAN. Mr. Chairman, just talking about your question, the answer—well, forget motion pictures. A photographer, an artist who authorizes a certain number of prints, why shouldn't they get the—why should just the software folks get—I mean they copyright their works. Why shouldn't they be able to deal with the trafficking and the licensing issue here like that?

Mr. LAMAGNA. Mr. Berman, before I respond to you, I must respectfully ask is this the devil I'm responding to or just—— [Laughter.]

Mr. BERMAN. No, no. This is now the real me.

Mr. LAMAGNA. Well, sir, we're not aware of any other industry that issues the same type of authentication certificate. Certainly

are willing to consider other scenarios, but at the present time, as my colleague, Mr. Simon——

Mr. BERMAN. I guess they are forging——

Mr. SIMON. Then it's no longer authentic.

Mr. BERMAN. Then it's no longer authentic.

Mr. SIMON. Then it's covered by the existing law.

Mr. BERMAN. That's right. That would be one answer. We'll try and figure out some other hypothetical here. [Laughter.]

Mr. SMITH. Thank you, Mr. Berman.

Any other questions? If not, let me thank the witnesses again for their very helpful testimony, and do appreciate your support of this legislation. We do expect possibly to mark it up next month. Thank you all again.

We stand adjourned.

[Whereupon, at 11 a.m., the Subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

PREPARED STATEMENT OF THE HONORABLE BOB GOODLATTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF VIRGINIA

Mr. Chairman, thank you for holding this hearing on this important legislation to curb counterfeiting.

Counterfeiting and piracy are unfortunately on the rise. The combination of enormous profits and relatively limited punishments, especially in foreign countries, makes counterfeiting an attractive cash cow for organized crime syndicates. Often specializing in audio and optical disc piracy, as well as business software piracy, these crime rings are capable of coordinating multi-million dollar efforts across national borders.

Over the years, legitimate businesses have become more accomplished in deterring counterfeiting by creating certificates of authenticity (COA) and other types of authentication documents included within the packaging of their products that serve as proof of the authenticity of the product. As these documents have become more complex and harder to copy, pirates have started to abandon efforts to copy these documents and have instead begun to either steal, or buy stolen, genuine authentication documents. These thieves then simply attach the stolen authentication documents to counterfeited goods and sell them as the real product.

The need to address this growing problem is clear. First, consumers lose when they pay for products that are presented as authentic, but that are actually of poor quality, or simply don't work. Second, businesses lose both revenue and goodwill when their products are counterfeited. Microsoft reports that as of 2004, approximately 500,000 genuine Microsoft COAs and COA labels were stolen. These documents are estimated to be worth $40 million. However, a potentially larger loss for businesses is the loss of future customers who are disillusioned with a company due to their experiences with the purchase of a counterfeited product.

H.R. 3632, the "Anti-counterfeiting Amendments," would address this growing problem by expanding the current law to expressly include genuine authentication documents within the definition of "counterfeit labels." The bill would also provide civil remedies for injured copyright owners and provide for the forfeiture of any equipment used to manufacture, reproduce, or assemble authentication documents or other types of counterfeit labels.

I look forward to hearing the testimony of our expert witnesses about the scope of this counterfeiting problem and how we can help better protect intellectual property rights.

PREPARED STATEMENT OF THE HONORABLE JOHN CONYERS, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN, AND RANKING MEMBER, COMMITTEE ON THE JUDICIARY

We all know that the piracy of digital content is a serious problem. After all, the copyright industries are this country's number one export, providing a positive trade balance of approximately $89 billion. It goes without saying that our content is a valuable resource.

Unfortunately, the value of copyrighted content makes it highly vulnerable to theft, and the losses for affected industries are staggering. The Business Software Alliance estimates that piracy cost software developers worldwide $13 billion in 2002. The music industry, including songwriters, artists, and record label employees lost $4.2 billion worldwide the same year. The movie industry loses $3 billion annually.

While there are laws on the books that deter and punish content piracy, they do not go far enough. There is a problem of copyright pirates getting genuine labels for content and then putting those labels on fake products. This not only harms the real manufacturer of the products but also the consumers. This conduct is virtually permissible because current law makes it illegal to sell fake labels but does not prohibit selling the real labels.

As we consider crafting a new remedy against piracy, though, we should make sure not to outlaw conduct that is and should remain legal. For instance, various industries take advantage of the parallel market to provide goods to consumers at a lower than normal cost. The Supreme Court has upheld this practice, but the market can continue only as long as goods are not tracked by their manufacturers to determine the chain of custody. It is my understanding that this bill would not do that.

PREPARED STATEMENT OF THE HONORABLE HOWARD L. BERMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Thank you Mr. Chairman and I appreciate your holding this hearing on H.R. 3632, the "Anti-counterfeiting Amendments OF 2003." In the last Congress, similar bills were introduced in both the House (H.R. 5057) and the Senate (S. 2395), but this subcommittee has never had a chance to analyze this issue. I am therefore looking forward to hearing from our witnesses about this bill.

Every day, thieves around the world steal millions of dollars worth of American intellectual property from the rightful owner. American innovation is a cornerstone of the American economy. The copyright industry alone employed over 8 million Americans in 2001. Software piracy alone has cost the U.S. economy thousands of jobs, and drains almost 11 billion dollars each year. According to the International Anti-Counterfeiting Coalition, the US Customs service seized more then $98 million in counterfeit and pirated goods in 2002—a 58 percent increase over 2001. To exacerbate the problem, counterfeiters of software, music CDs and motion pictures are no longer limiting themselves to pirating the actual goods. Counterfeiters are now tampering with component parts of the goods, the authentication features, which are used to ensure the genuineness of the product. This is what the bill is designed to address.

Just two weeks ago, Microsoft filed a suit in federal court alleging the sale of counterfeit software and related items. The complaint alleges that the defendants distributed counterfeit Certificate of Authenticity labels. Federal law currently provides a remedy for this type of counterfeiting. However, H.R. 3632 aims to address a gap in federal law that fails to address the trafficking genuine labels which are then used with counterfeit or pirated goods.

Last year Richard LaMagna of Microsoft Corporation (and we welcome him back again) testified before this subcommittee about the global threat of software counterfeiting. In his written testimony, he described the cheap, fake software sold on street corners which is typically marketed as the genuine article to unsuspecting customers who would never knowingly purchase counterfeit goods. To create the look of genuine packaged software, counterfeiters use state of the art technology to create near-perfect copies of CD ROMS, as well as the packaging, documentation, and other components. For many years, Microsoft, and I'm sure many other companies, have worked to outpace counterfeiting technology by developing physical features that help consumers and law enforcement agencies distinguish legitimate software from sophisticated counterfeits. However, as software makers have worked hard to ensure protection of their intellectual property, the counterfeiters have worked harder and smarter.

For example, Microsoft has included a certificate of authenticity that incorporates special inks, holograms and microtext with its software. So far, counterfeiters have found it impossible to replicate the technology. But as the technology used to protect intellectual property has gotten more sophisticated, so have the counterfeiters. Because physical anti-counterfeiting features are increasingly difficult to reproduce, counterfeiters are now combining pirated CD ROMs and packaging them with the genuine authentication components obtained through fraud or theft. Through a gap in the law we have actually created a separate market for merely the authentication components.

This bill expands the scope of "counterfeit labels" to include other physical authentication components such as certificates. In addition, it addresses the situation where genuine certificates are distributed not in connection with the product of the copyright owner, or where the label is altered to falsify the number of authorized copies. The bill also provides for civil remedies for violations of the Act.

While this bill confronts the concept of trafficking physical component parts, I would be interested in hearing from our witnesses about interpretation or expansion of the bill to include digital components. In an age in which technologies are rapidly developing, I believe there is a need to address the evolution of digital authentication features and the potential for copying or counterfeiting them as well. The legal dichotomy of physical and digital should be a distinction without a difference. Whether a physical or digital feature is counterfeited is equally problematic. I do not intend for this to become another digital rights management debate. I do, however, wish to address punishing and preventing counterfeiting. Counterfeiters do not only prey on the copyright owners. Counterfeiters prey on the consumers who have certain expectation when buying what appears to be a genuine product.

If the Chairman is so inclined, I look forward to working with him on these issues before mark-up.

○